Sentinel™ 5

Product Release Notes

Product

Sentinel™ 5.1.1 Full and Patch Release

Contents

Description

This is a full and patch Sentinel™ 5.1.1 release with iTRAC™.

Installation

See the following chapters in the Sentinel Install Guide.

- Oracle Install – see Chapter 3, Installing Sentinel 5 for Oracle
- MS SQL Install – see Chapter 4, Installing Sentinel 5 for MS SQL

Patching

NOTE: For upgrading, you cannot go directly from v4.2 to v5.1.1. You must first migrate data to v5.1 before patching to v5.1.1. For v5 and v5.0.1, you cannot upgrade directly to v5.1.1. You must first upgrade to v5.1 before patching to v5.1.1.

See the following chapters in the Sentinel Install Guide.

- Oracle Upgrade – see Chapter 5, Data Migration and Patch for Oracle
- MS SQL Upgrade – see Chapter 6, Data Migration and Patch for MS SQL

New Features

- Crystal XI upgrade from Crystal 9. New features include:

Version 5.1	Version 5.1.1
▪ Advisor ▪ Aggregation ▪ Analyst ▪ Compliance ▪ Incident Management ▪ Dashboard ▪ Operation Efficiency - IDS - Internal Events - Lockout - Source Destination Ports - Vulnerability	▪ Advisor and Vulnerability ▪ Top 10 Reports ▪ Security Events ▪ Compliance Events ▪ Incident Management ▪ Internal Events

  - Supported Operating System: Windows 2003 Server
  - Significant Performance Improvements in 'Top 10' reports

  For installation and configuration information, see the Sentinel 5.1.1 Installation Guide.

- SMTP authentication - User can set SMTP authentication in execution.properties file. There are two script files that can change and test the configuration of execution.properties file.
- Agent Command Line Interface (Agent_CLI) – This command line interface allows you to start, restart and stop individual Wizard Ports. The interface file is located:

  For Solaris:

  ```
  $WORKBENCH_HOME
  ```

  For Windows:

  ```
  %WORKBENCH_HOME%
  ```

  To use this command:

NOTE: Host name and Agent Port name arguments are case sensitive.

  For Solaris, login as esecadm:

  ```
  ./Agent_CLI (--version) (--start|--stop|--restart
    Agent_port:<IP|Host name>) (--sendEvents
    No.Events) (--debug)
  ```

  For Windows:

  ```
  Agent_CLI (--version) (--start|--stop|--restart
    Agent_port:<IP|Host name>) (--sendEvents
    No.Events) (--debug)
  ```

NOTE: Transient set to "yes" is required with service name 'agentmanager_cmd' in the configuration.xml file located in %ESEC_HOME% or $ESEC_HOME and should not conflict with existing service uuid's.

- Correlation engine now includes the first event when using the inside/outside rule.

Bug Fixes

Sentinel

6405

Issue: The correlation engine does not list the first event for inside/outside rule.

Fix: Fixed VTE for inside/outside rules.

7150

Issue: Able to create correlation rule folders with only blank spaces as the folder name.

Fix: Leading and trailing trimmed. Error message will appear is a user attempts to create a folder name with only blanks.

7241

Issue: An error message is not displayed when executing Agent_CLI.exe with invalid input arguments.

Fix: Added long option argument parsing logic.

7301

Issue: Crystal Reports does not work in the Sentinel Console Center.

Fix: When clicking save, duplicate inserts of the Crystal Server URL was entered into the database. This has been fixed.

7311

Issue: When running hpconfig.bat at the command prompt to reset the password, the command will throw back an exception.

Fix: The code has been fixed so that hpconfig.bat properly works and will not throw an exception.

7312

Issue: esec_toIpNum function was not installed.

Fix: Added to config.xml for installation.

7313

Issue: esec_utl.to_ip_num gives incorrect number, function omits last digit in output.

Fix: Added migration script and updated db_patch_matrix.xml.

7314

Issue: Unable to send an incident to HP Service Desk.

Fix: Incidents can be sent to HP Service Desk.

7331

Issue: Sentinel Console slows down in over time and runs out of memory. This results in a Sentinel system crash.

Fix: A memory leak and an Active Views null pointer has been fixed.

7337

Issue: Unable to modify responsible field for Incident associated to workflow.

Fix: The Incident Workflow panel has been modified such that the Incident Details "Responsible User" combobox is not disabled if an iTrac process is associated with an Incident.

7338

Issue: Each time an event table is created (Active Views, quick query, incidents, etc.), a remote request for the branding map is made. If this times out, it will freeze the Sentinel Control Center up for 30 seconds until the timeout.

Fix: Branding map is loaded one time when the first event table is loaded.

7344

Issue: For iTRAC, the show Diff button in the Import/Export Wizard doesn't work.

Fix: The show Diff button now works.

7346

Issue: email was being sent out without SMTP authentication from Sentinel.

Fix: Added SMTP authentication.

7348

Issue: Unhandled error code from MSSQL causes peer socket reset.

Fix: A SQL server state code was added to FatalError data structure

7349

Issue: The event field RN (Reporter Name) is missing.

Fix: RN field added.

7350

Issue: For Solaris, data migration would fail if the v4.2 and v5.1 database had a different user for the Oracle database schema owner. For Windows, data migration will fail if the MS SQL database administrator for v5.1 is set to Windows Authentication.

Fix: Added a script to Oracle and MS SQL installations. For Oracle, script will add esecdba to the v4.2 database. For Windows, script will add esecdba to the v5.1 installation.

Wizard

7330

Issue: The ODBC agents will unnecessarily close and reopen the database connection if the number of rows returned is less than the maximum row count. This is an overhead when the events flow is higher and less than the maximum row count for each iteration.

Fix: Fixed closing and reopening issue on the following agents: (1) Template ODBC, (2) Site Protector and (3) eEye Retina. The agents are not automatically installed but are available on the Sentinel installation disk.

Known Issues

- Overall Crystal Report formatting using the Sentinel Console Center is difficult to read. Workaround is to access Crystal Reports through the Crystal Console (Crystal Server) using an external browser such as Internet Explorer or Netscape.
- Advisor and Top 10 Crystal Reports are currently being enhanced. Please check with Technical Support for the latest Reports.
- Crystal Reports - Currently the reports from within the GUI cannot be printed, but can be exported. Only available export format type available is pdf. To export as pdf, click the print button within the report and in ‘save as’ dialog box rename the file with a pdf extension. Please check with Technical Support for the latest Reports.
- Crystal Reports - The graph for the 'Event Severity Trend' report does not represent a proper representation of event severity count trend.
- Crystal Reports - Date Range is displayed when selecting report type of Daily, Weekly or Monthly for the following reports: 'Event Count By Product Name’, 'Event Count Trend' (Oracle only), and 'Daily Event Trend By Sensor Name' (Oracle only).
- Crystal Reports - Title heading for ‘Daily Event Count By Sensor Name‘ is incorrect. When running this report, the report header displays 'Event Count Trend By Sensor Name'.
- Crystal Reports - Format for 'Correlated Incident Status' and 'Incident Status' is difficult to read and Incident Count is displayed in decimals.
- For Solaris, WorkFlow will not proceed beyond the Start Eradication Process when attempting to execute arp –a command. Workaround is to (1) login and user esecadm, (2) create a '.profile' file under '/export/home/esecadm' and modify it to add '/usr/sbin' to the path environment variable and (3) modify the template activity to run a different activity.
- When setting a filter in the view options for incidents, agents, agent managers or iTRAC, the attribute fields that hold dates may fail to work properly if included as part of the filter.
- In Sentinel Control Center > Admin Tab, Active User Sessions will temporarily display a session for a user that has logged in to Agent Builder.
- If the Analyst role is empty (on product install it is empty) and an auto response workflow is instantiated, the server assigns _WORKFLOW_SERVER. But when a user is later added to the Analyst role, the assignments are not recalculated and the new user does not get workitems associated with that process. The workarounds follow:
  - Before starting any workflow process, make sure that all assigned groups have at least one user. This will prevent the previously described problem.
  - If an iTRAC process was instantiated without a assigned group having at least one user, perform the following steps to resolve the issue:
    - Add a user to the affected group.
    - Edit the corresponding template and save. No change to the template is required for this. You may just double click on the manual activity to popup the customizer dialog, select the same resource again, click OK and save the template.

This should force recalculation of workitem assignments. Users in the analyst group will now see workitems for that activity.

- Cannot edit while creating a user-defined template in the same template customizer after saving. The workaround is after saving the newly created template, to make modifications on the template, close the template window and open again.
- Range Map is regenerated every 30 minutes until first non-empty version of map is generated.
- When using "Populate Network" capability in Agent Builder, UUIDs are not reset in the copied port configurations. This results in the events from copied port configurations having the same Source Id.
- Attempting to take a screenshot of the installer by typing Alt+PrintScreen results in the graphics in the installer being garbled. This is caused by a bug in InstallShield. The workaround is to use only the PrintScreen button.
- On Windows, on a system where the Sentinel 5.1 patch installer was used, uninstalling the Database may fail. The workaround is to uncheck the Database component in the uninstaller, run the uninstaller for the other components you wish to uninstall, perform the manual cleanup step in the Sentinel Install Guide for MS SQL.

Product Support

- For Technical Support, email at support@esecurity.net
- For information, email at info@esecurity.net
- Website: www.esecurity.net
- For 24x7 support, call technical support directly at 800-474-3131