

## Purging database tables

---

Slide 1

Tivoli

IBM

### IBM Security SiteProtector System v2.0 SP8.1

Purging database tables



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

© 2011 IBM Corporation

Slide 2



### Objectives

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

- Configure the frequency that the SiteProtector Database purges database tables
- Modify data retention settings
- Purge data manually

Slide 3



### Purging data from the database

- The amount of data that the SiteProtector Database processes and stores impacts database performance
- To improve performance, only store data that is essential and necessary

**Note:** The database table purge job does not purge rules that are associated with incidents and exceptions

# Purging database tables

Slide 4

The screenshot shows the SiteProtector Agent View interface. The main window displays a list of components with columns for Model, Name, Health Status, Status, and Version. A callout box highlights the 'SiteProtector Database' component.

Model	Name	Health Status	Status	Version
Proventia Server for Linux	proventia_server_1	Warning	Offline	1.5 (XPU PAM - 29.080, BOE...)
SiteProtector Database	SP Database	Warning	Active	2.0 (SP 9.1:XPU 1.301)
Event Collector	EventCollector_SITEPROTECTOR	Healthy	Active	6.9 (SP 1.20)
SiteProtector Core	SP Core	Healthy	Active	2.0 (SP 8.1)
Deployment Manager	DeploymentManager	Healthy	Active	2.0 (SP 8.4)
Agent Manager	AgentManager_SITEPROTECTOR	Healthy	Active	6.9 (SP 10.172)
X-Press Update Server	UpdateServer	Warning	Active	1.0 (XPU 1.10)
SecurityFusion Module	SecurityFusionModule	Healthy	Active	2.1 (SP 1.7)
Proventia Server for Windows	Proventia Server	Healthy	Active	2.1.14.2565 (XPU 30.091)
GV 1000	myhost	Healthy	Offline	4.1 (XPU 39.190)
GX4004	godzilla	Offline	Offline	1.0
GX5108	mothra	Offline	Offline	1.0

**In the Agent view, select SiteProtector Database.**

This demonstration shows you how to automatically purge data from the tables in the SiteProtector Database.

12 rows with 0 selected. administrator Notifications ALERTCON 1™

# Purging database tables

Slide 5

The screenshot shows the SiteProtector interface with the 'Agent View - Default' window. A yellow callout box points to the 'New' button with the text 'Select Object'. The main window displays a table of agents and their components. The table has columns for Model, Asset, Agent Name, Health Status, Status, and Version. The 'SiteProtector Database' row is highlighted in blue.

Model	Asset	Agent Name	Health Status	Status	Version
Proventia Server for Linux	192.168.5.142	proventia_server_1	Warning	Offline	1.5 (XPU PAM - 29.080, BOE...)
SiteProtector Database	SITEPROTECTOR	SP Database	Warning	Active	2.0 (SP 9.1:XPU 1.301)
Event Collector	SITEPROTECTOR	EventCollector_SITEPROTECTOR	Healthy	Active	6.9 (SP 1.20)
SiteProtector Core	SITEPROTECTOR	SP Core	Healthy	Active	2.0 (SP 8.1)
Deployment Manager	SITEPROTECTOR	DeploymentManager	Healthy	Active	2.0 (SP 8.4)
Agent Manager	SITEPROTECTOR	AgentManager_SITEPROTECTOR	Healthy	Active	6.9 (SP 10.172)
X-Press Update Server	SITEPROTECTOR	UpdateServer	Warning	Active	1.0 (XPU 1.10)
SecurityFusion Module	SITEPROTECTOR	SecurityFusionModule	Healthy	Active	2.1 (SP 1.7)
Proventia Server for Wind...	SITEPROTECTOR	Proventia Server	Healthy	Active	2.1.14.2565 (XPU 30.091)
GV 1000	myhost	myhost	Healthy	Offline	4.1 (XPU 39.190)
GX4004	192.168.5.199	godzilla	Healthy	Offline	1.0
GX5108	192.168.5.200	mothra	Healthy	Offline	1.0

12 rows with 1 selected. administrator Notifications ALERTCON 1™

# Purging database tables

Slide 6

The screenshot shows the SiteProtector Agent View interface. The main window displays a table of agents and their components. A yellow callout bubble with the text "Select Properties." points to the "Properties" menu item in the left sidebar.

Asset	Agent Name	Health Status	Status	Version
proventia_server_1	proventia_server_1	Warning	Offline	1.5 (XPU PAM - 29.080, BOE...)
SITEPROTECTOR	SP Database	Warning	Active	2.0 (SP 9.1:XPU 1.301)
SITEPROTECTOR	EventCollector_SITEPROTECTOR	Healthy	Active	6.9 (SP 1.20)
SITEPROTECTOR	SP Core	Healthy	Active	2.0 (SP 8.1)
SITEPROTECTOR	DeploymentManager	Healthy	Active	2.0 (SP 8.4)
SITEPROTECTOR	AgentManager_SITEPROTECTOR	Healthy	Active	6.9 (SP 10.172)
SITEPROTECTOR	UpdateServer	Warning	Active	1.0 (XPU 1.10)
SITEPROTECTOR	SecurityFusionModule	Healthy	Active	2.1 (SP 1.7)
SITEPROTECTOR	Proventia Server	Healthy	Active	2.1.14.2565 (XPU 30.091)
myhost	myhost	Healthy	Offline	4.1 (XPU 39.190)
192.168.5.199	godzilla	Healthy	Offline	1.0
192.168.5.200	mothra	Healthy	Offline	1.0

12 rows with 1 selected. administrator Notifications ALERTCON 1™

# Purging database tables

Slide 7

The screenshot displays the SiteProtector application window. The title bar reads "SiteProtector" and the menu bar includes "Object", "Edit", "View", "Action", "Tools", and "Help". The status bar shows "Agent : 192.168.5.128 : IBM-ISS" and "Properties : 192.168.5.128 : SP Datab...".

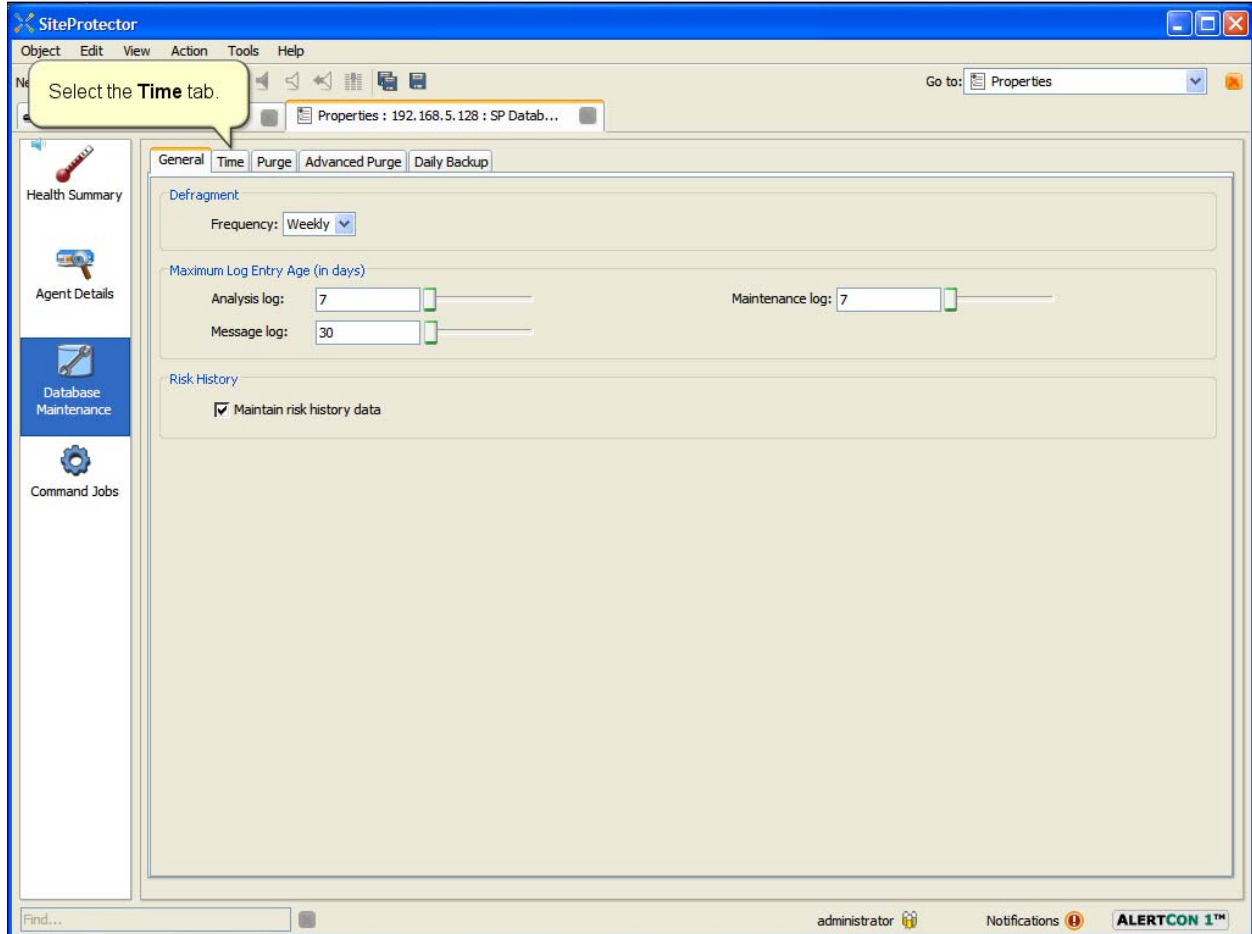
The main content area is divided into several sections:

- Health Summary:** A top row of indicators shows "DATABASE SIZE" (green checkmark), "Event Loading" (green checkmark), "Database Jobs" (green checkmark), "Performance" (yellow triangle), and "Agent Messages" (blue circle with 'i').
- Agent Details:** A section with a magnifying glass icon.
- Database Maintenance:** A section with a wrench icon. A yellow callout bubble points to this section with the text "Click Database Maintenance." Below this is a line graph showing "% Used" on the y-axis (0 to 80) and "Time" on the x-axis (4 PM, 8 PM, 12 AM, 4 AM, 8 AM, 12 PM). The graph shows a blue line that rises from 0 at 4 PM to approximately 10% at 12 AM, then remains flat. Horizontal lines indicate "Fail Level" at 80% and "Warning Level" at 70%.
- TempDB Database Size (MB):** A section with an information icon. It includes a line graph and a description: "Description: The size of the TempDB Database file in Megabytes. The SQL Server".

The bottom status bar shows "Find...", "administrator" with a user icon, "Notifications" with a red exclamation mark icon, and the "ALERTCON 1™" logo.

## Purging database tables

Slide 8





## Purging database tables

Slide 9

The screenshot displays the SiteProtector software interface. The main window is titled "SiteProtector" and has a menu bar with "Object", "Edit", "View", "Action", "Tools", and "Help". Below the menu bar is a toolbar with icons for "New", "Open", "Save", and "Print". The main content area is divided into several tabs: "General", "Time", "Purge", "Advanced Purge", and "Daily Backup". The "Purge" tab is selected, and its content is as follows:

The day and time specified here is the start time used by Defragment, Purge and Backup modules:

Database Maintenance Time

Eastern Standard Time  GMT

Weekly maintenance day: Saturday

Maintenance time of day: 20:00

On the left side of the interface, there is a sidebar with a "Health Summary" section and a "Maintenance" section containing a "Command Jobs" icon. At the bottom of the window, there is a status bar with a search field, the user name "administrator", a "Notifications" icon, and the "ALERTCON 1™" logo.

Three yellow callout boxes provide instructions:

- "Select the **Purge** tab."
- "Select either the **Eastern Standard Time** or **GMT** option."
- "Select the day of the week to purge the database."
- "Select the hour to purge the database."

## Purging database tables

Slide 10

The screenshot shows the SiteProtector interface with the Database Maintenance settings for purging database tables. The 'Purge' tab is selected, showing options for Emergency purge, Maximum Database Size, and Data Retention Settings. A callout box highlights the 'Purge Frequency' dropdown menu, which is currently set to 'Never'. Another callout box explains that the Express installation enables the database table purge job, while the Recommended installation disables it. The interface also includes a section for setting up notification rules for Database Purge and Size Status.

**Maximum Database Size**

- Emergency purge
- Database size threshold: 185 %
- Purge margin: 5 %

**Data Retention Settings**

Purge Frequency: **Never**

Maximum Item Age (in days)

Analysis summary events:		Cleared analysis summary events:	14
Analysis detail events:	90	Cleared analysis detail events:	14
Incidents:	90	Exceptions:	14
Audit:	999	Job history:	7
Metrics:	180	Unused assets:	30
Resolved tickets:	30	Mail data:	90

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

Open Tools menu and select Central Responses.  
Open Response Rules and select the Add button.  
Select Database Status Configuration from the drop down menu and select the rule parameters.

# Purging database tables

Slide 11

The screenshot displays the SiteProtector application window. The main content area is titled 'Purge' and contains several configuration sections:

- Maximum Database Size:** Includes an unchecked 'Emergency purge' checkbox, a 'Database size threshold' set to 85%, and a 'Purge margin' set to 5%.
- Data Retention Settings:** Features a 'Purge Frequency' dropdown menu with 'Never', 'Daily', and 'Weekly' options. A yellow callout box points to this menu with the text: "Select the appropriate frequency to purge the database tables. In this demonstration, **Daily** is selected."
- Sliders for various metrics:** Includes sliders for 'analysis summary events' (14), 'analysis detail events' (14), 'Incidents' (14), 'Job history' (7), 'Unused assets' (30), 'Mail data' (90), 'Audit' (999), 'Metrics' (180), and 'Resolved tickets' (30).

At the bottom of the window, there is a section titled 'To set up notification rules for Database Purge and Size Status:' with the following instructions:

- Open Tools menu and select Central Responses.
- Open Response Rules and select the Add button.
- Select Database Status Configuration from the drop down menu and select the rule parameters.

A blue callout box in the upper right corner of the settings area contains the text: "When you purge daily, the amount of data to be purged is smaller. As a result, the purge job finishes more quickly and there is less fragmentation."

## Purging database tables

Slide 12

The screenshot shows the SiteProtector Advanced Purge configuration window. The 'Advanced Purge' tab is selected, as indicated by a yellow callout bubble: "Select the **Advanced Purge** tab." The window is divided into several sections:

- Maximum Database Size:** Includes an unchecked "Emergency purge" checkbox, a "Database size threshold" of 85%, and a "Purge margin" of 5%.
- Data Retention Settings:** Shows "Purge Frequency" set to "Daily".
- Maximum Item Age (in days):** A table of settings for various database tables, with red boxes highlighting the "Analysis summary events" and "Analysis detail events" rows. A yellow callout bubble points to the sliders: "Use the slide bar or type the maximum number of days to retain data in the selected table."

Item	Value	Item	Value
Analysis summary events:	90	Cleared analysis summary events:	14
Analysis detail events:	30	Cleared analysis detail events:	14
Incidents:	90	Exceptions:	14
Audit:	999	Job history:	7
Metrics:	180	Unused assets:	30
Resolved tickets:	30	Mail data:	90

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

Open Tools menu and select Central Responses.  
Open Response Rules and select the Add button.  
Select Database Status Configuration from the drop down menu and select the rule parameters.

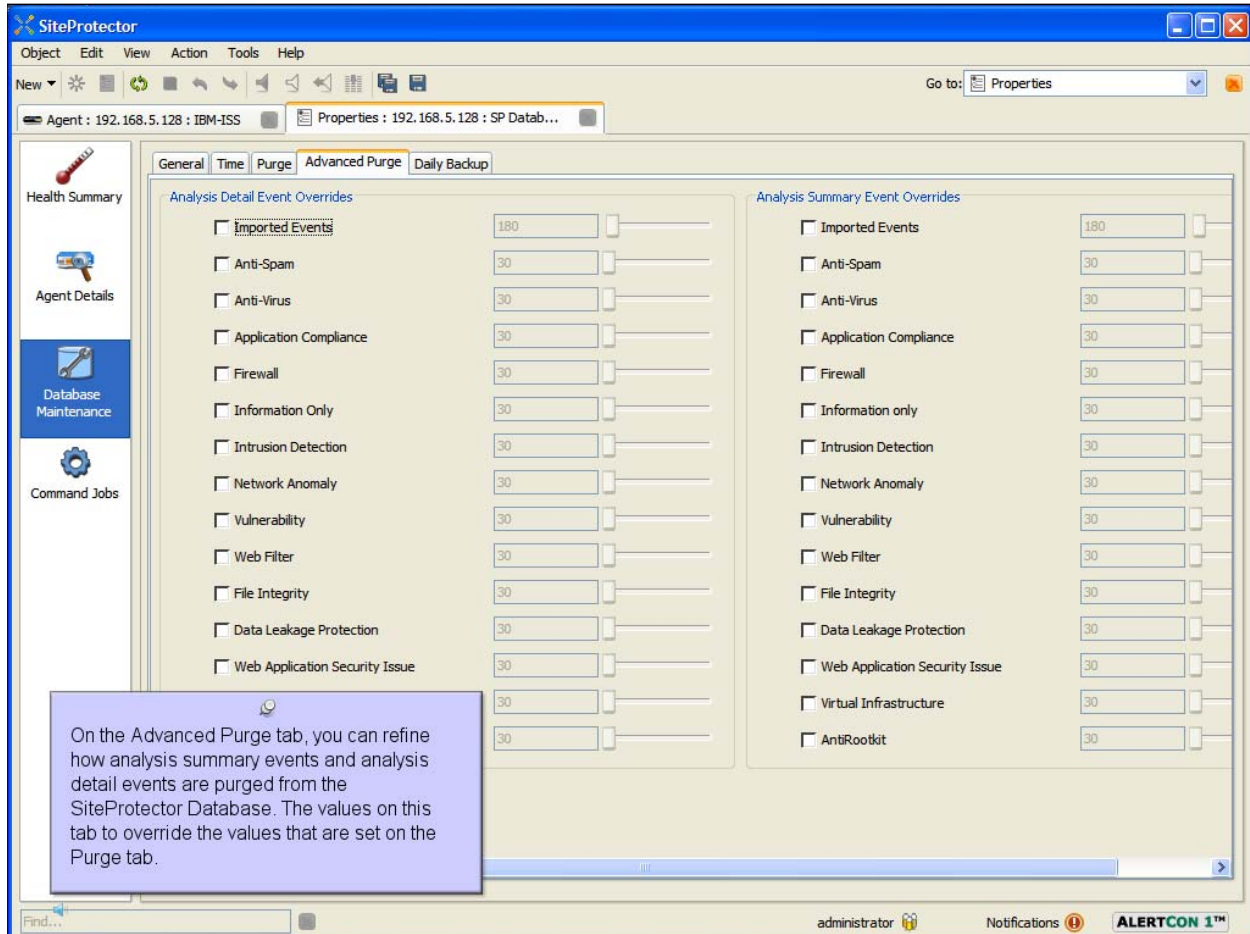
This job purges an item that is older than the user-defined age. Use the default Maximum Item Age settings for the various database tables. If you must change the default values:

- \* Keep **Analysis summary events** (observances) longer than **Cleared analysis summary events**.
- \* Keep **Analysis detail events** (agent data) longer than **Cleared analysis detail events**.

The bottom of the window shows a search bar, the user "administrator", a notifications icon, and the "ALERTCON 1™" logo.

## Purging database tables

Slide 13



The screenshot shows the SiteProtector interface with the 'Advanced Purge' tab selected. The window is titled 'SiteProtector' and has a menu bar with 'Object', 'Edit', 'View', 'Action', 'Tools', and 'Help'. Below the menu bar is a toolbar with various icons. The main area is divided into two columns: 'Analysis Detail Event Overrides' and 'Analysis Summary Event Overrides'. Each column contains a list of event types with checkboxes and numerical input fields. The 'Imported Events' checkbox is checked in both columns, and its value is set to 180. Other event types have their checkboxes unchecked and values set to 30. A callout box in the bottom left corner explains that these values override the default settings from the Purge tab.

Event Type	Analysis Detail Event Overrides	Analysis Summary Event Overrides
Imported Events	<input checked="" type="checkbox"/> 180	<input checked="" type="checkbox"/> 180
Anti-Spam	<input type="checkbox"/> 30	<input type="checkbox"/> 30
Anti-Virus	<input type="checkbox"/> 30	<input type="checkbox"/> 30
Application Compliance	<input type="checkbox"/> 30	<input type="checkbox"/> 30
Firewall	<input type="checkbox"/> 30	<input type="checkbox"/> 30
Information Only	<input type="checkbox"/> 30	<input type="checkbox"/> 30
Intrusion Detection	<input type="checkbox"/> 30	<input type="checkbox"/> 30
Network Anomaly	<input type="checkbox"/> 30	<input type="checkbox"/> 30
Vulnerability	<input type="checkbox"/> 30	<input type="checkbox"/> 30
Web Filter	<input type="checkbox"/> 30	<input type="checkbox"/> 30
File Integrity	<input type="checkbox"/> 30	<input type="checkbox"/> 30
Data Leakage Protection	<input type="checkbox"/> 30	<input type="checkbox"/> 30
Web Application Security Issue	<input type="checkbox"/> 30	<input type="checkbox"/> 30
Virtual Infrastructure		<input type="checkbox"/> 30
AntiRootkit		<input type="checkbox"/> 30

On the Advanced Purge tab, you can refine how analysis summary events and analysis detail events are purged from the SiteProtector Database. The values on this tab to override the values that are set on the Purge tab.

# Purging database tables

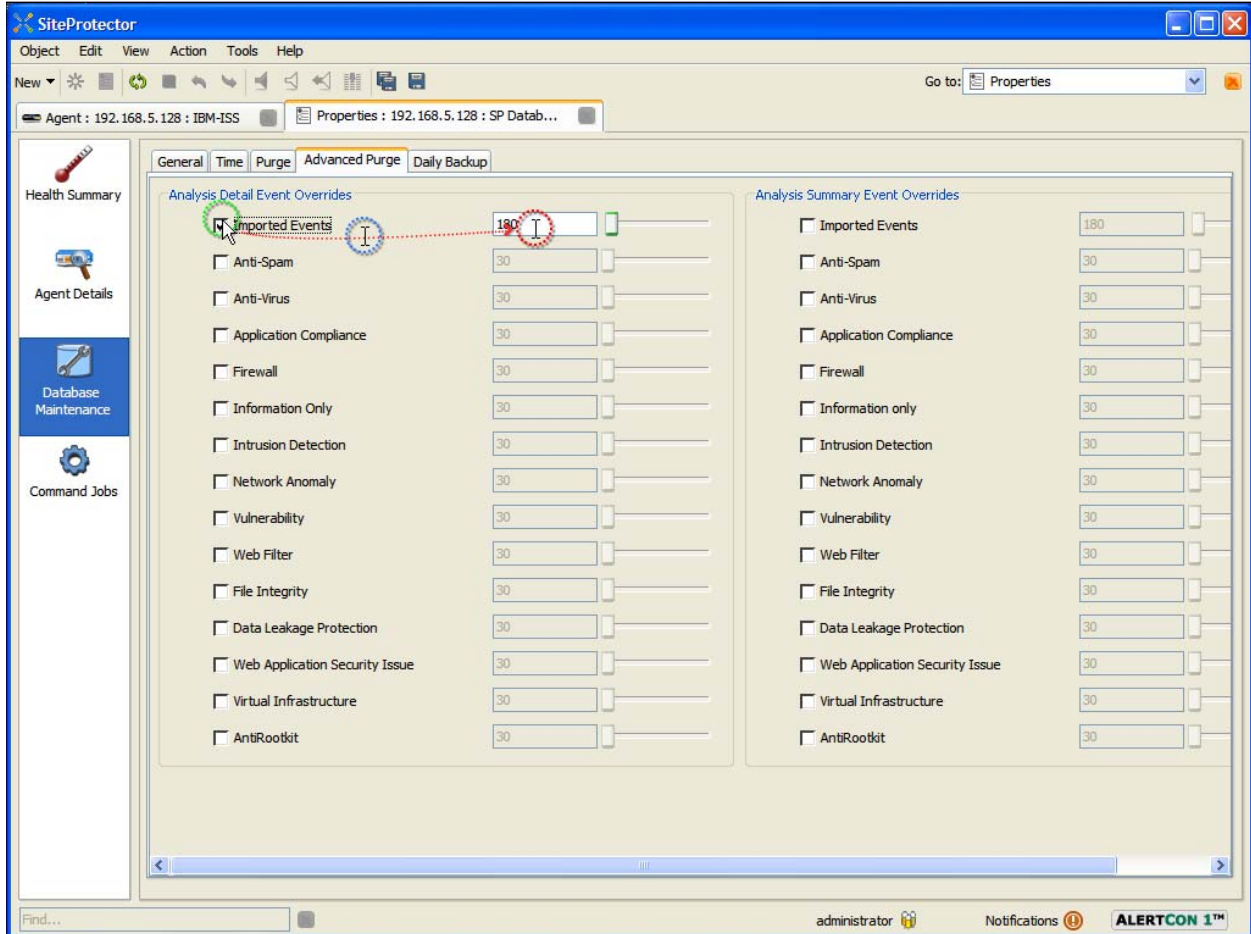
Slide 14

To refine the Analysis Detail Events included in the purge, activate the appropriate override option and then modify the number of days to retain the data.

Event Category	Event Type	Retention Period (Days)
Analysis Detail Event Overrides	<input checked="" type="checkbox"/> Imported Events	180
	<input type="checkbox"/> Anti-Spam	30
	<input type="checkbox"/> Anti-Virus	30
	<input type="checkbox"/> Application Compliance	30
	<input type="checkbox"/> Firewall	30
	<input type="checkbox"/> Information Only	30
	<input type="checkbox"/> Intrusion Detection	30
	<input type="checkbox"/> Network Anomaly	30
	<input type="checkbox"/> Vulnerability	30
	<input type="checkbox"/> Web Filter	30
	<input type="checkbox"/> File Integrity	30
	<input type="checkbox"/> Data Leakage Protection	30
	<input type="checkbox"/> Web Application Security Issue	30
	<input type="checkbox"/> Virtual Infrastructure	30
	<input type="checkbox"/> AntiRootkit	30
	Analysis Summary Event Overrides	<input type="checkbox"/> Imported Events
<input type="checkbox"/> Anti-Spam		30
<input type="checkbox"/> Anti-Virus		30
<input type="checkbox"/> Application Compliance		30
<input type="checkbox"/> Firewall		30
<input type="checkbox"/> Information only		30
<input type="checkbox"/> Intrusion Detection		30
<input type="checkbox"/> Network Anomaly		30
<input type="checkbox"/> Vulnerability		30
<input type="checkbox"/> Web Filter		30
<input type="checkbox"/> File Integrity		30
<input type="checkbox"/> Data Leakage Protection		30
<input type="checkbox"/> Web Application Security Issue		30
<input type="checkbox"/> Virtual Infrastructure		30
<input type="checkbox"/> AntiRootkit		30

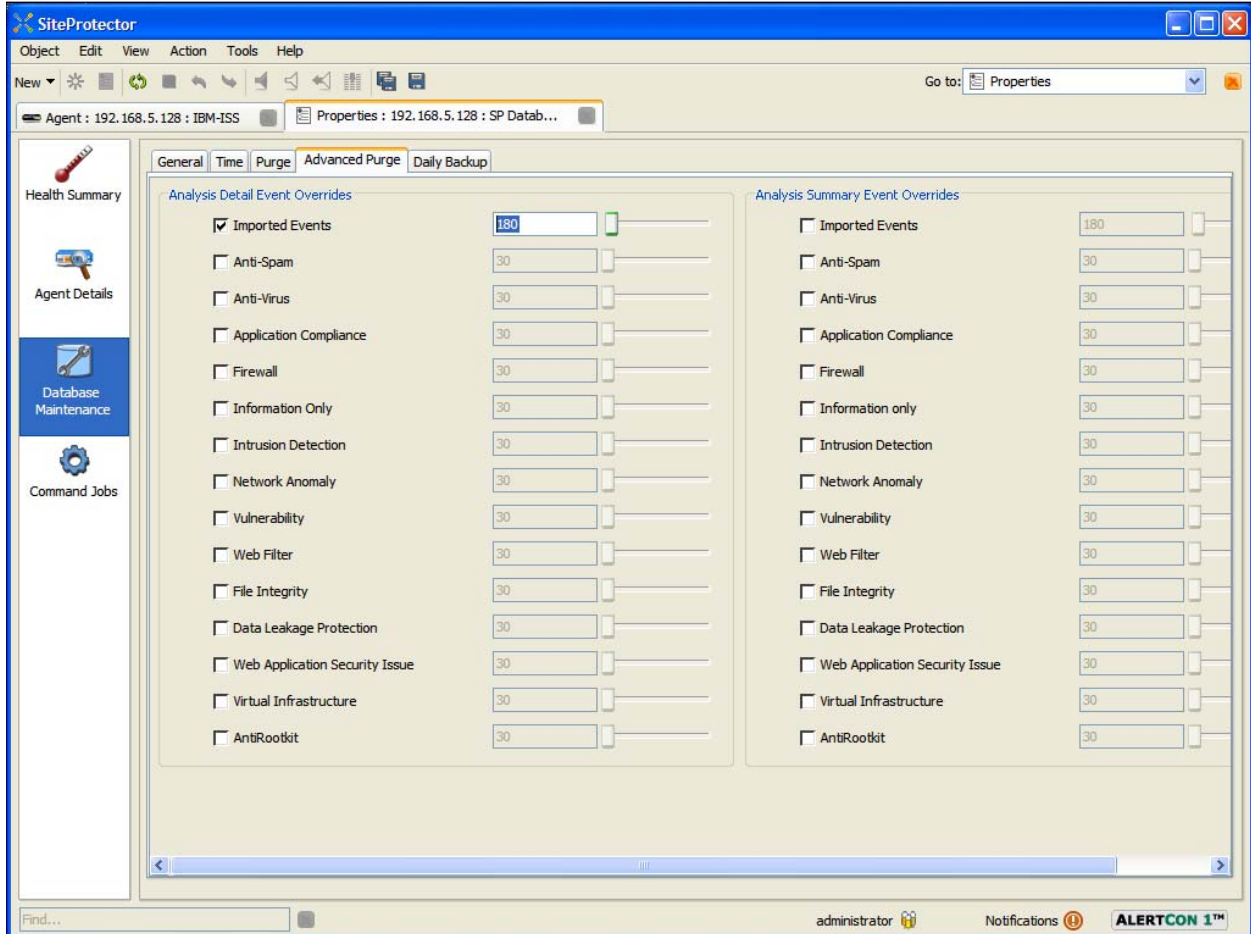
# Purging database tables

Slide 15



# Purging database tables

Slide 16





# Purging database tables

Slide 17

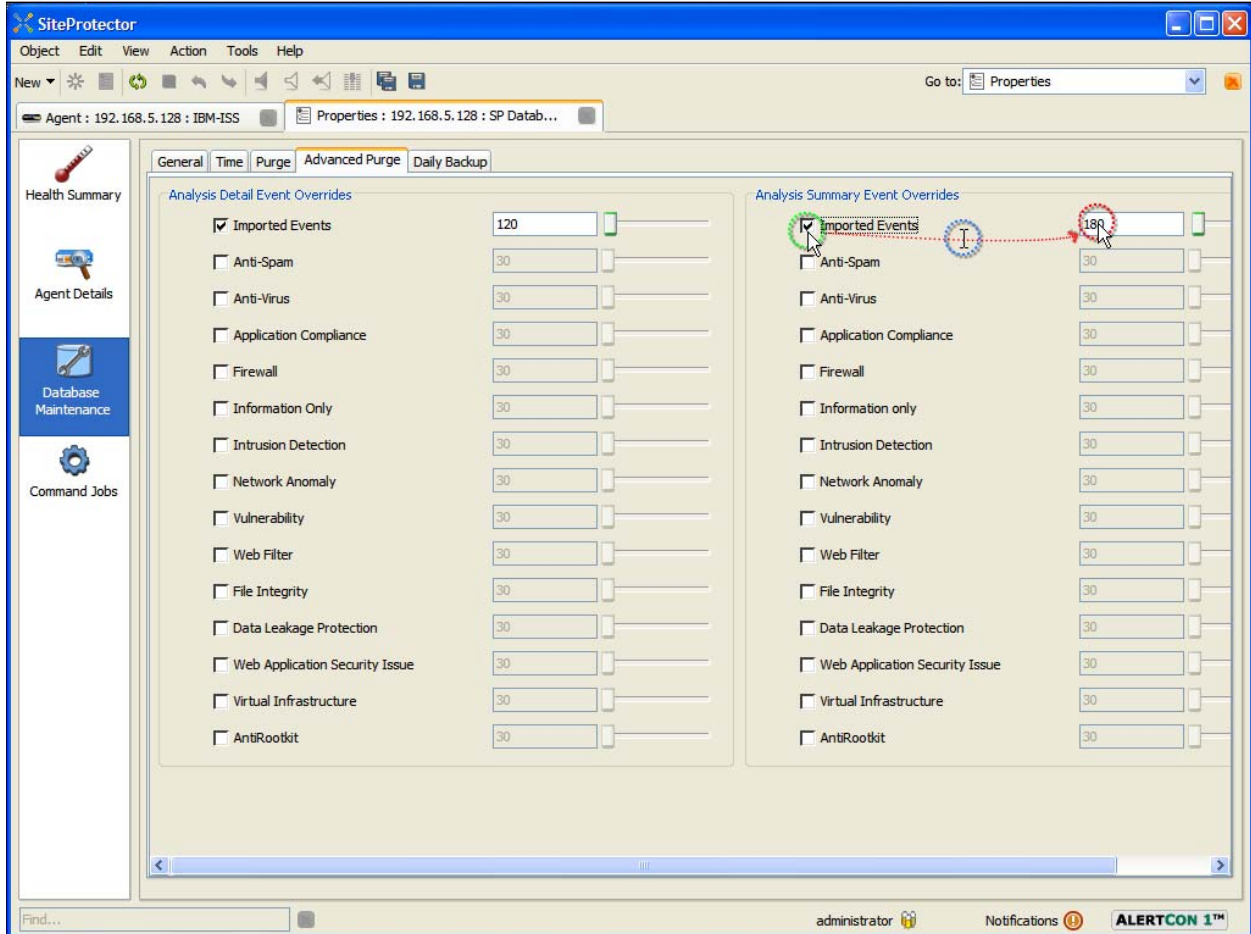
The screenshot shows the SiteProtector Advanced Purge configuration window. The 'Advanced Purge' tab is active, displaying two columns of event overrides. The left column is titled 'Analysis Detail Event Overrides' and the right column is 'Analysis Summary Event Overrides'. Both columns list various event categories with checkboxes and numeric input fields for retention days. A yellow callout box points to the 'Imported Events' checkbox in the 'Analysis Summary' column, which is checked. A red dashed arrow points from the '120' value in the 'Analysis Detail' column to the '180' value in the 'Analysis Summary' column. The 'Imported Events' checkbox in the 'Analysis Detail' column is also checked.

Event Category	Analysis Detail (Days)	Analysis Summary (Days)
<input checked="" type="checkbox"/> Imported Events	120	180
<input type="checkbox"/> Anti-Spam	30	30
<input type="checkbox"/> Anti-Virus	30	30
<input type="checkbox"/> Application Compliance	30	30
<input type="checkbox"/> Firewall	30	30
<input type="checkbox"/> Information Only	30	30
<input type="checkbox"/> Intrusion Detection	30	30
<input type="checkbox"/> Network Anomaly	30	30
<input type="checkbox"/> Vulnerability	30	30
<input type="checkbox"/> Web Filter	30	30
<input type="checkbox"/> File Integrity	30	30
<input type="checkbox"/> Data Leakage Protection	30	30
<input type="checkbox"/> Web Application Security Issue	30	30
<input type="checkbox"/> Virtual Infrastructure	30	30
<input type="checkbox"/> AntiRootkit	30	30

To refine the Analysis Summary Events included in the purge, activate the appropriate override option and then modify the number of days to retain the data.

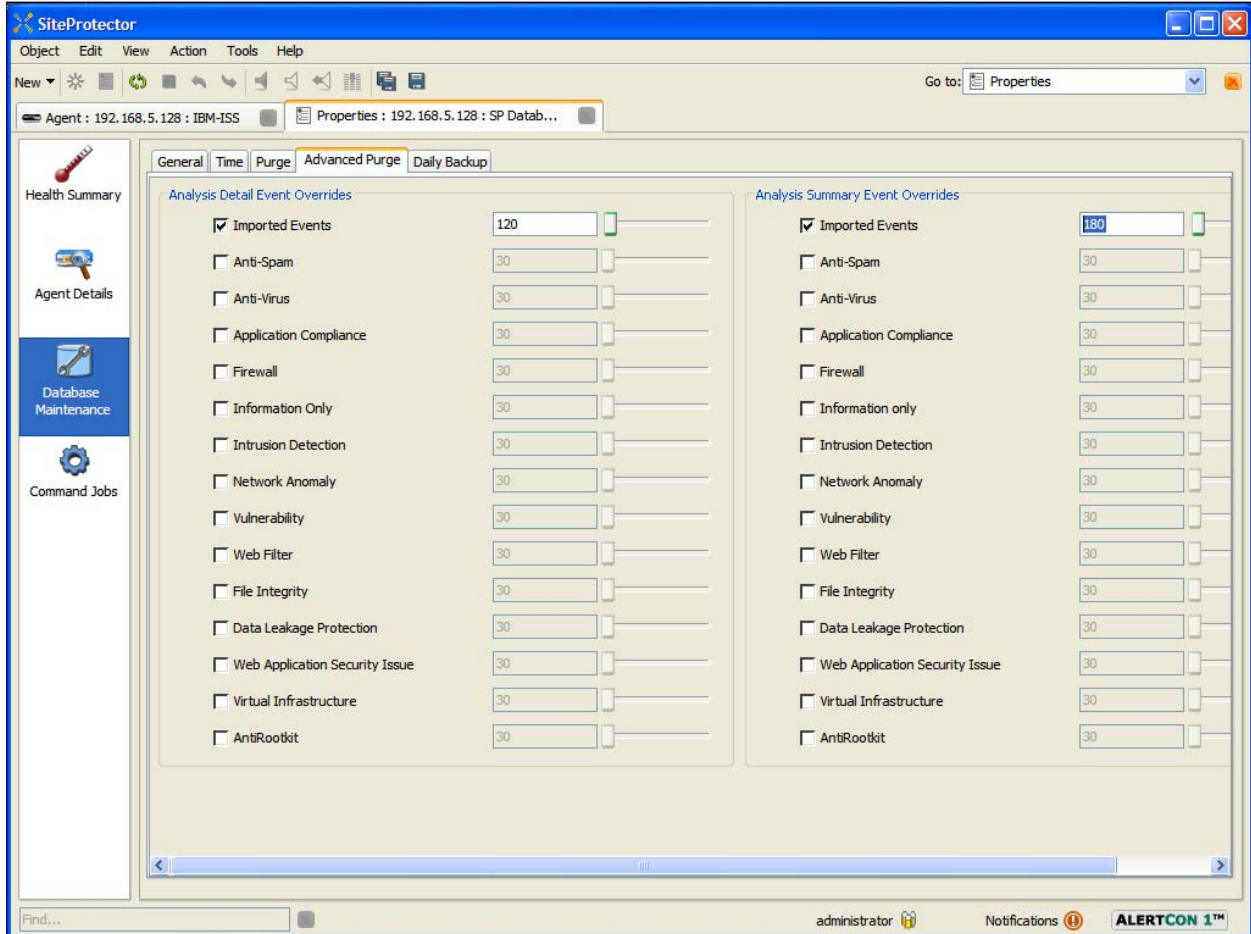
# Purging database tables

Slide 18



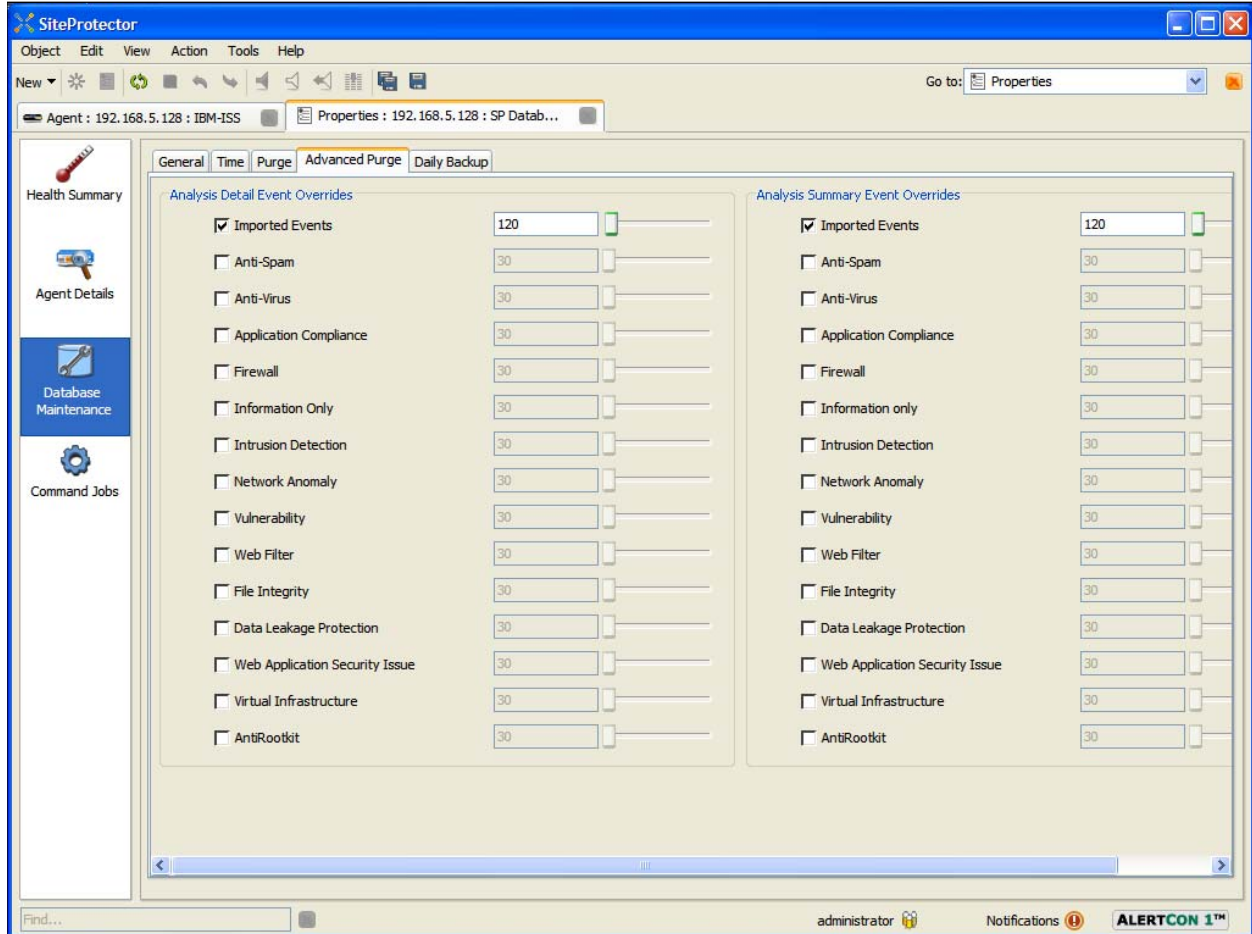
# Purging database tables

Slide 19



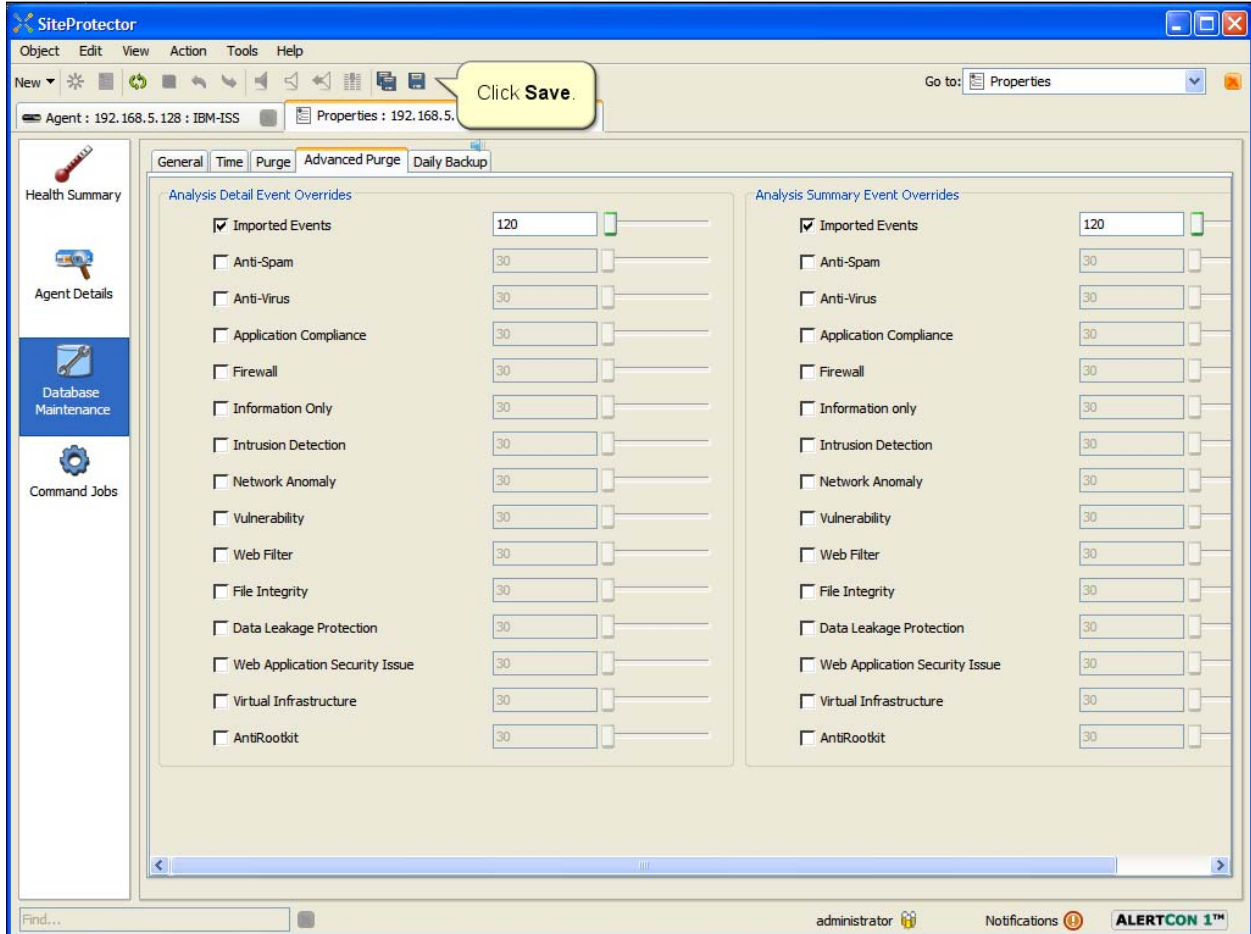
# Purging database tables

Slide 20



# Purging database tables

Slide 21



## Purging database tables

Slide 22



### Purging data

The most common procedures used to purge data are `iss_PurgeObs` and `iss_PurgeSD`

The screenshot shows the SiteProtector Event Analysis interface. The main window displays a table of events with columns for Severity and Event. A callout box on the left explains that `iss_PurgeObs` removes records from the Analysis Summary Events (Observances) tables, which correspond to the first level of event information. A callout box on the right explains that `iss_PurgeSD` removes records from the Analysis Detail Events (SensorData) tables, which correspond to the detailed information seen when viewing the Event Details. The interface also shows filters for Time, Tag Name, Source IP, and Target IP, and a 'Data last loaded' timestamp of 11:34 AM EDT.

Event Name	Severity	Event
Detected event	High	10
Detected attack (Se...	High	4
Detected event (Se...	High	3
H_IP_faxsurvey	Medium	3
No Evil	Medium	1
H_IP_faxsurvey	Low	5

**Note:** Run queries to purge data from either Microsoft SQL Management Studio or `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
```

Slide 24



### Observance data

Purge ObsType data (Analysis Summary Events) from the SiteProtector Database. The following list includes the type and description of the observance 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

© 2011 IBM Corporation



Slide 25



---

### Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, Netcool, 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.

© 2011 IBM Corporation