SecureIdentity DLP

Upgrade guide

v15.13.1

SecurEnvoy
A Shearwater Group plc Company

Intellectual Property Rights

This document is the property of SecurEnvoy. No part of this document shall be reproduced, stored in a retrieval system, translated, transcribed, or transmitted by any means without permission from SecurEnvoy.

Information contained within this document is confidential and proprietary to SecurEnvoy and should not be disclosed to anyone other than the recipients and reviewers of this document.

However, in the event of award to SecurEnvoy, this information may be disclosed to and will be used on behalf of and according to the interests of the client to whom it is addressed.

Confidentiality Statement

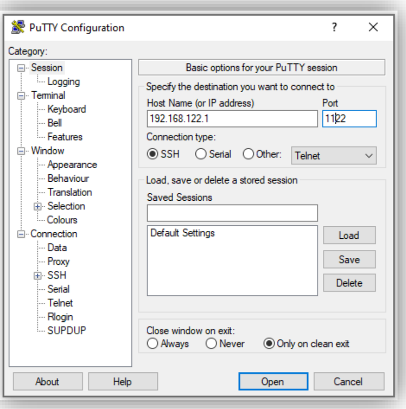
The descriptive materials and related information in this document contain information that is confidential and proprietary to SecurEnvoy. This information is submitted with the express understanding that it will be held in strict confidence and will not be disclosed, duplicated, or used, in whole or in part, for any purpose other than evaluation of this document.

Upgrading the Central Console

IMPORTANT – Take a backup of the Configuration settings including the Event logs. Also, it is best practice to take a complete server backup (or snapshot) of the current server state BEFORE performing the upgrade.

1) Log in to the Console CLI using PuTTY and root credentials on port 1122

Username: root
Password: pass8397@



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.122.1
Port: 1122

Connection type: ● SSH ○ Serial ○ Other: Telnet

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

2) Once logged in you need to obtain the latest upgrade patch, this actual filename can be obtained by contacting your partner or SecurEnvoy, in this example we are upgrading to 15.13.1x *(make a note of the exact file name you've been given for the command below).*

3) Type the following command at the prompt:

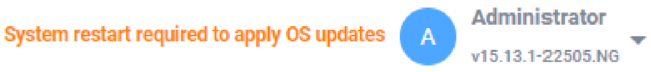
rpm -Uhv https://downloads.securenvoy.com/dlp/SecurEnvoy-cc-securEnvoy-cc-15.13.1-22505.NG.SecurEnvoy.el7.x86_64.rpm

4) Once this has installed type the following command

yum update

Note: "yum update" updates all the presently installed packages to their latest versions that are available in the repositories.

5) Answer "Y" to any prompts and wait for "Complete!". Then type "exit" to close the PuTTY session.
6) **Open the Central Console URL from a browser**. You will note the "System restart required…" message. Click the 'Restart' button and wait for the system to restart…



System restart required to apply OS updates

Administrator

v15.13.1-22505.NG

Troubleshooting

Access to the internet during upgrade process
The upgrade process needs to download some additional packages from our technical development site. If it cannot reach this external site, the upgrade will fail with a number of "package" errors. For example:

"Package javapackages-tools do not exist…"

Please grant the machine temporary internet access so that the process can complete successfully. If this is not possible, the packages will need to be obtained from your SecurEnvoy partner or SecurEnvoy support.

Once the packages have been obtained and placed on the Central Console machine, type the command (note: filename may change depending on the build).

rpm -Uvh se-localrepository-15.13.1-22516.el7.x86_64.rpm

Release Notes

Changes to 15.13.1
August 2022

Detection Engine

Enhancements:

1. Improved Brazilian CPF policy. Added validation and Dirty version.
2. Improved built-in regex for ISBN-13 pattern.
3. Improved built-in regex for ISBN-10 pattern.
4. Improved buil-it regex for common financial dollar.
5. Improved Indian Password and Indian Tax (PAN).

Fixes:

1. Detection Engine does not find the breach in the attached XLSX file due to the wrong Filter Output (#11641).

Central Console

New Features:

1. Added Last Seen column to the Endpoint Network Status tab.
2. Implemented IP addresses support in the Asset Templates tab.
3. Implemented Endpoint Agent Uninstall Password mechanism.
4. Added Zoom protocol to the Endpoint Agent ACL rules.

Enhancements:

1. Updated internal backend database to v12.
2. Added the License expiration and Low free disk space checkboxes to the email Alert page of the User Management tab.
3. Added search to the LDAP object tree.
4. Implement export to the CSV of the Devices.
5. Removed an old interface functionality from the Central Console.
6. Added two new columns on Child Consoles: IP and Status.
7. Extended the Antivirus Exception list on the Downloads tab.
8. Added validation for the Negative Patterns creation to avoid of broken patterns.
9. Enabled LOG I/O for MTP devices.
10. Added validation for importing Policy JSONs which may contain duplicates.

11. Added security fixes to the Inspector.
12. Add support for MTP/PTP Device channel.
13. Included a username into the SIEM Inspector event.
14. Included LAST SEEN column in the CSV report.
15. Included the full File Path to the CSV Export of Monitoring events.
16. Added destination Map tab for All events in Network events case.

Fixes:

1. Added the latest security fixes to the Central Console.
2. Add the tooltip with objects distribution by LDAP categories to the LDAP Objects value (#4366).
3. Change mislabel settings input fields to plain text (#4460).
4. The long list with applied filters is broken in the tooltip (#7148).
5. Fix the tooltips for Update and Uninstall buttons in the Network Status (#7153).
6. The domain PC is not available in the Non-domain PC category if was added LDAP with Base DN filter that excludes this PC (#4515).
7. Normalize filter work at the Policy Editor page (#4914).
8. Select by default the data in motion report by scan type in the Create Report window (#5577).
9. The Applied filters value is shifted if the chart name is too long (#5920).
10. Filter by column Violation does not work (#5843).
11. User with the Event Reviewer role should not able to see SRT/DST metadata in the Graphical Reports (#7005).
12. Add the result message after deleting the report (#5868).
13. The scan report wasnt send after the scan finished (#7108).
14. Forbid creating the Reports with equals names in the same category (#7120).
15. Change the font size of the message if no report inside the category (#7150).
16. Reset doesnt drop the search result in the Reports (#7154).
17. CSV report for the Event Handler role should include only those events, which assigned on this user (#7245).
18. Token Updated On ON column is not updated (#6999).
19. Inspector is always OFFLINE if the custom port is using (#7103).
20. The names of Classification actions Taken are mismatched in the widgets legend (#6281).
21. Add the confirmation window while exporting to with unapplied filters (#6285).
22. Search doesnt work for simple policy values (#6465).
23. File type info is not displayed for some channels in Classification events tab (#6483).
24. Add the MTP/PTP Device channel to the export CSV file (#6592).
25. Add exclude OneDrive FB Locations for scan (#6678).
26. Add validation for prohibit adding .e symbols (#6865).
27. Add status message for saving the System Update settings (#7028).

28. Clipboard alerts are send for Classification Device Control events (#7056).
29. Connection error in the Exchange scan while synchronization (#7057).
30. Record numeration is not good starting from the 2nd page on the Network Status tab (few records always missing) (#7063).
31. Fix the url to the Central Console in the License expired email (#7064).
32. An email SecurEnvoy DLP license is about to expire! was sent to the user if licensing is Perpetual (#7066).
33. Display the password button is not displayed after unsuccessful password sending (#7069).
34. Manual Check System update doesnt update Last run value (#7078).
35. Refresh Fingerprints button doesnt work in the Classification setting (#7137).
36. Add the text update status to the Endpoint Agent Details window (#7104).
37. Attach the Scan Job Summary PDF into the Scan Job Complete email notification related to Cloud Scan (#7109).
38. [Discover File Shares] When you try to add credentials the window that opens freezes (#7112).
39. [SharePoint] Scanjob window freezes after scanning with copy and exclude (#7118).
40. [Network Status] Filter not working in table # (#7128).
41. [Network Status] Domain filter does not work for non-domain machines (#7145).
42. Cannot save the build-in policy if was changed Proximity only (#7174).
43. The MS Exchange scan table is not updated after starting the scan by the start command (#7136).
44. View button does not work properly in Policy Management (#7186).
45. [Policy Management] Infinite loading when trying to clone a regular expression with the same name (#7189).
46. [Policy Management] In policy editor, it turns out to add policies with empty objects (#7212).
47. [Policy Management] Need to add scrolling if many objects are added to the policy. (#7220).
48. Chinese text appears in the getCustomizeNotifications in the uj_network array for the French language (#4358).
49. The sorting arrow is above the column name in the TMR chart (#4653).
50. Window Processing is hanging until all widgets are loaded (#4656).
51. If was enabled incremental scan the CC adds all scans as a new object to the local scan at PC level (#4766).
52. Keep the selected values of the X/Y Axis at the report settings on Report Type changing (#5041).
53. Different events quantity in the Policy Violations grouped by data and total (#5595).
54. Change the date format in the downloaded Dashboard report (#6502).
55. The search does not work in the add new target mail window (#6731).
56. Custom date filters apply the wrong date period in the grid chart (#6933).

57. The search does not work in the Add Mailbox Groups (#7002).
58. Actions filter is not applied for the Actions Taken chart grouped by Date (#7014).
59. Fingerprint test connection failed if set non-CC IP address (#7127).
60. After adding the WhatsApp channel the build-in reports were duplicated (#7173).
61. Deploy is blinking when no changes are done in Network DLP (#7176).
62. The Category combo-box is not active while importing the policy when only 1 Category is created (#7187).
63. Cleanup previous FP Storage after IP changing at Fingerprints Settings (#7191).
64. The file type was not copied using Copy to feature (#7210).
65. Ignore Case sensitive in LDAP object tree search (#7217).
66. [Policy Management] If you write a long object name, then the add window goes beyond the workspace. (#7218).
67. [Policy Management] Can Edit the name of the policy to an existing one (#7223).
68. [Policy Management] Error in case of category cloning (#7236).
69. Test connection to the FPS success with a wrong FS port (#7272).
70. Values in the Local PC Paths table are not by the center (#7317).
71. Need to put proper Remedial Action names for Printing DLP while Viewing Endpoint Policy (#7336).
72. Investigate why some policies from the categories cannot be removed (#7354).
73. Empty tooltip in the LOGGED ON USER column if no value (#7363).
74. Need to forbid Copy From to itself for Copy of Policy Management (#7373).
75. Add autocomplete to the Assign to field in the workflow settings (#7376).
76. Extend the list of Linux family OS (#7381).
77. Exported CSV with events should contain Justification text (#7384).
78. OS value is not reported to the CSV file from Network Status (#7385).
79. No need to clean up computers from the table agents if the Events Only backup was restored (#7391).
80. The cloud scan with the same name was not created, no information was provided (#7424).
81. Clients complain about Agents disappearing from the Network Status tab (#7429).
82. Compare Endpoints Policies does not work for Application Controls (#7433).
83. Added policies are not displayed during adding them to the category (#7440).

Endpoint Agent

New Features:

1. Implemented Zoom inspection.
2. Implemented Endpoint Agent Uninstall Password mechanism.
3. Implemented Proxy and PAC auto-config file integration.

Enhancements:

1. Optimized License grabbing mechanism.
2. Implemented fast load of fingerprints hashes to the PC RAM.
3. Implemented detection of creating/open, read/write and commit/close operations on MTP devices.
4. Improved service management mechanism. Get it work in another way: stopping, updating config, starting services.
5. Added a bunch internet headers after MS Outlook email inspection: skip/success/fail.

Fixes:

1. Endpoint Agent Manager produces a lot of logs on the PC Registration Check (#15455).
2. The Update Manager feature does not support the Custom Port option (#15476).
3. No need to send the LDAP GUID in the Update Manager API if the PC is non-domain (#15466).
4. Some big enough files were not classified and temp files for small files scan were not deleted (#14533).
5. In some cases, violations are not detected in embedded files: EMF/WMF, inc. embedded, are OCRed (#14665).
6. The local scan was run when the Scan start expiration option expired (#12388).
7. Endpoint Agent uninstall with the REMOVE_SCANNER key should not remove imported client certificate from the ROOT TRUSTED storage in the Certificate Manager (#15411).
8. Report the update message Reboot required if it needs while self-update (#15479).
9. The user is not able to paste the print-screen result if the Greenshot, ShareX, Win + Shift + S application is running (#15494).
10. Allowed Domain feature does not work if Classify based on content Email Mapping or Network inspection is disabled (#15521).
11. Detect MIP Classification for files only using GUID from the MSIP_Label_GUID_Name (#15528).
12. SRC and DST are n/a in the SMTP event generated on Outlook email (#15522).

13. Make it possible to patch/re-patch already installed Endpoint Agent by running a script (#15514).
14. MS Outlook inspection window was not closed after the email has been sent (#15518).
15. PASS rule for the HTTPS does not work in Firefox (#15512).
16. Endpoint Agent wrongly applies the PASS rule for the HTTP protocol however it should PASS only the HTTPS traffic due to the ACL Rule in the Internet Explorer (#15513).
17. Unclassified duplicate email remains in Outbox for Exchange email accounts (#15555).
18. Network Endpoint Agent does not detect a breach in non-txt files uploaded in Firefox (#14355).
19. Excluding Outlook TCP inspection does not work for objects in the Application Control (#13987).
20. Incorrect ACL Rule (the last one Any) triggers instead of those which are present above (#15549).
21. Assigned LDAP does not work for domain users (#15571).
22. Consider the possibility to move temp files from C:\Windows\cap to the C:\ProgramData\SecurEnvoy\ (#15446).
23. Endpoint Agent should report UserName who runs the scan to the Central Console > Logs (#15484).
24. Make the SecurEnvoy Classifier window wider (#15603).
25. Network Inspection on Google Drive does not work from sidenly (#15595).
26. [Customize Notification] Change the source fields for the Blocked Executing pop-up (#15356).
27. Clipboard inspection does not work for MS Excel files in the Protected view and PowerPoint files (#15606).
28. Make it possible to patch/re-patch already installed Endpoint Agent by running a script (#15514).
29. The Endpoint Agent assigns META_ACTION value = 0 for classified outlook emails if the ACL rule only has a classification policy (#15622).
30. RMA process crashes every time if the license for the App control is not persisted (#15627).
31. Copy/Move operation failed with error: Cannot move(via copy) Error: Access is denied (#15410).
32. Please send a full classification name for EP and Discovery events when MSIP integration is enabled (#15648).
33. No classification is detected in one of the OPC files if the classification was made with ShellExtension/Discovery (#15610).
34. Cannot write folders with files exceptions to USB when the Write access is blocked (#15646).
35. Clipboard inspection stopped working unexpectedly - deadlock fixed (#15375).
36. The user is not able to paste the print-screen result for ShareX (#15494).

37. The Endpoint Agent may wrongly apply the File Share DLP/Audit settings for the local path (#14678).
38. The Endpoint Agent shows the fake popup window Saving to Removable Media is not allowed on copying files to the File Share if the Files hare Audit license is missing (#15674).
39. The Endpoint Agent tries to classify zip64 OPC files (#15662).

Discovery Server

New Features:

1. Made it possible to perform a remedial action Copy/Move to the cloud SP/SPO/S3/Google locations.

Fixes:

1. Spam warning in Endpoint Agent logs in the OneDrive for Business scan (#15483).
2. MS Exchange scanning will fail if Microsoft Office Standard is used (#15604).
3. Discovery Server scans the files in Exclude URL folder in the OneDrive for Business (#15418).

Network Inspector

New Features:

1. Implemented Enforcing Header to Encrypt after inspection. The internet header forces the Inspector to Encrypt the email after inspection. The message is being sent to the Encryption Gateway. Adds Encryption Headers to the email and could be used by the Endpoint Agent or email client plugins. Example: EPAgentEncrypt: yes.

Enhancements:

1. Added security fixes to the Inspector.

Fixes:

1. Added the latest security fixes to the Inspector.
2. Fixed description of multiple Encryption Gateways in the Inspector Configuration tab.

3. Retain events with META_CONTENT_PARENT_STREAM_NUMBER (#8050).
4. File Capture for multiple email attachments became broken after implementing a single event (#15500).
5. Inspector may generate 2 or more events on the same sent email that was quarantined (#8040).
6. Inspector does not inspect emails via MTA if in the Encryption subject keywords parameter is empty at Configuration > Quarantine & Encrypt (#15507).
7. Apply a filter to the System Logs selector (#15499).
8. Allow to define not only the ACSII symbols at Configuration > Quarantine and Encrypt > Encryption subject keywords (#15508).
9. Custom Port of Central Console does not work properly (#15493).
10. Inspector does not detect the breach in email attachments if 2 or more emails were forwarded attachments (#15502).
11. Fixed NPL crash in CLogger::SystemLog (#15639).
12. The Email Backup feature does not copy the e-mail to the Files Share in the case when a lot of breaches are detected in the email (#15650).