

Emergency Database Purge

Slide 1

Tivoli

IBM

IBM Security SiteProtector System v2.0 SP8.1

Emergency database purge



This is a self-running demonstration that shows you how to complete a task.
Controls are available at the bottom of the screen.

© Copyright IBM Corporation 2011 All rights reserved.

Emergency Database Purge

Objectives



Objectives

When you complete this module, you will be able to:

- Describe how the emergency purge job removes data
- Configure thresholds and purge margins for an emergency data purge
- Purge data manually



Emergency purge process

The emergency purge job keeps the SiteProtector Database within user-defined size limits

- 1 The emergency purge job removes the oldest data based on the Purge Item Age settings
- 2 If the first purge does not bring the database size below the Database Size Threshold, the job runs again removing a bulk percentage of data regardless of data age
- 3 If the second purge does not bring the database size below the Database Size Threshold, the job runs every 10 minutes until the database size is below the Database Size Threshold

Note: You cannot interrupt the process once the emergency database purge has begun

Emergency Database Purge

Slide 4

The screenshot shows the SiteProtector Agent View interface. On the left, a tree view shows the site structure: My Sites > 192.168.5.128 > IBM-ISS > Network IPS > Ungrouped Assets. The main area displays a table of installed components. A yellow callout box points to the 'SiteProtector Database' row, with the text: 'In the Agent view, select the SiteProtector Database.' A purple callout box at the bottom left contains the text: 'This demonstration shows you how to configure an emergency purge.'

Model	Asset	Agent Name	Status
SiteProtector Database	SITEPROTECTOR	SP Database	Active
Event Collector	SITEPROTECTOR	EventCollector_SITEPROTECTOR	Active
SiteProtector Core	SITEPROTECTOR	SP Core	Active
Deployment Manager	SITEPROTECTOR	DeploymentManager	Active
Agent Manager	SITEPROTECTOR	AgentManager_SITEPROTECTOR	Active
X-Press Update Server	SITEPROTECTOR	UpdateServer	Active
SecurityFusion Module	SITEPROTECTOR	SecurityFusionModule	Active
GV1000	myhost	myhost	Offline
GX4004	192.168.5.199	godzilla	Offline
GX5108	192.168.5.200	mothra	Offline

Find... 10 rows with 1 selected. administrator Notifications

Emergency Database Purge

Slide 5

The screenshot shows the SiteProtector interface. A yellow callout bubble with the text "Select Object." points to the "Object" menu item in the top navigation bar. The main window displays the "Agent View - Default" with a table of agents. The table has four columns: Model, Asset, Agent Name, and Status. The first row is selected.

Model	Asset	Agent Name	Status
SiteProtector Database	SITEPROTECTOR	SP Database	Active
Event Collector	SITEPROTECTOR	EventCollector_SITEPROTECTOR	Active
SiteProtector Core	SITEPROTECTOR	SP Core	Active
Deployment Manager	SITEPROTECTOR	DeploymentManager	Active
Agent Manager	SITEPROTECTOR	AgentManager_SITEPROTECTOR	Active
X-Press Update Server	SITEPROTECTOR	UpdateServer	Active
SecurityFusion Module	SITEPROTECTOR	SecurityFusionModule	Active
GV1000	myhost	myhost	Offline
GX4004	192.168.5.199	godzilla	Offline
GX5108	192.168.5.200	mothra	Offline

At the bottom of the window, a status bar shows "10 rows with 1 selected." and "administrator" with a user icon. A "Notifications" icon is also present.

Emergency Database Purge

Slide 6

The screenshot shows the SiteProtector application window. The main area displays a table of agents. A yellow callout bubble with the text "Select Properties." points to the "Properties" section on the left sidebar. The table has columns for Asset, Agent Name, and Status. The status of the agents is as follows:

Asset	Agent Name	Status
SITEPROTECTOR	SP Database	Active
SITEPROTECTOR	EventCollector_SITEPROTECTOR	Active
SITEPROTECTOR	SP Core	Active
SITEPROTECTOR	DeploymentManager	Active
SITEPROTECTOR	AgentManager_SITEPROTECTOR	Active
SITEPROTECTOR	UpdateServer	Active
SITEPROTECTOR	SecurityFusionModule	Active
GV1000	myhost	Offline
GX4004	192.168.5.199 godzilla	Offline
GX5108	192.168.5.200 mothra	Offline

At the bottom of the window, a status bar indicates "10 rows with 1 selected." and shows the user "administrator".

Emergency Database Purge

Slide 7

The screenshot shows the SiteProtector console interface. The main window displays a 'DATABASE SIZE' chart with a 'Fail Level' at 80% and a 'Warning Level' at 70%. The chart shows the database size is currently near 0%. A yellow callout bubble points to the 'Database Maintenance' icon in the left sidebar, with the text 'Click Database Maintenance.' Below the chart, there is a section for 'TempDB Database Size (MB)' with a description: 'The size of the TempDB Database file to store data that is updated during m...'. The 'Remedy' link is 'What can I do if the system al...'. The console also shows 'Agent Messages' with 'Event Loading' status.

SiteProtector

Object Edit View Action Tools Help

New [Icons] Go to: Properties

Agent : 192.168.5.128 : IBM-155 Properties : 192.168.5.128 : SP Datab...

Health Summary

Agent Details

Database Maintenance

Command Jobs

Database Jobs Performance

DATABASE SIZE

1 day 3 day 7 day 1 month 3 month 6 month 12 month

Fail Level

Warning Level

80

70

60

20

10

0

8 AM 12 PM 4 PM 8 PM 12 AM 4 AM

Time

Agent Messages

Event Loading

Description: The percentage of used space to the amount of space allocated to the TempDB database file to store data that is updated during m...

Your Site will stop functioning if the database file becomes full.

Remedy: [What can I do if the system al...](#)

TempDB Database Size (MB)

1 day 3 day 7 day 1 month 3 month 6 month 12 month

Description: The size of the TempDB Database file to store data that is updated during m...

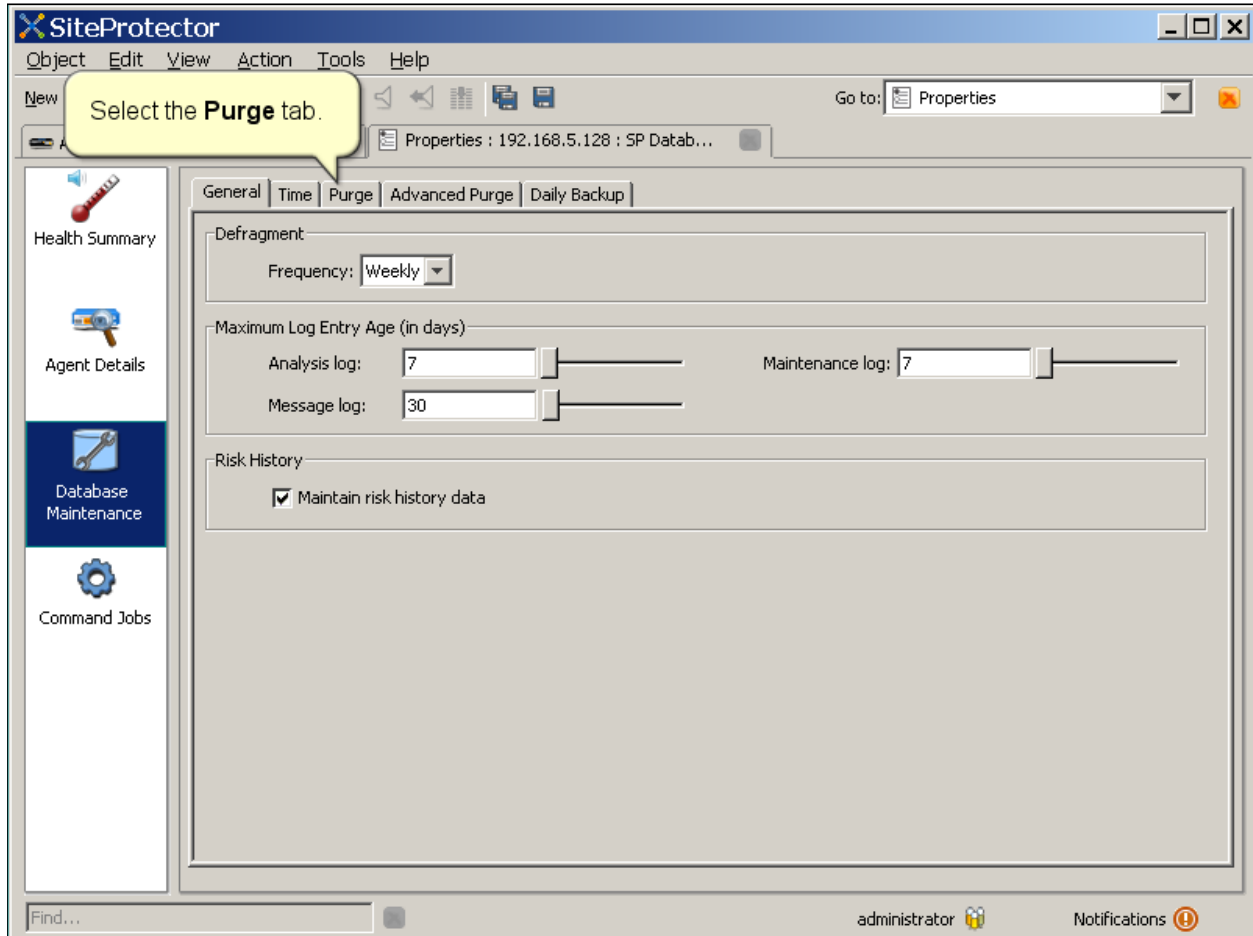
Find...

administrator [User Icon]

Notifications [Icon]

Emergency Database Purge

Slide 8



The screenshot shows the SiteProtector application window with the 'Database Maintenance' tab selected. A yellow callout bubble points to the 'Purge' tab in the navigation bar. The 'Purge' tab contains the following settings:

- Defragment:** Frequency: Weekly
- Maximum Log Entry Age (in days):**
 - Analysis log: 7
 - Message log: 30
 - Maintenance log: 7
- Risk History:** Maintain risk history data

The interface includes a menu bar (Object, Edit, View, Action, Tools, Help), a toolbar, a 'Go to:' dropdown menu, and a status bar at the bottom showing the user 'administrator' and a 'Notifications' icon.

Emergency Database Purge

Slide 9

The screenshot shows the SiteProtector interface for Database Maintenance. The 'Purge' tab is selected, showing the 'Emergency purge' checkbox, which is currently unchecked. A yellow callout bubble points to this checkbox with the text: "Select the Emergency Purge option." Below this, the 'Database size threshold' is set to 85% and the 'Purge margin' is set to 5%. A blue callout bubble at the top right of the settings area contains the text: "Purges might take a long time, especially if your database is large." The 'Data Retention Settings' section shows 'Purge Frequency' set to 'Never' and various item age limits for different event types. At the bottom, a section titled 'To set up notification rules for Database Purge and Size Status:' is partially visible. The interface includes a menu bar (Object, Edit, View, Action, Tools, Help), a toolbar, and a status bar at the bottom showing the user 'administrator' and a 'Notifications' icon.

SiteProtector

Object Edit View Action Tools Help

New [Icons]

Go to: Properties

Agent : 192.168.5.128 : IBM-I55 Properties : 192.168.5.128 : SP Datab...

Health Summary

Database Maintenance

Command Jobs

General Time Purge Advanced Purge Daily Backup

Maximum Database Size

Emergency purge

Database size threshold: 85 %

Purge margin: 5 %

Data Retention Settings

Purge Frequency: Never

Maximum Item Age (in days)

Analysis summary events:	90	Cleared analysis summary events:	1
Analysis detail events:	30	Cleared analysis detail events:	1
Incidents:	90	Exceptions:	1
Audit:	999	Job history:	7
Metrics:	180	Unused assets:	6
Resolved tickets:	30	Mail data:	5

To set up notification rules for Database Purge and Size Status:

Find...

administrator [User Icon] Notifications [Icon]

Emergency Database Purge

Slide 10

The screenshot shows the SiteProtector Database Maintenance configuration window. The 'Purge' tab is active, showing the 'Maximum Database Size' section with 'Emergency purge' checked, a 'Database size threshold' of 85%, and a 'Purge margin' of 5%. The 'Data Retention Settings' section shows 'Purge Frequency' set to 'Never' and various event retention counts. Callouts provide instructions on saving and setting the threshold and margin. A purple box explains the default settings for Express vs. Recommended installations.

Click **Save**.

Select the percentage the database must exceed before an emergency purge begins. The default value is 85.

Select the percentage of data SiteProtector purges when the database size threshold is reached.

If you used the Express installation, the emergency purge is enabled with a size threshold of 85% and a purge margin of 5%. If you used the Recommended installation, the emergency purge is disabled.

Emergency Database Purge

Purging Data

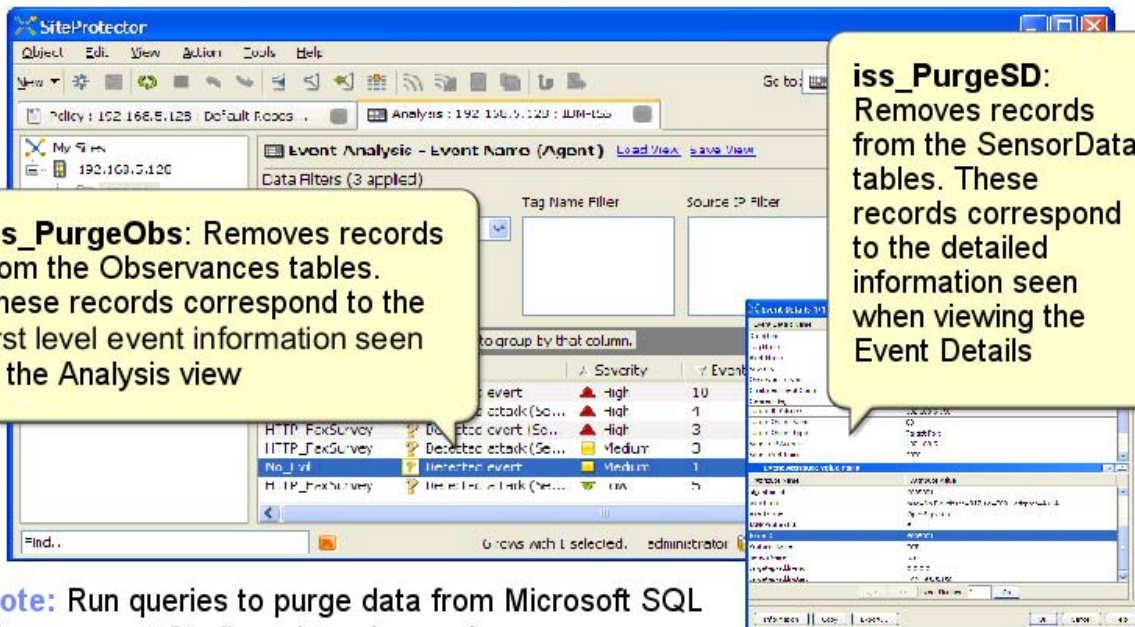


Purging data

The most common procedures used to purge data are:

iss_PurgeObs: Removes records from the Observances tables. These records correspond to the first level event information seen in the Analysis view

iss_PurgeSD: Removes records from the SensorData tables. These records correspond to the detailed information seen when viewing the Event Details



Note: Run queries to purge data from Microsoft SQL Management Studio or by using osql

© 2011 IBM Corporation



Purging data manually

- **To purge all types of data time-stamped before a date, use the command:**
`exe iss_PurgeSD @BeginDate='June 15, 2011',
@ObsType='0,1,2,3,4,5,6,7,8,9,10,11,12,13'`
- **To purge incomplete and intrusion detection data time-stamped before a date, use the command:**
`exe iss_PurgeSD @BeginDate='June 15, 2011',
@ObsType='0,1'`
- **To only purge data that has been cleared from the Analysis view time-stamped before a date, use the command:**
`exe iss_PurgeObs @BeginDate='June 15, 2011',
@ObsType='0,1,2,3,4,5,6,7,8,9,10',
@PurgeFlag=1, @clearedonly=1'`
- **To monitor a data purge, use the command:**
`exec iss_GetPurgeStatus`



Observance data

Purge ObsType data from the SiteProtector Database. The following list includes the type and description of the data

<u>Type</u>	<u>Description</u>
0	Incomplete data
1	Intrusion detection
2	Vulnerability
3	Informational only
4	AntiVirus
5	Firewall
6	WebFilter
7	AntiSpam
8	Application compliance
9	Network anomaly detection
10	File integrity

Slide 14

Trademarks, copyrights, and disclaimers

IBM, the IBM logo, ibm.com, and Tivoli are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "[Copyright and trademark information](http://www.ibm.com/legal/copytrade.shtml)" at <http://www.ibm.com/legal/copytrade.shtml>

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.

© Copyright International Business Machines Corporation 2011. All rights reserved.