

ObserveIT Configuration Guide

Version 5.8



Copyright (c) 2015 ObserveIT Ltd.

Contents

Configuration Guide	7
Admin Dashboard	8
Walkthrough: Two Steps to Agent Health	10
Mini Admin Dashboard	13
Colored Severity Levels and Icons	14
Agents	15
Application Servers	24
Deployed Agent Versions and Recently Installed/Uninstalled Agents	26
System Services	28
Refreshing the Admin Dashboard	29
Console Users	30
Creating Local or Active Directory-based Console Users	31
Creating and Managing Local Console Users	32
Creating Active Directory Console Groups	34
Assigning Console User Permissions to View Recordings	34
Identification Services	37
Viewing Forced-Identification Users in the Web Console	38
Steps for Configuring ObserveIT Identification Services	38
Enabling Secondary Identification for Linux/Unix Policies	39
Configuring Forced-Identification Users	40
Configuring Active Directory Identification Targets	45
Configuring Active Directory Groups	46
Configuring Local ObserveIT Identification Users	49
Forced-Identification User Login	51
Preventing Windows Users from Bypassing the ObserveIT Identification Prompt	53
Servers	55
Viewing Servers	55
Filtering Servers	57
Renaming Servers	58
Unregistering Servers	60
Unlinking a Server Policy from Servers	61
Configuring Server Settings	62
Server Groups	63
Creating Server Groups	64
Modifying Members in Server Groups	64
Deleting Server Groups	66
Server Policies	67
Creating Server Policies	67
Modifying Server Policies	68
Deleting Server Policies	69
Linking Servers to Server Policies	69
Linking Server Groups to Server Policies	72
Configuring Server Policy Settings	74
Enabling Agent Recording	75
Enabling Identity Theft Detection	75

Enabling Agent API.....	76
Showing/Hiding the Agent Tray Icon.....	77
Restricting Recording to RDP Sessions.....	78
Enabling Hotkeys.....	79
Enabling Key Logging.....	80
Optimizing Screen Capture Data Size.....	81
Enabling Recording Notification	82
Recording in Color or Grayscale.....	84
Setting Session Timeout.....	86
Setting Keyboard Recording Frequency	88
Setting Continuous Recording	89
Data Recording Policy.....	91
Offline Recording Policy	93
Identification Policy.....	94
User Recording Policy	96
Application Recording Policy	98
Agent Logging and Debugging	100
Memory Management.....	101
Implementing Security	103
Renaming Application Servers	104
Enabling Image Security	105
Enabling Installation Security	109
Enabling Session Replay Privacy	111
Activity Alerts.....	114
Managing Activity Alerts	116
Viewing Alert Indications in the Web Console	130
Managing Alert Rules	134
Integrating Alerts in SIEM Products	166
System Events	167
Event Types	168
Viewing System Events.....	177
Filtering Events	179
Adding Comments to Events	181
Defining the Remediation Status of Events.....	181
Configuring Email Notification Settings for Events	182
Identity Theft Detection.....	185
Configuring Pairing Requests	187
Configuring Identity Theft Settings	189
Managing Messages	192
Creating Messages	193
Editing Messages	197
Viewing Messages	197
Deleting Messages	200
Disabling Messages	200
Acknowledging and Replying to Messages	201
Ticketing System Integration	202
Configuring Ticketing Policies.....	205
Configuring Ticketing Systems.....	209
SMTP Configuration	211

Monitoring Log Files	212
Monitoring ObserveIT Logs	212
Integrating Logs into SIEM Systems	215
LDAP Settings Configuration	218
Automatic LDAP Targets and Adding Domains	220
Adding Manual LDAP Targets	221
Deleting LDAP Targets	223
Changing the Default LDAP Email Field Name	223
Recording Metadata Information	224
Managing ObserveIT Storage	226
Viewing Database Information	227
Configuring Screen Capture Data Storage	229
Viewing Servers Database Information	233
Archiving Information	235
Scheduling an Archive Job	237
Managing the Archive Storage	244
Viewing the Archive Log	250
Best Practices for Storage of Large Scale Deployments	251
Backing Up the ObserveIT Databases	253
Saving Sessions	254
Auditing Access to the Web Console	256
Auditing Logins	257
Auditing Session Replays	258
Auditing Saved Sessions	259
Auditing Configuration Changes	260
Using Hotkeys	262
Sticky Notes	263
Context Sensitive Search	265
Managing Reports	266
Creating Custom Reports	266
Running Reports	271
Scheduling Reports	273
Editing Reports	275
Deleting Reports	277

Configuration Guide

After you have completed the installation process for ObserveIT, you will need to configure the application as required by your design criteria and operational needs. This configuration guide describes all the configuration tasks that should be typically performed by an ObserveIT Administrator. For ObserveIT usage guidelines, refer to the User Guide.

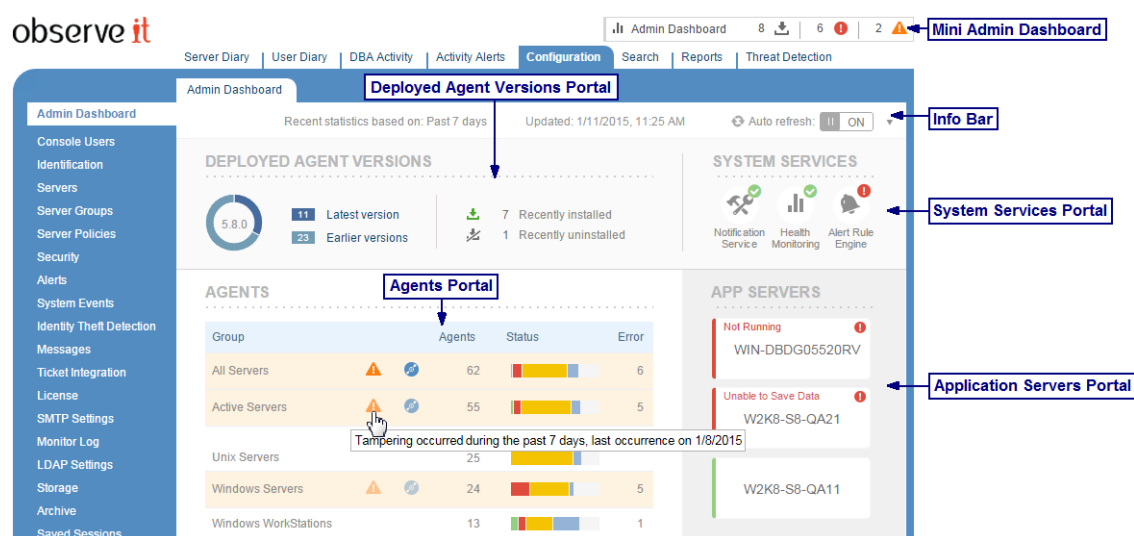
Most configuration tasks are performed via the **Configuration** tab in the Web Console. However, some additional configuration tasks need to be done using various system tools and operating system settings.

Admin Dashboard

The **Admin Dashboard** provides at-a-glance graphical summaries of the operational statuses of installed ObserveIT Agents and infrastructure (Application Servers, and so on), and easy navigation to drill down and perform root-cause analysis and corrective action. Operational statuses and system events are color coded in ObserveIT per severity (for example, "red" is the highest and may require immediate attention). This enables ObserveIT administrators to quickly identify events and statuses across the system, and respond accordingly. Note that every change on a local Agent triggers a system event, so that some events are "normal" (OK status) and do not require attention, such as when the Agent service is started.

A **mini Admin Dashboard** (located on the upper right of the Web Console) is viewable from every page in the Web Console. It provides a quick preview of the Agents' operational statuses and quick access to the full **Admin Dashboard**. For further details, see [Mini Admin Dashboard](#).

ObserveIT administrators can access the **Admin Dashboard** by navigating to the **Configuration > Admin Dashboard** tab of the Web Console, or by clicking on the **mini Admin Dashboard**.



The portals of the **Admin Dashboard** provide system health status information (and easy navigation to drill down to further details):

- **Agents:** displays a list of Agent groups, the number of Agents, colored-coded statuses, and the number of Agents with errors. When any of the Agents in a particular Agent group have been tampered with and/or have experienced data loss in the past 7 days, the relevant row is marked with the **Tampered With**  icon and/or **Data Loss**  icon, and each icon has a tooltip indicating the last date of occurrence. (The row marked by  is shaded orange as well, to easily identify which Agent group has been tampered with.) The shades of orange and blue on these icons vary per how recently the tampering or data loss has occurred (the darkest shades   indicate today, the medium shades   indicate within the past 2-3 days, and the lightest shades   indicate earlier in the week). (You can click the icons, the colored statuses, and the error numbers to drill down to further details.)
- **App Servers:** displays a list of Application Servers and their statuses. (You can click the Application Servers to drill down to further details.)
- **Deployed Agent Versions:** (at the top of the **Admin Dashboard**) displays the current Agent version, the number of Agents running the latest software version and earlier software versions, and the number of Agents recently installed/uninstalled in the past 7 days. (You can click the **Latest/Earlier version** links, and the **Recently installed/uninstalled** links and icons to drill down to further details.)
- **System Services:** (at the top of the **Admin Dashboard**) displays information about the Notification Service, Rule Engine Service, and Health Monitoring Service statuses, whether OK (marked by ) or with errors (marked by ). (You can click each service icon to drill down to further details.)

The info bar at the top of the **Admin Dashboard** provides the following information and functionality:

- Recent Statistics based on (on the left of the info bar): shows the time period (past 7 days) of the various statistics displayed in the **Admin Dashboard**.
- Updated (in the middle of the info bar): shows the last date and time the data on this page was updated (refreshed).
- **Manual/Auto refresh** (on the right of the info bar): displays a **Refresh**  button to manually refresh the page, and an **Auto refresh** button and options to automatically refresh the page (every 5, 10, or 15 minutes).

The easy-to-use **Admin Dashboard** provides a quick overview of system health—just two clicks away from understanding the specific Agent event that occurred due to tampering or other errors (see [Walkthrough: Two Steps to Agent Health](#)).

Workflow for ObserveIT Health Monitoring

- 1) Notification that health status has changed — via the **mini Admin Dashboard** and email notification (see [Mini Admin Dashboard](#) and [Configuring Email Notification Settings for Events](#)).
- 2) View the **Admin Dashboard** to analyze component statuses (see [Admin Dashboard](#)).
- 3) Pinpoint components experiencing events: Agent group, Application Server, or system service (see [Agents](#), [Application Servers](#), and [System Services](#)).
- 4) Focus on an ObserveIT component and investigate status details and causes.
- 5) Drill down to the Agent to assess its operational status details (see [Drilling Down to Agent Details](#)).

- 6) Investigate Agent system events to understand the root cause (see [Investigating System Events](#)).
- 7) Integrate system events into the organization's existing SIEM system.

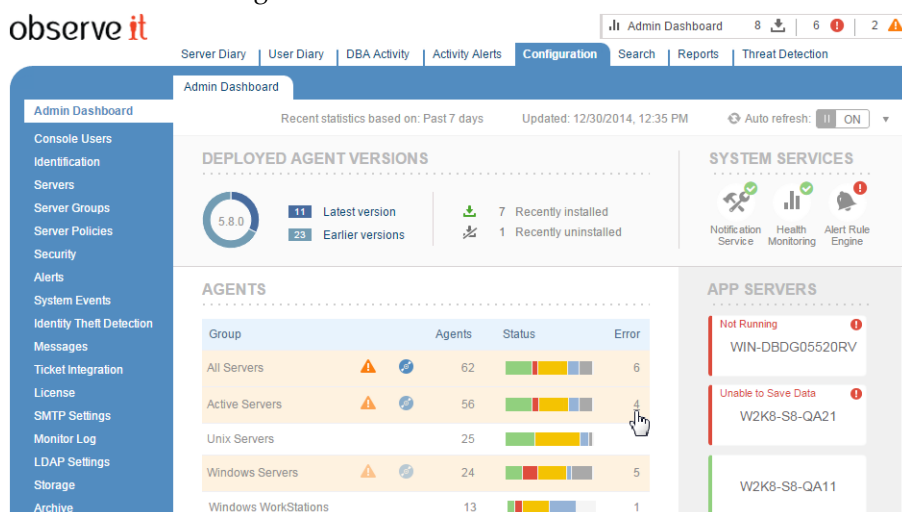
Walkthrough: Two Steps to Agent Health

This topic describes how to assess/restore Agent health in "two steps" using the **Admin Dashboard**.

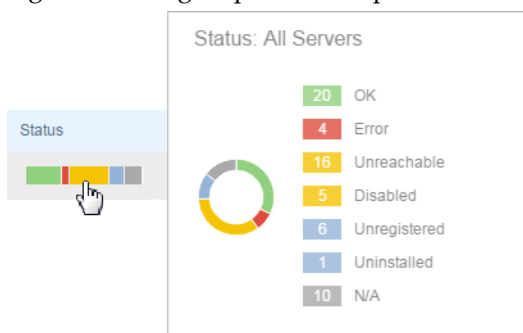
The **mini Admin Dashboard** provides immediate indication of Agent health. When you notice errors or problems, you can click on the **mini Admin Dashboard** to jump right away to the full **Admin Dashboard** to examine the details.

To assess/restore Agent health using the Admin Dashboard

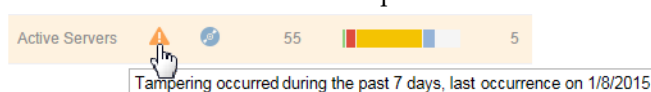
- 1) Go to the **Agents** portal of the **Admin Dashboard** to view the Agent group with the error status and the number of Agents with errors.



- 2) Hover the mouse over the colored status bar to view popup details about the statuses of the Agents in this group. For example:



- 3) When any of the Agents in the group have been tampered with or incurred data loss in the past 7 days, place the mouse over the **Tampered With** icon or **Data Loss** icon to view the date of the last occurrence. For example:



- 4) Click the **Error** number to display the **Servers** list where you can view expanded details of the Agent group member with errors.

The **Status Details** field displays "Tampered With". The colored severity bars indicate the event severity level (for example, Red=High).

Server Name	Server Policy	Version	Status	Installation	Last Activity
W2K8-2	Default Windows-based Po...	5.8.0.0	Error	12/4/2014	12/4/2014
Status Details Tampered With OS Type Windows OS Version Windows Server 2008 R2					

- 5) Click the **Error** link (or the **System Events** link) in the **Servers** list to view the event in the **System Events** list where you can view expanded details, including **Additional Info**.

10:35 AM 1210	Tampering	Agent installation files were tampered with	W12-S12-D02		
Severity	High	Agent installation files were tampered with			
Component	Agent				
Source	Agent				
Event Description	The ObserveIT Agent service has reported that installation files were tampered with.				
Email Sent	No				
Additional Info	Total files that were tampered with: File= C:\Program Files\ObserveIT\ObserveITAgent\bin\rcdcl.exe has been missing				
Remediation Status	New				
Comment	Add Comment				

- 6) Assess the problem and perform the required corrective action. Go to the directory in which the files are stored (shown in **Additional Info**) and verify what happened, see if the file is missing or has been changed. If the file is missing, it is recommended to reinstall the Agent with the latest software version used (or copy the file from another location). If the file has been modified, then correct it as needed.
- 7) When you are finished resolving the event, the **Admin Dashboard** displays the Agent group's status as "OK" (green). (The **mini Admin Dashboard** is also "error-free".)

observe it

Admin Dashboard 2

Server Diary | User Diary | DBA Activity | Activity Alerts | Configuration | Search | Reports | Threat Detection

Admin Dashboard

Recent statistics based on: Past 7 days Updated: 1/6/2015, 10:38 PM Auto refresh: OFF

DEPLOYED AGENT VERSIONS

5.8.0 2 Latest version

2 Recently installed
0 Recently uninstalled

SYSTEM SERVICES

Notification Service Health Monitoring Alert Rule Engine

AGENTS

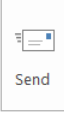
Group	Agents	Status	Error
Windows Servers	1	OK	
Unix Servers	1	OK	

APP SERVERS

W2K8-S8-QA11

Note: The **Tampered With** icon stays on the **Admin Dashboard** for up to one week after the tampering event occurred (as a reminder that tampering had occurred on this Agent group within the last week). The row remains shaded orange as well, to easily identify which Agent group has been tampered with.

An additional way to handle ObserveIT health monitoring is by receiving digest summaries of system events via email notifications.

Send

To...

Cc...

Bcc...

Subject

System Event Summary

High-severity Events

- 1296 [Unrecorded Agent sessions](#)
- 767 [Agent service stopped](#)
- 70 [Agent service was terminated](#)
- 9 [Agent installation failed](#)

Medium-severity Events

- 530 [Agent registration was successful](#)

System Event Details

10 of 3793 shown here | [view all](#)

[High-severity Events](#) (10 of 2192 shown here)

Agent service stopped (Event ID: 1)

Received Time: Monday, 10/6/2014 3:22 PM

Severity: High

Event Code: 1202

Event Name: Agent Service has stopped

Event Description: The ObserveIT Agent Service has reported that it has stopped.

Server: OIT-LILI

Component: Agent

Source: Agent

Remediation: New

Status:

[View Details](#)

For further details about Agent statuses, system events, and event email notifications, see [Assessing Agent Statuses and Details](#), [Investigating System Events](#), and [Configuring Email Notification Settings for Events](#).

Mini Admin Dashboard

ObserveIT administrators can view the **mini Admin Dashboard** (which is located on the upper right of the Web Console) from every page in the Web Console. Its colored icons indicate at-a-glance the ObserveIT Agents' operational statuses, thereby providing a quick preview to the system health. ObserveIT administrators can quickly access the full **Admin Dashboard** by clicking on the **mini Admin Dashboard**. This enables the administrators to drill down quickly to further details to identify the root cause of a problem and respond accordingly.



The colored icons on the **mini Admin Dashboard** indicate data from the past 7 days, including when relevant, the number of:

-  Installed/uninstalled Agents (in the above example there are 6)
-  Agents with errors (in the above example there are 2)
-  Agents that have been tampered with in the past 7 days (in the above example there is 1)

For further information about the icons and colored severity levels, see [Colored Severity Levels and Icons](#).

Colored Severity Levels and Icons

In ObserveIT, system events and operational statuses are colored per severity/status to enable administrators to quickly identify these and respond accordingly.

The following color-coded severity levels/operational statuses appear in the ObserveIT Web Console:

Color	Severity Level/ Status	Operational Status
Green 	Normal/Active	OK
Red 	High	Error
Orange 	Medium	Unreachable/Disabled
Blue 	Low/Administrative	Unregistered/Uninstalled
Gray 	N/A	Not Available (relevant for older Agent versions lower than 5.8, which have unknown or unavailable statuses)

The following icons appear in the **Admin Dashboard** (and throughout the ObserveIT Web Console):

Icon	Name	Description
	Error	Agents that have errors.
	Tampered With	Agents that have been tampered with. (The row in which this icon appears in the Agents portal is shaded orange as well.) Note that the shade of orange on this icon varies per how recently the tampering has occurred:  Tampering occurred today (darkest orange)  Tampering occurred within that past 2-3 days (medium orange)  Tampering occurred earlier in the week (lightest orange)
	Data Loss	Agents which have incurred data loss. Note that the shade of blue on this icon varies per how recently the data loss has occurred:  Data loss occurred today (darkest blue)  Data loss occurred within that past 2-3 days (medium blue)  Data loss occurred earlier in the week (lightest blue)
	Installed	Agents that have been installed.
	Uninstalled	Agents that have been uninstalled.
	Installed/Uninstalled	(Relevant only for the mini Admin Dashboard) Agents that have been installed and uninstalled.

Agents

In the **Agents** portal of the **Admin Dashboard**, you can view the statuses of Agent groups. This enables you to easily identify problematic Agents in the system, whether any have incurred tampering or data loss, for example. From the **Agents** portal, you can drill down to examine further details about the Agents, including operational statuses and system events, in order to identify the causes and respond accordingly.

Each row in the **Agents** list represents an Agent group and displays the name of the group and number of Agents in the group, as well as status and error information.

To view Agent status

- 1) In the **Agents** portal, view a list of Agent groups, the number of Agents in each group, colored-coded statuses ("red" when with errors, "orange" when unreachable/disabled, "green" when OK, and so on), and the number of Agents with errors.
- 2) When any of the Agents in a particular Agent group have been tampered with and/or have experienced data loss in the past 7 days, the relevant row is marked with the **Tampered With**  icon and/or **Data Loss**  icon. (When tampering has occurred, the relevant Agent group row is shaded orange as well, for easy identification.)

Place the mouse over the relevant icon  or  to view a tooltip indicating the date of the last occurrence of tampering or data loss. For example:

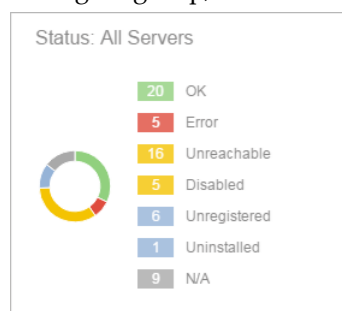
AGENTS

Group		Agents	Status	Error
All Servers	 	62		6
Active Servers	 	55		5
Unix Servers		25		
Windows Servers	 	24		5
Windows WorkStations		13		1

Tooltip for Active Servers: Tampering occurred during the past 7 days, last occurrence on 1/8/2015

The shades of orange and blue on these icons vary per how recently the tampering or data loss has occurred. (The darkest shades   indicate today, the medium shades   indicate within the past 2-3 days, and the lightest shades   indicate earlier in the week.)

- 3) Click the Agent's colored **Status** bar to display details in a popup window, including the name of the Agent group, the number and color-coded statuses of the Agent group members. For example:



For explanations of the icons and colored severity levels of system events and operational statuses, see [Colored Severity Levels and Icons](#).

Other tasks you can perform from the **Agents** portal include:

- [Drilling Down to Agent Details](#)
- [Assessing Agent Statuses and Details](#)
- [Investigating System Events](#)
- [Adding Agent Groups](#)

Drilling Down to Agent Details

From the **Agents** portal, you can drill down to the **Servers** list to examine further details about the Agent operational statuses in order to identify the causes and respond accordingly.

To drill down to Agent group members by group name

- In the **Agents** portal, click an Agent group name.

The **Servers** list opens, displaying the Agent group's member and related details. You can expand the Agent group member to view more details, including status details (when not "OK"), OS type, and OS version.

As shown in the following figure, for example, the Unix server/version Ubuntu 1204 has an "Error" status (colored "red" on the severity bars) and has been "Tampered With" (as shown in **Status Details**).

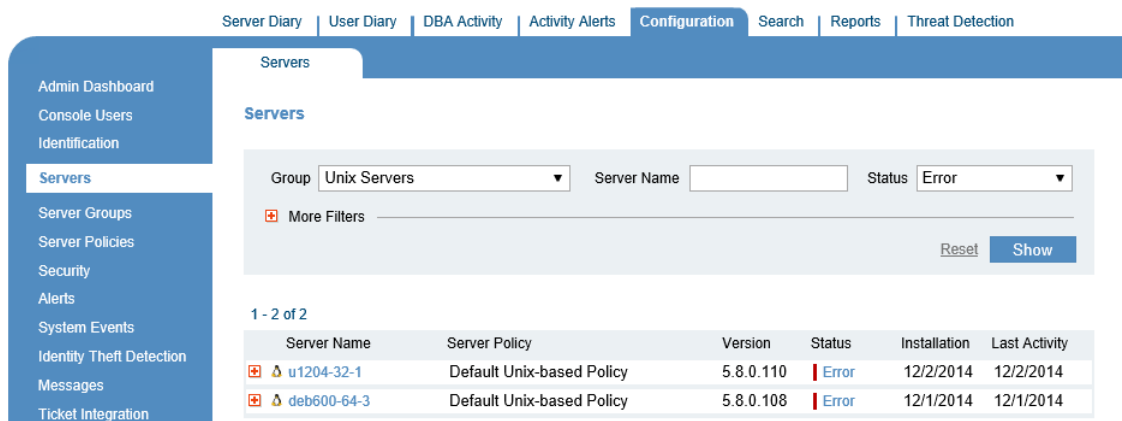
Server Name	Server Policy	Version	Status	Installation	Last Activity
  u1204-32-1	 Default Unix-based Policy	5.8.0.110	 Error	12/2/2014	12/2/2014
Status Details Tampered With OS Type Unix OS Version Ubuntu 1204					
				Unregister	System Events

You can click the **System Events** link (or the **Status** link) to drill down to the system event details (see [Investigating System Events](#)).

To drill down to examine Agents with errors

- In the **Agents** portal, click the **Error** number next to the relevant Agent group.

The **Servers** list opens, filtered to display only the particular Agent group members with "Error" status.



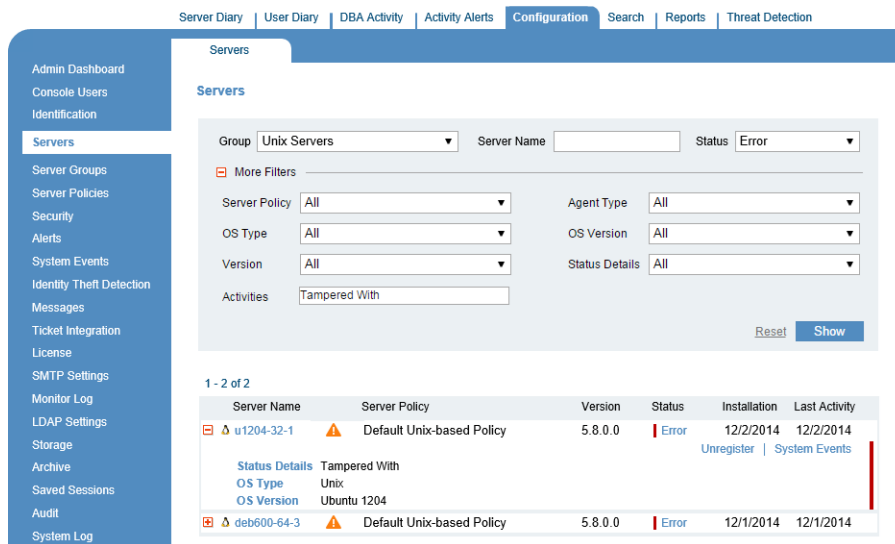
The screenshot shows the ObserveIT Agents portal interface. The top navigation bar includes links for Server Diary, User Diary, DBA Activity, Activity Alerts, Configuration (selected), Search, Reports, and Threat Detection. The left sidebar contains a menu with options: Admin Dashboard, Console Users, Identification, Servers (selected), Server Groups, Server Policies, Security, Alerts, System Events, Identity Theft Detection, Messages, and Ticket Integration. The main content area is titled 'Servers' and displays a filter section with 'Group' set to 'Unix Servers', 'Server Name' as an empty text box, and 'Status' set to 'Error'. Below the filters is a 'More Filters' link and 'Reset' and 'Show' buttons. The table below shows 2 results (1 - 2 of 2):

Server Name	Server Policy	Version	Status	Installation	Last Activity
  u1204-32-1	Default Unix-based Policy	5.8.0.110	 Error	12/2/2014	12/2/2014
  deb600-64-3	Default Unix-based Policy	5.8.0.108	 Error	12/1/2014	12/1/2014

To drill down to examine Agents that have been tampered with

- In the **Agents** portal, click the **Tampered With**  icon next to the relevant Agent group. The **Servers** list opens, filtered to display the Agent group members that have been "tampered with" in the last week. Each row displays the "tampered with" group member marked by the  icon.

In the expanded details of the Agent group member, the **Status Details** field displays "Tampered With". The colored severity bars indicate the event severity level (for example, Red=High).



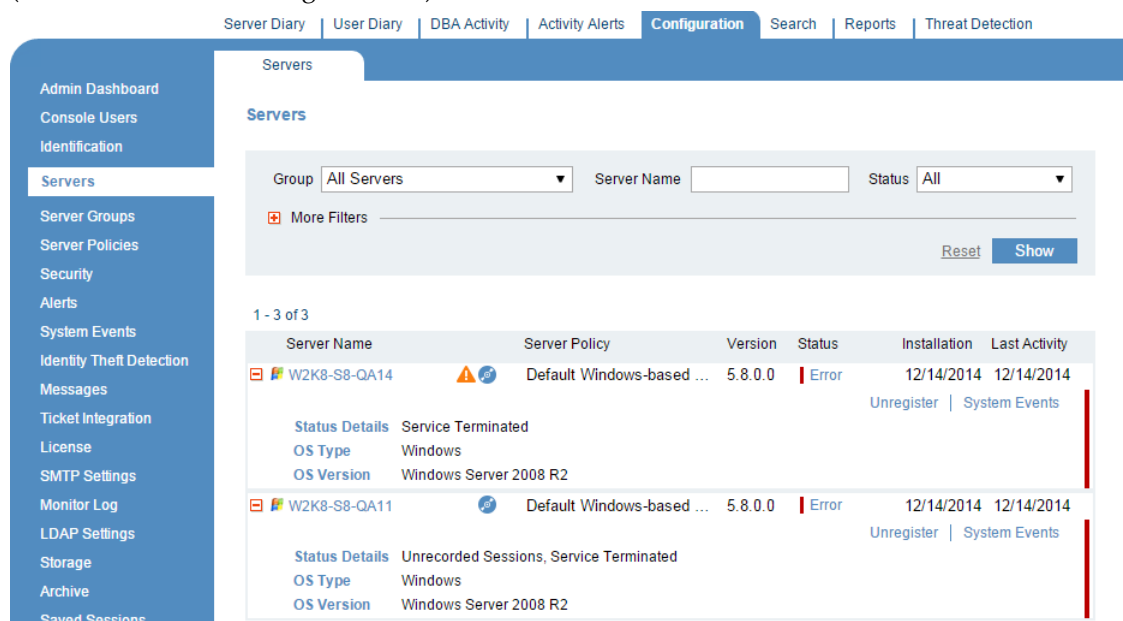
The screenshot shows the 'Servers' page in the Admin Dashboard. The left sidebar contains navigation links: Admin Dashboard, Console Users, Identification, Servers, Server Groups, Server Policies, Security, Alerts, System Events, Identity Theft Detection, Messages, Ticket Integration, License, SMTP Settings, Monitor Log, LDAP Settings, Storage, Archive, Saved Sessions, Audit, and System Log. The 'Servers' section is active, showing a list of servers. The top navigation bar includes links for Server Diary, User Diary, DBA Activity, Activity Alerts, Configuration, Search, Reports, and Threat Detection. The 'Servers' section has a filter bar with the following settings: Group: Unix Servers, Server Name: (empty), Status: Error, More Filters: Server Policy: All, Agent Type: All, OS Type: All, OS Version: All, Version: All, Status Details: All, Activities: Tampered With. Below the filter bar, there is a table with 2 rows of server data. The first row is for server 'u1204-32-1' with status 'Error' and last activity '12/2/2014'. The second row is for server 'deb600-64-3' with status 'Error' and last activity '12/1/2014'. The table has columns for Server Name, Server Policy, Version, Status, Installation, and Last Activity. The first row also has a 'Status Details' section showing 'Tampered With' and 'OS Type: Unix, OS Version: Ubuntu 1204'.

Server Name	Server Policy	Version	Status	Installation	Last Activity
u1204-32-1	Default Unix-based Policy	5.8.0.0	Error	12/2/2014	12/2/2014
deb600-64-3	Default Unix-based Policy	5.8.0.0	Error	12/1/2014	12/1/2014

To drill down to examine Agents with data loss

- In the **Agents** portal, click the **Data Loss**  icon next to the relevant Agent group. The **Servers** list opens, filtered to display the Agent group members that have incurred data loss in the last week. Each row displays the group member that incurred data loss marked by the  icon.

In the expanded details of the Agent group member, the **Status Details** field displays "Data Loss". The colored severity bars indicate the event severity level (for example, Red=High, if the data loss occurred while the Agent was running). If the data loss occurred while the Agent was offline (due to a threshold error (when the limit in MB was exceeded) or lack of disk space), the status is OK (the status does not change to error).



For explanations of the icons and colored severity levels of system events and operational statuses, see [Colored Severity Levels and Icons](#).

For descriptions of the Agent statuses and details, see [Assessing Agent Statuses and Details](#).

Assessing Agent Statuses and Details

The following table describes the ObserveIT Agent statuses and status details that appear through the Web Console (in the **Admin Dashboard**, in the **Servers** list, in the **System Events** list). To identify the causes, go to the [System Event](#) list and resolve it.

Agent Status	Status Details	Possible Reasons/Triggers
OK	N/A	The Agent is Active, functioning normally. The Agent Service is up and running. The Agent machine and service are accessible.
Error	Service Stopped	The Agent Service has stopped.
	Service Killed/Terminated	The Agent Service was killed by a command or was terminated (due to system causes), however, the machine is responsive.
	Tampered With	- Installation files were tampered with (missing files, changed files) - Offline data files were tampered with - Interception configuration/Agent Registry keys were tampered with

	Unrecorded Sessions	There are unrecorded Agent sessions. This occurs when a user ends the Agent process (or disables interception in Unix). (There are currently x missing sessions out of y sessions.)
	Interception Off	The Agent interception is off. The Unix Agent internal Watchdog "obitd" service failed to start the ObserveIT logger after a problem was detected, and recording was disabled. (When interception is marked as off, missing sessions are not shown.)
	Data Loss	Recorded data was lost by the Agent (while the Agent was running). - Online data loss: Data is not transmitted to the server. - Offline data loss: Data files were tampered with while the Agent was offline, and the threshold limit (in MB) was exceeded or there was a lack of disk space, the status is OK (the status does not change to error).
Unreachable	Communication Error	The machine is pingable, but does not respond. The machine is disconnected from the network (for example, when it is in hibernate mode, or has been shut down).
	Unknown Reason	The Agent machine is not pingable. It is not responsive and does not communicate with the Application Server. However, the system did not detect that the Agent Service was stopped or killed (via commands).
Disabled	N/A	The recording mode was disabled in the Server Policy.
Uninstalled	N/A	The Agent was uninstalled.
Unregistered	N/A	The Agent is disconnected from the licensing (unregistered/blocked from accessing the system).

Investigating System Events

From the **Servers** list, you can navigate to the **System Events** list to examine the system events that occurred on Agent group members to understand the root causes and what corrective actions to perform.

To drill down to investigate system events

- 1) In the **Servers** list, in the expanded details of the relevant Agent group member with error status, click the **System Events** link (or the **Status** link).

Server Name	Server Policy	Version	Status	Installation	Last Activity
W2K3-S8-QA06	Default Windows-based ...	5.8.0.0	Error	12/14/2014	12/15/2014

[Status Details](#) Tampered With
[OS Type](#) Windows
[OS Version](#) Windows Server 2003

[Unregister](#) | [System Events](#)

The **System Events** page opens, displaying all the related system events that occurred on the Agent group member. (The most recent event appears at the top of the list.)

System Events

Severity: All Server: All

More Filters:

Category: All Event Code: All

Component: All Source: All

Login: All Remediation Status: All

Client: All Email Sent: All

Event ID: Status Details: All

Comment:

Period: ☒ During last 1 Months ☐ Between 12/30/2014 and 01/07/2015

[Reset](#) [Show](#)

21 - 40 of 45 1 2 3 << First < Prev Next > Last >>

Received	Code	Category	Name	Server
1/6/2015				
12:46 PM	1210	Tampering	Agent installation files were tampered with	W12-S12-D02
12:45 PM	1610	Installation	Uninstallation of Agent without a password wa...	W12-S12-D02
12:45 PM	1611	Installation	Agent was unregistered	W12-S12-D02
12:45 PM	1202	Functionality	Agent service has stopped	W12-S12-D02
12:44 PM	1304	Functionality	Application Server is running	W12-S12-D02
12:44 PM	1323	Functionality	Rule Engine Service is OK	W12-S12-D02
12:44 PM	1329	Functionality	Rule Engine Service has started	W12-S12-D02
1/5/2015				
11:06 AM	1301	Functionality	Application Server is not working properly	W12-S12-D02
11:06 AM	1330	Functionality	Rule Engine Service has stopped	W12-S12-D02
10:37 AM	1218	Tampering	Agent offline data files were tampered with	W12-S12-D02
10:35 AM	1602	Installation	Agent Registration was successful	W12-S12-D02
10:35 AM	1304	Functionality	Application Server is running	W12-S12-D02
10:32 AM	1301	Functionality	Application Server is not working properly	W12-S12-D02
1/4/2015				
5:46 PM	1240	Recording	Agent is now recording active sessions	W2K8-S8-QA11
4:47 PM	1204	Functionality	Unrecorded Agent Sessions	W2K8-S8-QA11
4:46 PM	1201	Functionality	Agent service has started	W2K8-S8-QA11
4:46 PM	1221	Communication	Agent machine and service are accessible	c59-32-3

Note: If the Agent group member has been tampered within the last week (or has incurred data loss), in the **Servers** list, you can click the **Tampered With** (or the **Data Loss**) to open the **System Events** list filtered to display the last week's "tampered with" (or "data loss") events related to this Agent group member.

- 2) You can expand an event to view more details.

4:45 PM	1301	Functionality	Application Server is not working properly	W2K8-S8-QA11
Severity	High			
Component	Application Server			
Source	Application Server			
Status Details	Not Running			
Event Description	The ObserveIT Application Server is not working properly.			
Email Sent	No			
Additional Info	URL of the Application Server or Web Console= Comment=Application server is unreachable			
Remediation Status	New			
Comment	Add Comment			

For further details about the information displayed in the **System Events** list and the event types (possible causes and solutions), see [Viewing System Events](#) and [Event Types](#).

Adding Agent Groups

Administrators can add more Agent groups to the **Admin Dashboard**.

To add Agent groups to the Admin Dashboard

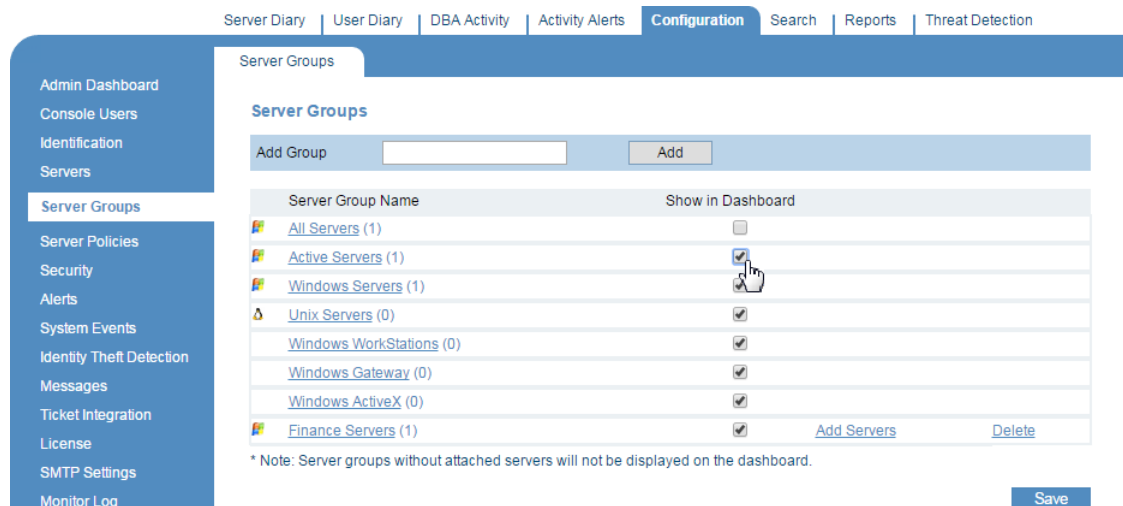
- 1) In the **Agents** portal of the **Admin Dashboard**, click the **Add more groups** link (this is available when there is only one row in the **Agents** list). Otherwise, you can navigate directly to **Configuration > Server Groups**.

The **Server Groups** page opens, where you can select existing groups (or add new groups) to display in the **Admin Dashboard**.

- 2) Select the relevant check box(es) of the server group(s) that you want to show in the **Admin Dashboard**.

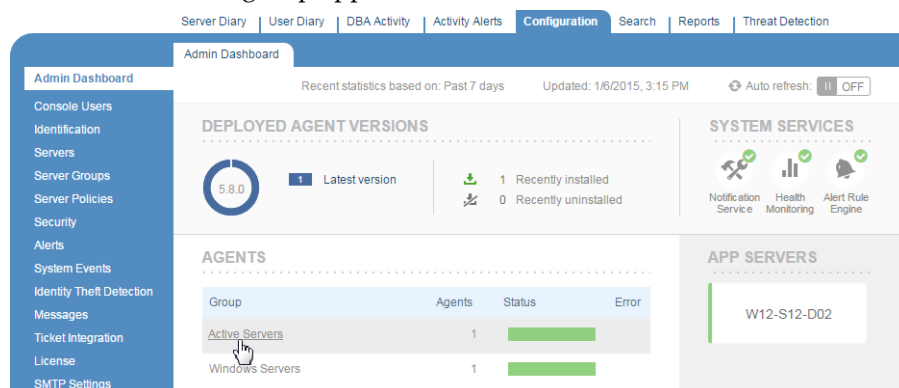
When you add a new server group, the **Show in Dashboard** check box is selected by default, and the new server group is automatically displayed in the **Admin Dashboard** (in the **Agents** portal).

(To remove a server group from the **Admin Dashboard**, clear the **Show in Dashboard** check box next to the relevant server group in the **Server Groups** page.)



- 3) Click **Save** to save the settings.

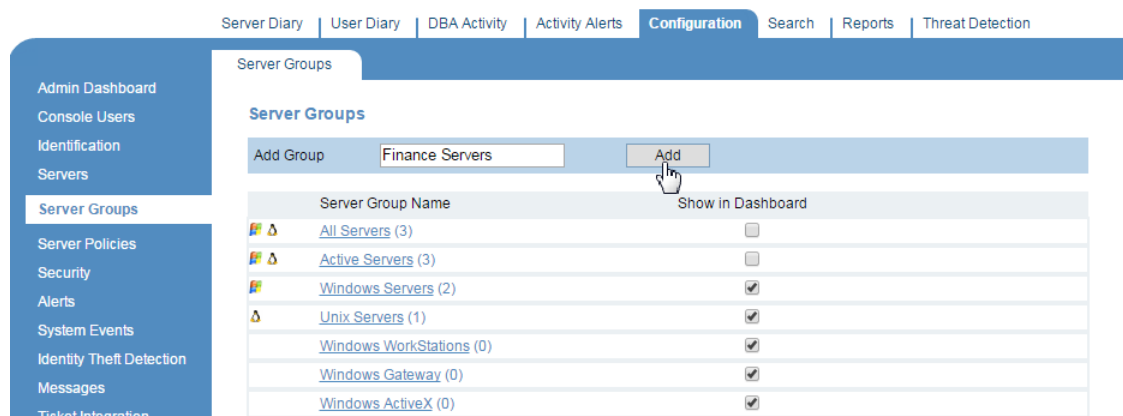
The selected server group appears in the **Admin Dashboard**.



To add a new server group to the Server Group list and display it in the Admin Dashboard

- 1) In the **Server Groups** page, type the name of the new server group and click **Add**.

The following figure shows how to add a new group, "Finance Servers" to the list.



The new server appears in the **Server Groups** list (but without servers).

Note: Server groups without attached servers will not be displayed in the **Admin Dashboard**.

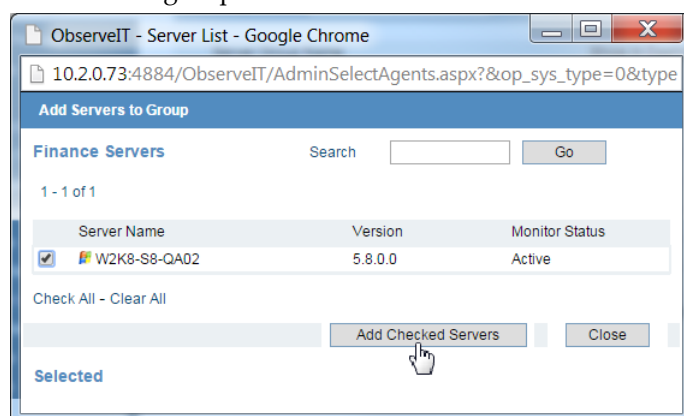
Server Groups

Successfully added

Add Group		Add
Server Group Name	Show in Dashboard	
All Servers (1)	☐	
Active Servers (1)	☐	
Windows Servers (1)	☒	
Unix Servers (0)	☒	
Windows WorkStations (0)	☒	
Windows Gateway (0)	☒	
Windows ActiveX (0)	☒	
Finance Servers (0)	☒	Add Servers Delete

* Note: Server groups without attached servers will not be displayed on the dashboard.

- 2) To add servers to the new server group, click the **Add Servers** link.
- 3) In the **Add Servers to Group** dialog box, select the check boxes of the servers you want to assign to the server group.



- 4) Click **Add Checked Servers**.
A message dialog box opens, prompting you to confirm.
- 5) Click **OK** to confirm to add the server(s) to the group.
The new server group is added with its servers.

Server Groups

Add Group		Add
Server Group Name	Show in Dashboard	
All Servers (1)	☐	
Active Servers (1)	☐	
Windows Servers (1)	☒	
Unix Servers (0)	☒	
Windows WorkStations (0)	☒	
Windows Gateway (0)	☒	
Windows ActiveX (0)	☒	
Finance Servers (1)	☒	Add Servers Delete

* Note: Server groups without attached servers will not be displayed on the dashboard.

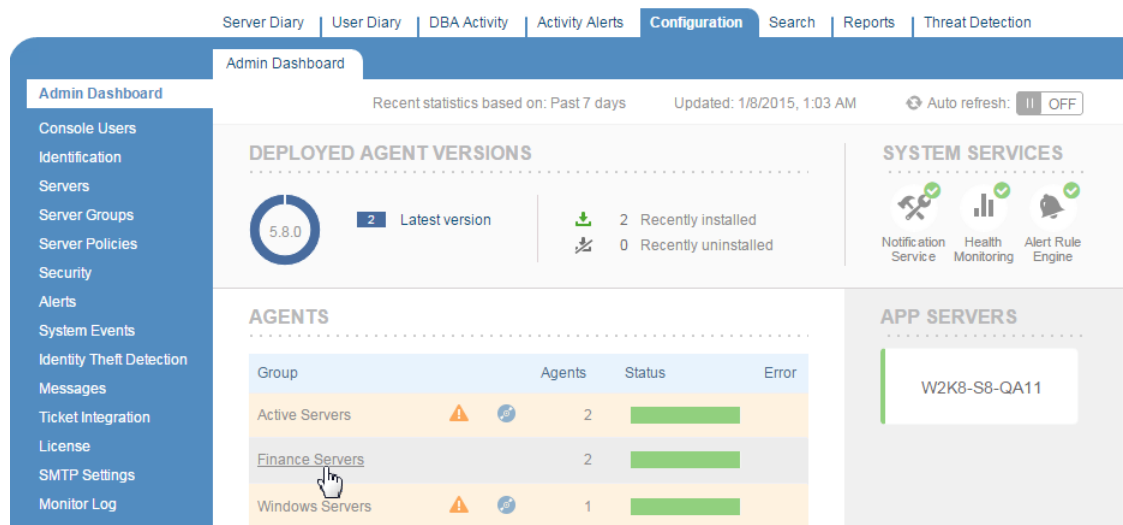
Save

- 6) When you add a new server group, the **Show in Dashboard** check box is selected by default, and the new server group is automatically displayed in the **Admin Dashboard** (in the **Agents** portal).
You can select additional check boxes to show several server groups in the **Admin Dashboard**.

(To remove a server group from the **Admin Dashboard**, clear the **Show in Dashboard** check box next to the relevant server group in the **Server Groups** page.)

- 7) In the **Server Group** list, click **Save** to save the settings.

The new server group is displayed in the **Agents** portal in the **Admin Dashboard**.

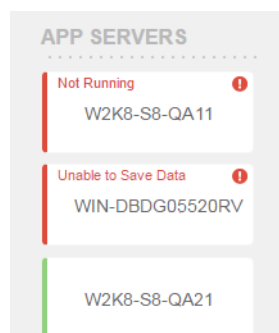


Application Servers

In the **App Servers** portal of the **Admin Dashboard**, you can view the statuses of Application Servers to verify whether they are working properly. This enables you to easily identify problematic Application Servers and issues regarding connections to the database or to your file system, which may affect whether recorded data is saved. From the **App Servers** portal, you can drill down to investigate related system events to identify the causes and respond accordingly.

To view Application Server status and to drill down to related events

- 1) In the **App Servers** portal, view a list of Application Servers and statuses (color coded per severity). The colored severity bar (on the left) indicates the event/operational status severity level. For descriptions of the Application Server statuses, see [Assessing Application Server Statuses and Details](#).



- 2) To drill down to examine event details, click the relevant Application Server.

The **System Events** page opens, filtered to display the Application Server and the related system events that caused the error. (The most recent event that caused the error appears at the top of the list.)

System Events

Severity: Server:

☒ More Filters

Category: All	Event Code: All
Component: Application Server	Source: All
Login: All	Remediation Status: All
Client: All	Email Sent: All
Event ID:	Comment:
Status Details: All	

Period: ☒ During last ☐ Between and

[Reset](#) [Show](#)

1 - 12 of 12

Received	Code	Category	Name	Server
1/7/2015				
☒ 11:03 AM	1301	Functionality	Application Server is not working properly	W2K8-S8-QA11
Severity High Component Application Server Source Application Server Status Details Not Running Event Description The ObserveIT Application Server is not working properly. Email Sent No Additional Info URL of the Application Server or Web Console=http://w2k8-s8-qa11:4884/ObserveITApplicationServer/ Comment Comment=Application server is unreachable Remediation Status New Comment Add Comment				
☒ 10:41 AM	1304	Functionality	Application Server is running	W2K8-S8-QA11
☒ 10:41 AM	1301	Functionality	Application Server is not working properly	W2K8-S8-QA11
☒ 10:33 AM	1304	Functionality	Application Server is running	W2K8-S8-QA11

- Expand an event to view more details.
- Assess the problem and perform the required corrective action. (For example, if the Application Server is not working properly, then you need to restart the Internet Information Service (IIS) to restart the Application Server.)

For further details about system events and event types (and some possible causes and solutions), see [Viewing System Events](#) and [Event Types](#).

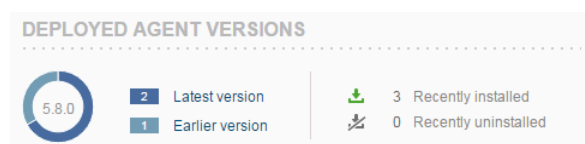
Assessing Application Server Statuses and Details

The following table describes the ObserveIT Application Server statuses and status details that appear through the Web Console (in the **Admin Dashboard**, in the **Servers** list, in the **System Events** list). To identify the causes, go to the [System Events](#) list and resolve as necessary.

Application Server/ Load Balancer Status	Status Details	Possible Reasons/Triggers
OK	N/A	The Application Server is active, functioning normally.
Error	Not Running	The Application Server is not working properly.
	Unable to Save Data	The Application Server failed to save recorded data.

Deployed Agent Versions and Recently Installed/Uninstalled Agents

In the **Deployed Agent Versions** portal (located at the top of the **Admin Dashboard**), you can view the current Agent version number and how many Agents are running the latest software and earlier software versions. This enables you to easily identify whether the upgrade was successful and what is the main software version that you are working with (that most of the Agents are running), which may help you determine whether you want to upgrade other Agents that are currently running earlier versions. You can also view the number of Agents that were recently installed and uninstalled in the past 7 days. From the **Deployed Agent Versions** portal, you can drill down to examine further details about the Agents (including operational statuses).



To view deployed Agent versions and to drill down to further details

- 1) On the left of the **Deployed Agent Versions** portal, view the colored pie chart and the adjacent list which display the three-digit version number of the current Agent version, the number of Agents deployed with the latest software version, and the number of Agents still running earlier versions (not yet updated).

The Agent versions are color-coded (Current=Dark Blue, Previous=Light Blue).

- 2) To drill down to examine Agent details, click the **Latest version** (or **Earlier version**) link.

The **Servers** list opens, filtered to display the Agents that were updated to the latest software version (or the Agents running earlier versions of the software). You can expand the Agent to view more details, including status details (when not "OK"), OS type, and OS version.

Servers

Group: Server Name: Status:

More Filters

Server Policy: Agent Type:

OS Type: OS Version:

Version: Status Details:

Activities:

[Reset](#) [Show](#)

1 - 2 of 2

Server Name	Server Policy	Version	Status	Installation	Last Activity
W2K8-S8-QA14	Default Windows-based ...	5.8.0.0	OK	12/28/2014	12/28/2014
W2K8-S8-QA11	Default Windows-based ...	5.8.0.0	OK	12/28/2014	12/28/2014

[Unregister](#) | [System Events](#)

OS Type: Windows
OS Version: Windows Server 2008 R2

To view the number of Agents that were recently installed/uninstalled and to drill down to further details

- 1) On the right of the **Deployed Agent Versions** portal, view the number of Agents that were recently installed and uninstalled in the past 7 days. (The info bar at the top of the **Admin Dashboard** displays the time period, which is not configurable.)
- 2) To drill down to examine Agent details, click the **Agents recently installed** (or **uninstalled**) links.

The **Servers** list opens, filtered to display the Agents that were installed (or uninstalled) in the past 7 days. You can expand the Agent to view more details, including status details (when not "OK"), OS type, and OS version.

Servers

Group: Server Name: Status:

More Filters

Server Policy: Agent Type:

OS Type: OS Version:

Version: Status Details:

Activities:

[Reset](#) [Show](#)

1 - 2 of 2

Server Name	Server Policy	Version	Status	Installation	Last Activity
c59-32-3	Default Unix-based Policy	5.8.0.153	OK	1/7/2015	1/17/2015
W2K8-S8-QA11	Default Windows-based ...	5.8.0.0	OK	1/7/2015	1/17/2015

[Unregister](#) | [System Events](#)

OS Type: Windows
OS Version: Windows Server 2008 R2

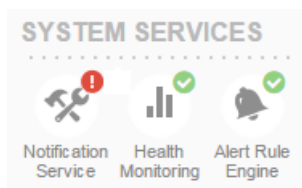
For explanations of the icons and colored severity levels of system events and operational statuses, see [Colored Severity Levels and Icons](#).

System Services

In the **System Services** portal (located at the top of the **Admin Dashboard**), you can view information about the following system services to verify whether they are working properly:

- **Notification Service:** impacts whether there are archives, event emails, and scheduled reports
- **Health Monitoring Service:** impacts whether system health statuses are reported, and whether the data displayed in the **Admin Dashboard** is updated
- **Rule Engine Service:** impacts whether alert rules are created

From the **System Services** portal, you can drill down to investigate related system events in order to identify the causes and respond accordingly.



Services that are OK (normal/active) are marked by . Services with errors are marked by .

To drill down to events related to the system services

- 1) In the **System Services** portal, click a service icon: **Notification Service** , **Health Monitoring** , or **Alert Rule Engine** .

The **System Events** page opens, displaying all the related system events that occurred on the particular system service. (The most recent event appears at the top of the list.)

System Events

Severity: All
Server: All

More Filters

Category: All
Component: Notification Service
Login: All
Client: All
Event ID:
Status Details: All

Event Code: All
Source: All
Remediation Status: All
Email Sent: All
Comment:

Period: During last 1 Months Between 12/30/2014 and 01/07/2015

Reset Show

1 - 2 of 2

Received	Code	Category	Name	Server
1/6/2015				
	3:20 PM 1306	Functionality	Notification Service has stopped	W12-S12-D02
Severity High Component Notification Service Source Notification Service Event Description The Notification Service has stopped. Email Sent No Remediation Status New Comment Add Comment				
1/4/2015				
	10:25 AM 1305	Functionality	Notification Service has started	W12-S12-D02

- 2) Expand an event to view more details.

- 3) Assess the problem and perform the required corrective action. (For example, if the service is not working properly, then you need to restart the service.)

For further details about system events and event types (and some possible causes and solutions), see [Viewing System Events](#) and [Event Types](#).

Refreshing the Admin Dashboard

You can refresh the data displayed in the **Admin Dashboard** (manually or automatically).

To manually refresh the Admin Dashboard

- On the info bar (on the upper right of the **Admin Dashboard**), click the **Refresh**  button.
The data in the **Admin Dashboard** is updated, and the **Updated** field displays the refresh date and time.

To automatically refresh the Admin Dashboard

- On the info bar (on the upper right of the **Admin Dashboard**), click **ON** the **Auto refresh** button and choose an option from the drop-down list to automatically refresh the page (every **5**, **10**, or **15 minutes**).

The data in the **Admin Dashboard** is updated per the set time interval, and the **Updated** field displays the refresh date and time.

Console Users

ObserveIT administrators are also known as Console Users. Console Users can log on to the ObserveIT Web Console and view recorded sessions and other information, as well as make configuration changes based upon their role.

There are three types of Console User roles:

- The **Admin** role has the highest permissions with full control over all the management features of ObserveIT. An Administrator can make changes to the ObserveIT configuration, and is allowed to view all session recordings. This is the default role.
- The **View-Only Admin** role can view session recordings, but cannot gain access to any ObserveIT configuration option.
- The **Config Admin** role allows administrative access to the Web Console without the ability to review user activity logs or screen recordings. Config Admin users can only access specific configuration areas, and can manage only other Config Admin user accounts.

See the following topics:

- [Creating Local or Active Directory-based Console Users](#)
- [Creating and Managing Local Console Users](#)
- [Creating Active Directory Console Groups](#)
- [Assigning Console User Permissions to View Recordings](#)

Creating Local or Active Directory-based Console Users

You can easily create additional Console Users. When you create a Console User, you can create either Local Console Users (which will be created in the ObserveIT database), or, if an LDAP Target has been established, Active Directory-based Console Users.

If the server on which the ObserveIT Application server is installed is a member of an Active Directory domain, that Active Directory domain will be automatically added to the list of LDAP Targets, and will be configured as an "Automatic"-type LDAP Target. This will enable the usage of Active Directory users and groups from all domains in all the Active Directory forests that are connected to the current forest.

ObserveIT easily integrates with your Active Directory forest, enabling you to use user and group objects from any domain in the forest in which the ObserveIT server-side components are installed, and in which the ObserveIT Agents are deployed (if different). Cross forest trusts can also be used. Although using groups from Active directory domains is possible with any group scope (domain local, global, or universal), it is recommended that you follow Microsoft's best practices on group object usage. For further details, refer to [Active Directory Best Practices](#).

If the server was not a member of any domain during the ObserveIT installation, then after adding the server to a domain, you will be able to add the LDAP Target later. If the server on which the ObserveIT Application server is installed is not a member of any Active Directory domain, you can manually add LDAP Targets, and these will be configured as "Manual"-type LDAP Targets. This will enable the usage of Active Directory users, however it will not be possible to use groups from that domain.

Creating Console Users for an Active Directory domain will NOT create actual Active Directory user objects. These Console Users are just "pointers" to Active Directory user objects that are supposed to exist in the target Active Directory domain. That is why the "Password" field is grayed-out whenever an Active Directory domain is selected. If you are using "Automatic"-type LDAP Target, and the user name is not verified, you will get an error message. This check is NOT performed if you are using "Manual"-type LDAP Targets or when you specify a domain manually. When a user that is configured as an ObserveIT Console User tries to log on to the ObserveIT Web Console, and that user's Authentication target is selected as the Active Directory domain, the ObserveIT Web Console will connect to the destination domain and try to authenticate the user given the user's credentials.

Console Users can be granted **Admin**, **View-Only Admin**, or **Config Admin** roles, and given permissions on specific servers, groups of servers, or individual users, based upon the organization's requirements. This allows the administrator to grant granular replaying access control permissions for specific security managers or auditors (for example, to be allowed to view servers only in the "SQL Servers" server group, or to be allowed to view sessions only for a limited scope of users).

Console Users can also be configured to receive email notifications.

The entire configuration process is done through the **Configuration > Console Users** page.

See the following topics:

- [Creating and Managing Local Console Users](#)
- [Creating Active Directory Console Groups](#)
- [Assigning Console User Permissions to View Recordings](#)

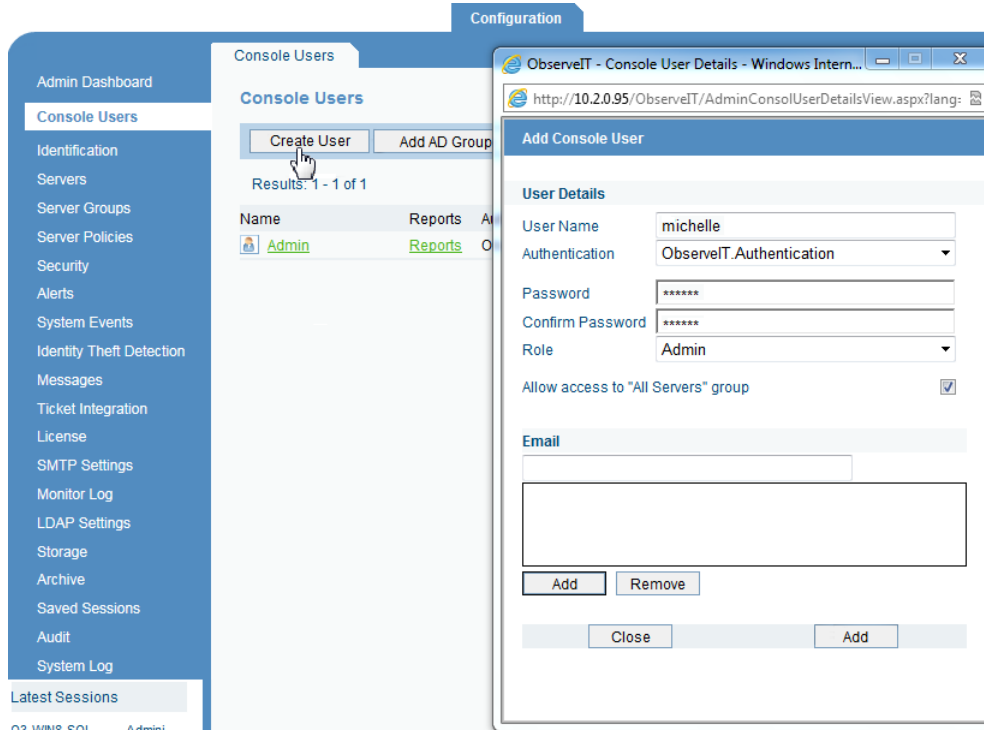
Creating and Managing Local Console Users

This topic describes how to create a new console user, edit the details of a console user, delete a console user, and create a report about a console user.

To create a new Console User

- 1) In the **Configuration > Console Users** tab, click the **Create User** button.

The **Add Console User** dialog box opens.



- 2) Enter the required name for the new Console User.
- 3) Enter a local ObserveIT user, or select an Active Directory domain for authentication.
- 4) Enter a password, and confirm the password.
- 5) From the **Role** drop-down list, select the role of the Console User:
 - **Admin:** This role has full control over all the management features of ObserveIT. An Administrator can make changes to the ObserveIT configuration, and is allowed to view all session recordings.
 - **View-Only Admin:** This role can view session recordings, but cannot gain access to any ObserveIT configuration option.
 - **Config Admin:** This role can see all users and their permissions, but can create or delete only "Config Admin" users. Config Admin users are unable to view session recordings.

By default, the **Allow access to "All Servers" group** check box is selected for new Console Users, which allows them access to all the deployed ObserveIT Servers. If required, you can clear the check box, and then manually grant the Console User the appropriate access rights to either single ObserveIT Servers or to Server Groups.

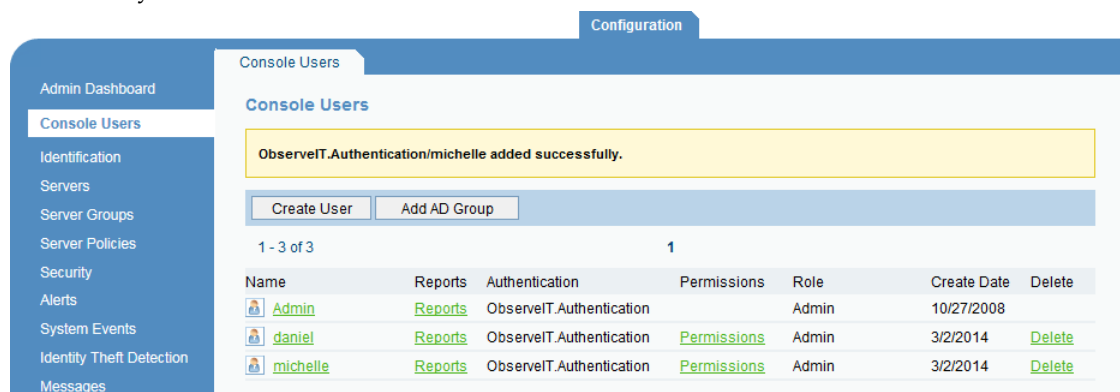
- 6) To configure an email address to enable the Console User to receive email notifications:
 1. Enter the user's email address in the **Email** field, and click **Add**.
The email address will be added to the list.
 2. Repeat the above step for each email address you want to add.

Note: To remove an email address from the list, select it and click **Remove**.

- 7) When you have finished configuring the new user, click **Add**. If required, you can repeat this procedure to add another user.
- 8) Click **Close** to close the **Add Console User** dialog box.

The new user is added to the list in the **Console Users** page.

A message is displayed at the top of the page, confirming that the new user was added successfully.



To update the details of an existing Console User

- 1) In the **Console Users** list, click the name of the user whose details you want to update.
The **Edit Console User** dialog box opens.
- 2) In the **Edit Console User** dialog box, you can change the **Role** and/or the email address for the Console User.

Note: You cannot edit the user's credentials or "Authentication" method.

- 3) Click the **Update** button. A message is displayed at the top of the **Console Users** page, confirming that the user was updated successfully.

To delete a Console User

- In the **Console Users** page, click the **Delete** link next to the user you want to delete from the **Console Users** list.

Note the following:

1. Deleting Console Users does not result in any data loss to the recorded sessions, but this action cannot be reversed. If you need to create the Console User after you have deleted it, you will need to create a new Console User and make sure it has the exact same name and password.
2. Deleting Console Users that are configured with an external Active Directory or LDAP domain will NOT delete the actual user objects from the target Active Directory domain. The deletion will simply prevent these users from using the ObserveIT Web Console.

To schedule a report or create a new report about a Console User

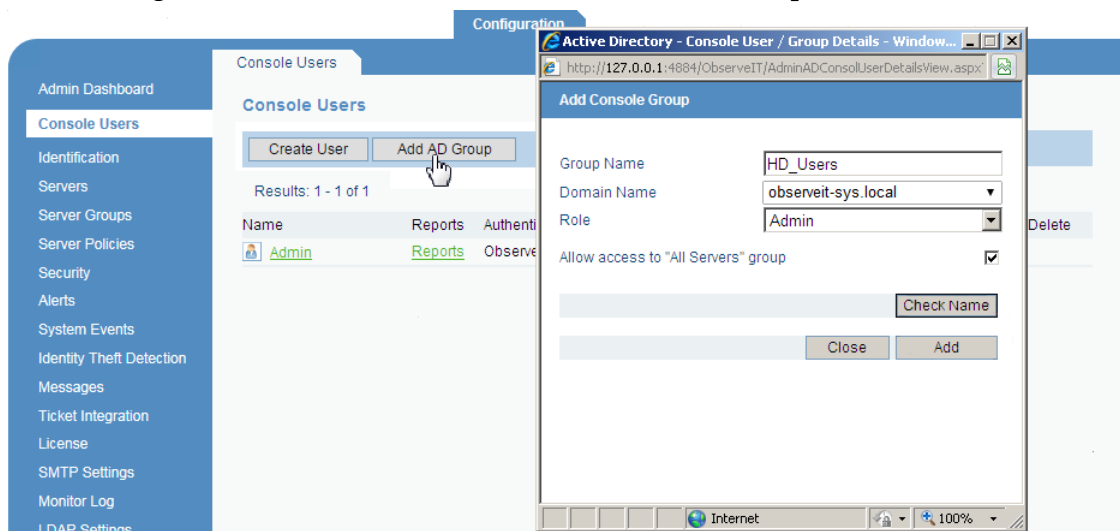
- In the **Console Users** page, click the **Reports** link next to the required user. For further details, see [Managing Reports](#).

Creating Active Directory Console Groups

Note: When creating Active Directory-based groups in ObserveIT, a check will be performed against the domain to make sure that the group exists.

To create an Active Directory group in ObserveIT

- 1) In the **Configuration > Console Users** tab, click the **Add AD Group** button.



- 2) Enter the **Group Name**.
- 3) In **Domain Name**, enter the required domain for the console group, or select it from the drop-down list which displays all the domains in the Active Directory forest in which the ObserveIT Application Server is a member.
- 4) If required to change the permissions assigned to the group, from the **Role** list, select **Admin**, **View-Only Admin**, or **Config Admin**.
- 5) Click **Check Name** to verify the group name.
If the group name is verified, a confirmation message is displayed.
- 6) Click **Add** to add the console group.

Assigning Console User Permissions to View Recordings

Console Users can be granted permissions to view recorded sessions on one or more servers (on which the ObserveIT Agent is installed), on server groups, and for specific users. These permissions are given to users based on their defined role.

To grant permissions for Console Users

- 1) In the **Configuration > Console Users** tab, click the **Permissions** link next to the Console User name whose permissions you want to modify. The following dialog box opens.

By default, new Console Users have permissions to the **All Servers** group, which means that they can access all the deployed ObserveIT Servers. If required, you can deselect the "All Servers" check box, and then manually grant the user the appropriate access rights to either single ObserveIT Servers, or to Server Groups. For example, you might want to configure a specific Console User to only view recorded sessions on five individual SharePoint servers, and to restrict a different Console User to view recorded sessions on only three different SQL servers.

The screenshot shows the 'Configuration' tab in the ObserveIT console. The 'Console Users' section is active, displaying 'User Permissions for user: daniel'. The 'Servers' section has a table with the following data:

Name	Type	Version	Status	Date
☒ All Servers	Group			

The 'Users' section is currently empty. Both sections have 'Add' and 'Remove' buttons, and a 'Check All - Clear All' link at the bottom.

2) To assign the console user permissions to view recordings made on specific servers or groups of servers:

1. If you do not want the Console User to be able to monitor all the installed servers, in the **Servers** section, you must remove the **All Servers** group from the permissions list of the user. Click the check box next to the **All Servers** group, and click **Remove**.

Note: If you do not add at least one server to this list, the Console User will not be able to view any servers, and therefore will be rendered useless. You will not be able to save the settings if no server or server group exists in the server list.

2. After you have removed the **All Servers** group from the list of permissions, you must add at least one valid server to the list of permissions for that Console User. Click the  button, select a server, and click **Add**.
The server is added to the list.

3. To grant permissions for the Console User to view entire groups of machines, click the **Server Groups** drop-down list, select the **Server Group**, and click **Add**.
The Server Group is added to the list.
 4. To remove a server from the list, in the permissions screen for the Console User, in the **Servers** area, select the server you want to remove, and click **Remove**.
- 3) To assign the Console User permissions to view the recorded sessions of specific users:
1. In the **User** area, enter the user login (in the format Domain\Username) of the specific user, and click **Add**.
The user is added to the list.
 2. Repeat the above step for each user whose recordings you want to allow the Console User to view.
-
- Note: You can also allow the Console User to view sessions of users who do not have recorded sessions. By not listing any user, access is also permitted to users without recorded sessions.
-
3. To remove a specific user from the permission list of the Console User, select the check box next to the user name, and click **Remove**.
- 4) Click **Save** to save your settings when you have finished assigning permissions on specific servers, groups of servers, or individual users.

Identification Services

Note: The Identification Services feature is supported on Windows and Unix/Linux Agents.

When multiple users have access to a generic account (such as the default Administrator account), it can be difficult, even impossible to identify the actual person who is using the account. By enabling and configuring ObserveIT's Identification Services, the system can be configured to require users that log on to the monitored servers to identify themselves with a secondary ObserveIT log on prompt, before they can access a Windows server desktop or a published application. On Linux/Unix Agents, generic users with shared user accounts (such as "root" or "sysadmin") will be prompted to enter their secondary credentials before they can open an interactive user session on an ObserveIT-monitored Linux/Unix computer. These users are also known as "Forced-Identification" users. The exact names of Forced-Identification users is decided by the client, based on the client configuration and particular needs. The names should include user accounts that are widely known, to enable more than one person to use them for logging on to the monitored systems.

ObserveIT's Identification Services can integrate with Active Directory. After completing the Windows/Unix logon process, users receive a secondary ObserveIT logon prompt, in which they must enter their own personal user name and password before continuing (see [Forced-Identification User Login](#)). These user credentials are then checked against an Active Directory source. When no central Active Directory is available against which ObserveIT Identification services can authenticate, you can define local ObserveIT targets for user authentication. In this case, after users enter their personal user name and password during ObserveIT Identification Services log on, their credentials can be checked against a predefined list of ObserveIT local users.

Note the following:

- When you configure a Forced-Identification user, that user account cannot be used for the secondary ObserveIT log on. This means that if a Forced-Identification user such as "*"\\Administrator" is created, and a user logs on to a server with the "PROD\\Administrator" account, they will be required to provide secondary user authentication credentials using a different account, either from Active Directory or from the Local ObserveIT Identification Users database.
- When ObserveIT's Identification Services are integrated with Active Directory, you can allow only users that are members of a specific Active Directory group to log on to the monitored machines. In this scenario, you can restrict users from gaining access to the desktop, unless they are members of a predefined Active Directory group. Note that using Active Directory groups is only possible if the LDAP target is an "Automatic"-type LDAP Target.
- ObserveIT supports only Microsoft Active Directory services. Users or groups that are not members of domain local groups *must* be synchronized with Active Directory.
- Any modifications you make when configuring Identification Services can be viewed for auditing purposes in the **Configuration Changes** tab of the Web Console. For further details, see [Auditing Configuration Changes](#).

See the following topics:

- [Viewing Forced-Identification Users in the Web Console](#)
- [Steps for Configuring ObserveIT Identification Services](#)
- [Enabling Secondary Identification for Linux/Unix Policies](#)
- [Configuring Forced-Identification Users](#)
- [Configuring Active Directory Identification Targets](#)

- [Configuring Active Directory Groups](#)
- [Configuring Local ObserveIT Identification Users](#)
- [Forced-Identification User Login](#)
- [Preventing Windows Users from Bypassing the ObserveIT Identification Prompt](#)

Viewing Forced-Identification Users in the Web Console

When Identification Services are configured and a Forced-Identification user has successfully logged in, in the ObserveIT Web Console you can view the name of the user who logged in with the shared user account in the **Server Diary**, **User Diary**, **Free-Text Search**, or **Reports** page, as shown in the following figure.

Note: When Identification Services are not configured, the only information available is the login name.

The screenshot displays the 'Server Diary' interface. On the left is a navigation menu with options like Activities, Applications, Inventory, Software, Search, and Messages. The main area is titled 'Activity View' and shows filters for Server (c65-64-3), Period (Last 1 Month), and Start/End Dates (Dec 29, 2013 to Jan 6, 2014). Below the filters is a table of sessions. The table has columns: Session Duration, Login, User, Server, Client, Slides, and Video. The 'User' column for the most recent session (12:42 PM - 12:45 PM) shows 'john'.

Session Duration	Login	User	Server	Client	Slides	Video
12:47 PM - 12:48 PM	root	n/a	c65-64-3	10.1.100.29	5	[icon]
12:47 PM - 12:47 PM	root	james	c65-64-3	10.1.100.29	16	[icon]
12:42 PM - 12:45 PM	root	john	c65-64-3	10.1.100.29	26	[icon]

Steps for Configuring ObserveIT Identification Services

To configure the ObserveIT Identification Services

- 1) In the ObserveIT Web Console, navigate to **Configuration > Identification**.
- 2) Create Forced-Identification users. Creating these users does not affect any actual user accounts; it simply instructs ObserveIT to require identification when any of these users log on to any ObserveIT-monitored server. For further details, see [Configuring Forced-Identification Users](#).
- 3) Configure the authentication targets for these users. Identification is performed against one or more LDAP targets (or domains) by adding Active Directory identification targets. When no central Active Directory is available against which ObserveIT Identification services can authenticate, you will need to use local ObserveIT targets for user authentication. For further details, see [Configuring Active Directory Identification Targets](#) and [Configuring Local ObserveIT Identification Users](#).
- 4) Configure which Active Directory groups can authenticate to the secondary ObserveIT logon. If the LDAP target is an "Automatic"-type, you can prevent users who are not members of a predefined Active directory group from gaining access and logging on to the monitored servers. For further details, see [Configuring Active Directory Groups](#).

- 5) Later, if required, you can configure either a Manual Server Policy or Server Policies to configure which server will be affected by the new Identification Policy. For further details, see [Identification Policy](#).

Important: To enable secondary authentication for ObserveIT users on Unix/Linux Agents, you must first enable secondary authentication for Unix/Linux policies in the ObserveIT Web Console. For further details, see [Enabling Secondary Authentication for Linux/Unix Policies](#).

Enabling Secondary Identification for Linux/Unix Policies

In the ObserveIT Web Console, you can configure the server policy settings that are required for user secondary identification on a Linux/Unix Agent. Before you can do this, you must enable secondary authentication for Linux/Unix policies in the Web Console.

To enable the secondary user authentication settings in the ObserveIT Web Console

- 1) Locate the `web.config` file of the ObserveIT Web Console located under:
`C:\Program Files (x86)\ObserveIT\Web\ObserveIT`.
- 2) In the `web.config` file, add the following line under the `<appSettings>` section:
`<add key = "EnabledUnixSecondaryAuth" value="true"/>`.
- 3) Save the `web.config` file.
- 4) Log off and then log back on to the Web Console.

The settings for user secondary authentication are available for configuration on Linux/Unix server policies.

For instructions on how to configure secondary identification policy settings, see [Identification Policy](#).

Configuring Forced-Identification Users

"Forced-Identification" users are required to identify themselves by a secondary log on prompt when logging on to any ObserveIT-monitored server. The secondary logon authentication process forces generic users (such as "Administrators" or "root") to be authenticated against an Active Directory identification target or against Local ObserveIT Users.

This topic describes how to add new Forced-Identification users. (It also describes how to delete Forced-Identification users.)

Note: Adding Forced-Identification users does NOT create any actual users and has no effect on user accounts. It just configures ObserveIT to request a secondary logon when any of these users log on to a monitored server.

To configure Forced-Identification Users

- 1) Navigate to **Configuration > Identification**.

The screenshot shows the 'Identification' configuration page. Under 'Forced-Identification Users', there is a 'Create' button and a table listing three users. Below this, the 'Users For Secondary Identification' section is visible, containing 'Active Directory Identification Targets' and a table with one entry.

Domain Name	Login	Manage	Delete
*	admin4ya	Manage	Delete
*	administrator	Manage	Delete
*	dba	Manage	Delete

Domain Name	Type
OBSERVEIT-DEMO.LOCAL	Auto

- 2) In the **Forced-Identification Users** section, click the **Create** button.

The **Identification User Policy Templates** window opens, where you can specify whether to apply identification policies to a specific user or to all users. Whenever the specified users log on to any of the servers that are linked to the selected policies, they will be required to provide secondary authentication credentials.

ObserveIT - Identification User Policy Templates - Windows Internet Explorer

Identification User Policy Templates

Please select **All Users** or enter **Domain Name \ Login** (e.g.: *administrator or OBSERVEIT\DanielP) to enforce identification policy.

☐ All Users

☒ User

Domain (* for all) Login

Apply to Server Policy Templates

Click to select one or more Server Configuration Policies from the list below. Anytime the above user will log on to any of the servers that are linked to the selected policies, they will be required to provide secondary authentication credentials.

Note: The Enforce login check box in the selected policies **must** be turned on in order to take effect.

Policy Name	Enforce login is turned on
☒ Default Windows-based Policy	Yes
☒ Default Metadata Only Policy	Yes
☐ Default Recording Disabled Policy	No
☒ Default Unix-based Policy	Yes

Apply to Server Policies

Note: Only servers that have manual configuration settings will be listed.

Note: The Enforce login check box in the selected servers **must** be turned on in order to take effect.

Server Name	Enforce login is turned on
☐ Manual - c55-64-5	No
☐ Manual - c58-32-11	Yes
☒ Manual - D008R264SQL8	Yes
☐ Manual - D02003X862	Yes

- 3) Select one of the following options:
 - **All Users:** to apply the identification policies to all users.
 - **User:** to apply the identification policies to a specific user.
- 4) If you selected the **User** option, select the domain name for the relevant Forced-Identification user, and specify the user's name.

The **Domain** drop-down list displays all the domains in the Active Directory forest in which the ObserveIT Application Server is a member. You can select "*" to select all domains.

Note: ObserveIT easily integrates with your Active Directory forest, enabling you to use user and group objects from any domain in the forest in which the ObserveIT server-side components are installed, and in which the ObserveIT Agents are deployed (if different). Cross forest trusts can also be used, if required. Although using groups from Active directory domains is possible with any group scope (domain local, global, or universal), it is recommended that you follow Microsoft's best practices on group object usage. For further details, refer to [Active Directory Best Practices](#).

As an example, consider a scenario in which the ObserveIT Web Console Server is installed in a DMZ (or perimeter network) and is not a member of any domain, and it will be used to monitor a Terminal Server farm consisting of 50 servers. These servers will be used by users that are members of two separate domains - PROD and DEV. In this example, all the users that log on to these servers with either the PROD\Administrator or the DEV\Administrator accounts will be identified. In this scenario, you can either add separately both users: "PROD\Administrator" and "DEV\Administrator", or just add one user that includes both these options: that is, "*\Administrator". If a third domain, "ACCTG", is later added to the scenario, and the "ACCTG/Administrator" must be identified, you will need to add a third user. If you specify "*\Administrator", you will not need to make any modifications. However, you cannot use "*\Administrator" if the "ACCTG/Administrator" is NOT required to be identified, since all users called "Administrator" from all domains would be forced to identify.

Important: When you configure a Forced-Identification user, that user account cannot be used in the secondary ObserveIT Windows logon screen/Unix prompt. This means that if a Forced-Identification user such as *\Administrator is created, and a user logs on to a server with the PROD\Administrator account, they will be required to log on to the secondary ObserveIT Windows logon screen/Unix prompt with another account, either from Active Directory or from the Local ObserveIT Identification Users database.

- 5) In the **Apply to Server Policy Templates** section, update the server policy templates by selecting the check boxes of all the server policies on which you want to configure the user(s). You must select at least one check box, but you can make changes to these settings later.

Apply to Server Policy Templates

Click to select one or more Server Configuration Policies from the list below. Anytime the above user will log on to any of the servers that are linked to the selected policies, they will be required to provide secondary authentication credentials.

Note: The Enforce login check box in the selected policies **must** be turned on in order to take effect.

Policy Name	Enforce login is turned on
☒ Default Windows-based Policy	Yes
☒ Default Metadata Only Policy	Yes
☐ Default Recording Disabled Policy	No
☒ Default Unix-based Policy	Yes

Note the following:

1. In order for Forced-Identification users to be prompted to enter their secondary credentials, **Enforce Login** must be turned on for the selected Server Configuration Policies. To enable **Enforce Login**, select the check box in the **Identification Policy** section in the **Server Policies Template** window accessed from the **Configuration > Server Policies** page. For further details, see [Identification Policy](#).
 2. You can also configure a recording policy for Forced-Identification users which specifies which users and/or user groups to include/exclude from being recorded. For further details, see [User Recording Policy](#).
- 6) Instead of using Server Policies, you can add individual Servers (or Agents) that will enforce the identification of the selected users. To do this, in the server list in the **Apply to Servers** section of the **Policy Templates for Identification User** window, select the check boxes next to the required server names.

Note that this option has additional administrative overhead, as you may need to manually add servers to the list. To manually add a server to the list, go to the **Configuration > Servers** page, select the required server name (which is currently linked to a default policy template), unlink the server from the server policy, and click **Save**. For further details, see [Servers](#). The server will be included in the list of servers in the **Apply to Servers** section.

Apply to Server Policies

Note: Only servers that have manual configuration settings will be listed.

Note: The Enforce login check box in the selected servers **must** be turned on in order to take effect.

Server Name	Enforce login is turned on
☐ Manual - c55-64-5	No
☐ Manual - c58-32-11	Yes
☒ Manual - D008R264SQL8	Yes
☐ Manual - D02003X862	Yes

Add **Close**

- 7) If you want to define more users, click the **Add** button in the **Identification Users Policy Templates** window, and repeat the above steps.
- 8) When you have finished defining all your required Forced-Identification Users, click **Close**. The **Forced-Identification Users** list displays the users that you configured to authenticate themselves when they log on to a monitored server.

Identification

Identification (2)

Forced-Identification Users - / added successfully.

Forced-Identification Users

These users will be forced to authenticate themselves whenever they log on to a monitored server (2)

Create

Results: 1 - 0 of 0

Domain Name	Login	Manage	Delete
All Users		Manage	Delete

- 9) The next step is to configure an LDAP (or Active Directory) Identification Target, or Local ObserveIT Identification users. A warning message is displayed if you do not configure at least one Active Directory Identification Target or at least one Local ObserveIT Identification user. For further details, see [Configuring Active Directory Identification Targets](#) and [Configuring Local ObserveIT Identification Users](#).

Note: After creating the Forced-Identification user, and adding it to at least one Server Configuration Policy or Server, in that policy or server, you will be able to see the Forced-Identification user in the **Identification Policy** section of the Server Policy Template.

Deleting Forced-Identification Users

Deleting a Forced-Identification user does not have any effect on the actual user object, either in Active Directory or on the Windows Local Users. However, these users will no longer be required to identify themselves when they log on to the ObserveIT-monitored servers.

You can delete Forced-Identification users either from the Forced-Identification Users list or from the Server Configuration Policy to which they were linked.

To delete users from the Forced-Identification Users list

- 1) Navigate to the **Configuration > Identification** page.
- 2) In the **Forced-Identification Users** section, click the relevant **Delete** link in the list of users.
You will be prompted to acknowledge your action.
- 3) Click **OK** to proceed, or **Cancel** to abort the deletion.

To delete Forced-Identification Users from the Server Configuration Policy to which they were linked

- 1) Navigate to the **Configuration > Server Policies** page.
- 2) Navigate to the relevant Server Configuration Policy.
- 3) In the **Identification Policy** section of the policy, select the check box next to the Forced-Identification users that you want to remove.

Identification Policy

☒ Enforce Login

Secondary authentication message (2) All activity on this machine is recorded and r Default

Please select All Users or enter Domain Name \ Login (i.e *administrator or OBSERVEITdanielp) to enforce identification for that user. You can add multiple users to this list.

☒ All Users ☐ User

Domain (* for all) Login

*administrator Add

Domain\User	Created Date
*administrator	12/29/2014

Remove

☒ Save last used login

- 4) Click **Remove**.
- 5) Click **Save** to save the server configuration policy.

Configuring Active Directory Identification Targets

Active Directory Identification Targets are the domains against which Forced-Identification users are authenticated. When you configure the targets correctly, they appear in the ObserveIT Identification Services page. To allow ObserveIT to use Windows Authentication against an Active Directory target, you will need to add an LDAP target.

If the server on which the ObserveIT Application server is installed is a member of an Active Directory domain, the Active Directory domain will be automatically added to the list of LDAP targets, and will be configured as an "Automatic"-type LDAP target. This will enable the usage of Active Directory users and groups from all domains in all the Active Directory forests that are connected the current forest.

Note: ObserveIT easily integrates with your Active Directory forest, enabling you to use user and group objects from any domain in the forest in which the ObserveIT server-side components are installed, and in which the ObserveIT Agents are deployed (if different). Cross forest trusts can also be used. Although using groups from Active directory domains is possible with any group scope (domain local, global, or universal), it is recommended that you follow Microsoft's best practices on group object usage. For further details, refer to [Active Directory Best Practices](#).

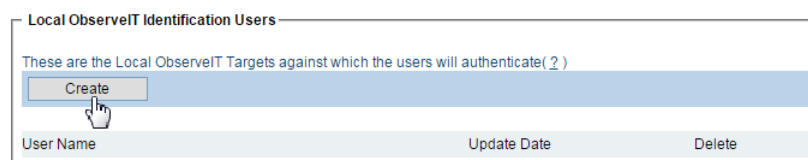
If the server was not a member of any domain during the ObserveIT installation, after adding the server to a domain, you will be able to add the LDAP target later. If the server on which the ObserveIT Application server is installed is not a member of any Active Directory domain, you can manually add LDAP targets, which will be configured as "Manual"-type LDAP targets. This will enable the usage of Active Directory users; however, you cannot use groups from that domain.

Note that only one automatic LDAP target domain can exist at any given time. Changes to the LDAP Targets are done through the **Configuration > LDAP Settings** page.

Note: The ObserveIT Web Console Server must be able to communicate through LDAP traffic with at least one of the domain controllers in the target Active Directory domain. LDAP traffic uses TCP port 389 in most cases. If a firewall exists between the ObserveIT Web Console Server and the domain controller, you must configure the firewall to allow LDAP traffic to and from that domain controller. For information on how to properly configure your firewall, consult with your firewall vendor, or user manual.

To configure an Active Directory Identification Target

- 1) Navigate to the **Configuration > Identification** page.
- 2) In the **Active Directory Identification Targets** section, click the **Create** button.



The **LDAP Settings** page opens.

- 3) Configure an automatic or manual LDAP target. For details, see [LDAP Settings Configuration](#).
- 4) Specify the **Domain**, **User Name**, and **Password** that will be used to access the domain, which will be used as the Active Directory Identification target.

After the LDAP connection is established, the domain against which the users will be authenticated appears in the **Active Directory Identification Targets** section of the **Configuration > Identification** page.

Configuring Active Directory Groups

By integrating ObserveIT with Active Directory, you can configure Identification Services so that no user can pass the ObserveIT Identification screen unless they are members of a specific Active Directory group. In this way, you can prevent users who are not members of a predefined Active directory group from gaining access to the Windows desktop and logging on to the monitored servers.

Note: Using Active Directory groups is only possible if the LDAP target is an "Automatic"-type LDAP Target. For further details, see [Configuring Active Directory Identification Targets](#).

By default, all Active Directory groups can authenticate. You can exclude specific groups from being able to authenticate, or allow only specific groups to authenticate. In the **Active Directory Groups** section of the **Configuration > Identification** page, you can include and exclude Active Directory groups from the specified Active Directory domain.

To include or exclude Active Directory groups from a domain

- 1) Navigate to the **Configuration > Identification** page and add Forced-Identification user(s). For further details, see [Configuring Forced-Identification Users](#).
- 2) In the **Active Directory Identification Targets** section, make sure that there is an "Auto"-type Active Directory Domain. If no "Auto"-type domain exists, you will not be able to use Active Directory groups.

Users For Secondary Identification :

Active Directory Identification Targets

These are the Active Directory Targets against which the users will authenticate (2)

Create

Domain Name	Type
OIT-DEMO.LOCAL	Auto

Active Directory Groups

Note: Active Directory groups are only available when using an Automatic LDAP Target.

Save

☒ Enable all groups from this Active Directory domain.

To exclude any group from being able to log-on, please enter the Active Directory group name (i.e. "Help Desk" or "Domain Admins"). You can add multiple groups to this list.

Exclude: Group

Domain Name	Group Name
OIT-DEMO.LOCAL	

Add

Domain\User	Created Date
-------------	--------------

Remove

☐ Disable all groups from this Active Directory domain

To enable specific groups from this domain to log-on, please enter the Active Directory group name (i.e. "Help Desk" or "Domain Admins"). You can add multiple groups to this list.

Enable: Group

Domain Name	Group Name
OIT-DEMO.LOCAL	

Add

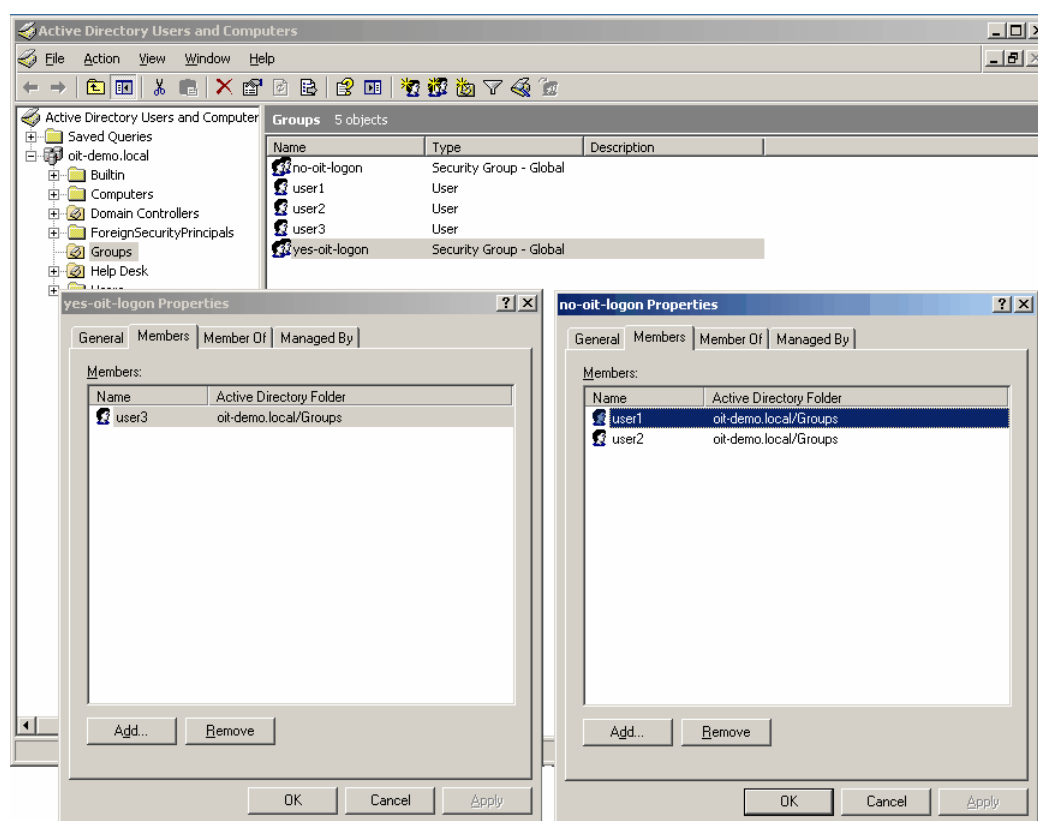
Domain\User	Created Date
-------------	--------------

Remove

- 3) In **Active Directory Users and Computers**, create the required group(s) and add members to them.

In the following example, two groups are defined in the domain **OIT-DEMO.LOCAL**:

- **no-oit-logon**: All users can authenticate in the ObserveIT Identification screen, except users that are members of this group (in this case, user1 and user2).
- **yes-oit-logon**: Only users that are members of this group can authenticate in the ObserveIT Identification screen.



- 4) If you want to configure the ObserveIT Identification Service to allow access to all Active Directory groups except those in the **Exclude** list:
 1. Select **Enable all groups from this Active Directory domain**.
 2. In **Exclude: Group**, enter the domain name of the Active Directory group that you want to exclude from the Identification Service, or select it from the list of all the domains in the Active Directory forest in which the ObserveIT Application Server is a member.

Note: ObserveIT easily integrates with your Active Directory forest, enabling you to use user and group objects from any domain in the forest in which the ObserveIT server-side components are installed, and in which the ObserveIT Agents are deployed (if different). Cross forest trusts can also be used. Although using groups from Active directory domains is possible with any group scope (domain local, global, or universal), it is recommended that you follow Microsoft's best practices on group object usage. For further details, refer to [Active Directory Best Practices](#).

- Enter the group name that you want to exclude (in this case, **no-oit-logon**), and click **Add**.

Active Directory Groups

Note: Active Directory groups are only available when using an Automatic LDAP Target.

☒ **Exclude all groups from this Active Directory domain.**

To exclude any group from being able to log-on, please enter the Active Directory group name (i.e "Help Desk" or "Domain Admins"). You can add multiple groups to this list.

Exclude: Group \

Domain\User	Created Date
☐ OIT-DEMO.LOCAL\no-oit-logon	3/21/2013

- Click **Save**.

Note: If you forget to click **Save**, then Active Directory group integration will not work.

As a result, when a user logs on to a monitored server by using the Administrator account, if they enter "user1" or "user2" in the ObserveIT Identification screen, they will not be able to gain access to the desktop, because these users are members of the **no-oit-logon** group. However, if "user3" attempts to authenticate, they will be granted access to the desktop.

- If you want to configure the ObserveIT Identification Service to deny access to all Active Directory groups except those in the **Enable** list:

- Select **Disable all groups from this Active Directory domain**.
- In **Enable: Group**, enter the domain name of the Active Directory group that you want to enable access to the Identification Service, or select it from the list of all the domains in the Active Directory forest in which the ObserveIT Application Server is a member.
- Enter the group name that you want to enable (in this example, **yes-oit-logon**). Click **Add**.

The group name will be verified against the Active Directory domain, therefore you must make sure that the group already exists in the domain.

☒ **Enable all groups from this Active Directory domain.**

To enable specific groups from this domain to log-on, please enter the Active Directory group name (i.e "Help Desk" or "Domain Admins"). You can add multiple groups to this list.

Enable: Group \

Domain/Group	Created Date
☐ OIT-DEMO.LOCAL\yes-oit-logon	3/21/2013

- Click **Save**.

As a result, when "user3" attempts to authenticate, they will be granted access to the desktop, but "user1" and "user2" will not be able to gain access to the desktop, because they are not members of the **yes-oit-logon** group.

Configuring Local ObserveIT Identification Users

After creating Forced-Identification users, you must configure an authentication target. This authentication target can be one or more Active Directory Identification targets (or domains) or Local ObserveIT Identification Users.

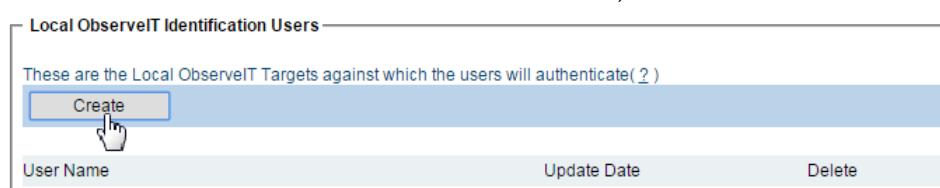
When no central Active Directory is available against which ObserveIT Identification services can authenticate, you will need to use local ObserveIT targets for user authentication.

Note: This feature does NOT create any actual local users. It just configures ObserveIT to check if the credentials of a Forced-Identification user at log on match those of any Local ObserveIT User.

This topic describes how to configure the local ObserveIT targets against which the users will authenticate. (It also describes how to delete local ObserveIT users.)

To configure Local ObserveIT Identification users

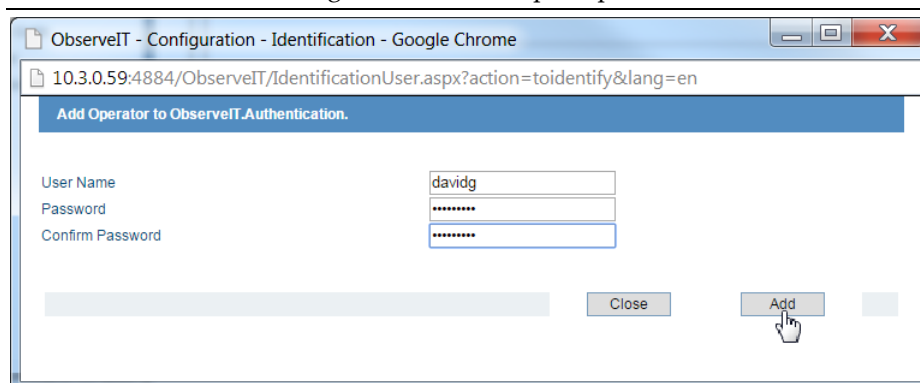
- 1) Navigate to the **Configuration > Identification** page.
- 2) In the **Local ObserveIT Identification Users** section, click **Create**.



The **Add Operator** window opens.

- 3) Type the user name, the required password, and confirm the password. You MUST enter a password.

Note: The user name and password are created locally inside the ObserveIT database, and are not matched against any external source. When a Forced-Identification user logs on to any ObserveIT-monitored server, they must enter this user name and password for secondary authentication in the ObserveIT Windows log on screen/Unix prompts. For details, see [Identification Services](#).



- 4) Click **Add**.
- 5) Repeat steps 2 and 3 for each user that you want to add.

The new Local ObserveIT users are displayed in the **Local ObserveIT Identification Users** section.

Local ObserveIT Identification Users

These are the Local ObserveIT Targets against which the users will authenticate(2)

Create

1 - 3 of 3

User Name	Update Date	Delete
bennynt	1/12/2015	Delete
davidg	1/12/2015	Delete
jamest	1/12/2015	Delete

Note: Local ObserveIT users cannot be modified. If you need to change the user's password or log on name, you must first delete the user, and re-create it.

After configuring the users, whenever a Forced-Identification users logs on to a monitored server, they will be able to use the user name and password credentials that were configured for this Local ObserveIT Identification User for secondary authentication.

In addition, the ObserveIT administrator or security auditor will be able to see exactly who used the Administrator's built-in account by looking at the **Server Diary**, **User Diary**, **Search**, or **Reports** page.

Session Duration	Login	User	Server	Client	Slides	Video
1/11/2015						
2:58 PM - 2:59 PM	Administrator	jamest	WIN2003-OITSRV	WIN2003-DC	49	
2:49 PM - 3:00 PM	Administrator	danielp	WIN2003-OITSRV (local)		58	
12:30 PM - 12:42 PM	Administrator	n/a	WIN2003-OITSRV (local)		107	
12:30 PM - 12:31 PM	Administrator	n/a	WIN2003-OITSRV (local)		1	
1/8/2015						
2:05 PM - 2:56 PM	Administrator	n/a	WIN2003-OITSRV (local)		203	
2:01 PM - 2:03 PM	Administrator	n/a	WIN2003-OITSRV (local)		43	

Deleting Local ObserveIT Users

Important: Deleting a Local ObserveIT user does not have any effect on the actual user object, either in Active Directory or on the Windows Local Users. However, if this user is still listed in the **Forced-Identification Users** section and configured in one or more Server Policies, then since it will not be able to authenticate against any available Local ObserveIT user, that user will NOT be able to log on to the ObserveIT-monitored server. Therefore, take caution before deleting Local ObserveIT users.

To delete a Local ObserveIT user from the list

- 1) Navigate to the **Configuration > Identification** page.
- 2) In the **Local ObserveIT Identification Users** section, click the relevant **Delete** link of the user that you want to delete.

Local ObserveIT Identification Users

These are the Local ObserveIT Targets against which the users will authenticate(2)

Create

1 - 3 of 3

User Name	Update Date	Delete
bennynt	1/12/2015	Delete
davidg	1/12/2015	Delete
jamest	1/12/2015	Delete

A window opens, warning that you are about to delete a Local ObserveIT Identification user.

- 3) Click **OK** to delete the user.

Forced-Identification User Login

After enabling and configuring ObserveIT's Identification Services, Forced-Identification users that log on to the monitored servers will be required to identify themselves with a secondary ObserveIT log on prompt, before they can access a Windows server desktop or a published application.

On Linux/Unix Agents, generic users with shared user accounts (such as "root" or "sysadmin") will be prompted to enter their secondary credentials before they can open an interactive user session on an ObserveIT-monitored Linux/Unix computer.

See the following topics:

- [Windows Secondary Identification Login Example](#)
- [Unix/Linux Secondary Identification Example](#)

Windows Secondary Identification Login Example

The following screen provides an example of the ObserveIT secondary authentication login screen that a Forced-Identification user receives after configuring a Windows machine for secondary authentication.



To log in for secondary authentication

- If the user is a local ObserveIT identification user:
 - a) Select the **Authenticate as ObserveIT user** check box.
 - b) Type a secondary user name and password.
 - c) Click **I Agree**.
- If an Active Directory domain has been configured for the user:
 - a) Type the domain and user name (in the format "domain\username")
 - b) Type the password.
 - c) Click **I Agree**.

Unix/Linux Secondary Identification Example

The following example shows the prompts that a Forced-Identification user receives after configuring a Unix/Linux machine for secondary authentication.

```
File Edit View Search Terminal Help
All activity on this machine is recorded and monitored
Authentication Type:
1. Authenticate as ObserveIT user
2. Domain authentication

Choose Type: 2
Domain: OBSDEV.LOCAL
Username: daniel
Password: █
```

To log in for secondary authentication

1) Select an option per the required type of authentication:

- 1 - Authenticate as ObserveIT user, or
- 2 - Domain authentication

Note: When using domain authentication, the domain name will be displayed by default.

2) Enter a secondary user name and password.

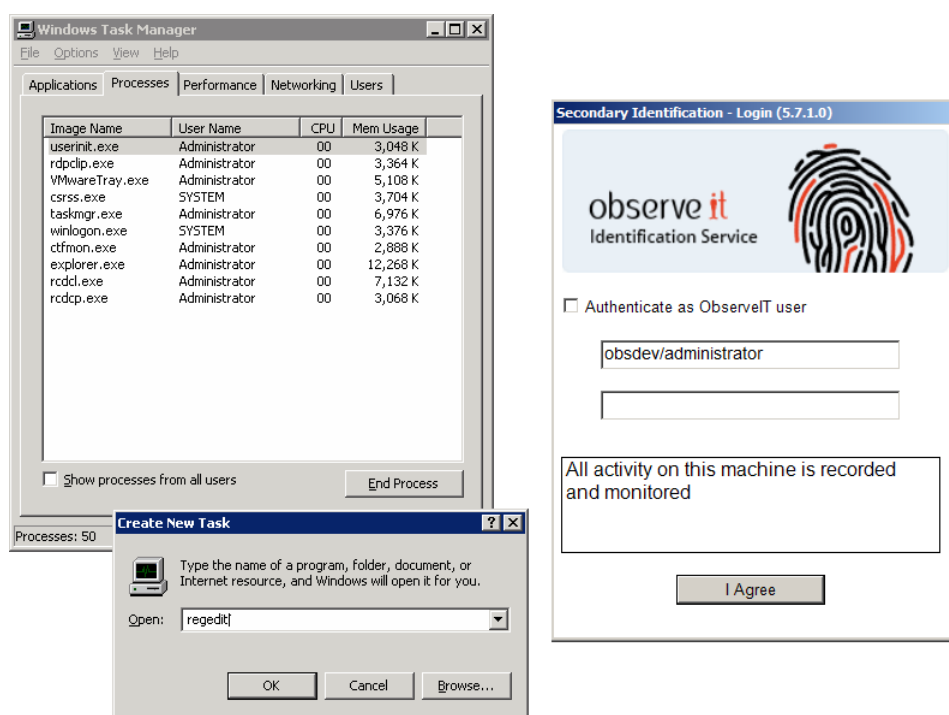
Note: If you enter incorrect credentials, you will be prompted to try again (the initial prompts reappear).

Preventing Windows Users from Bypassing the ObserveIT Identification Prompt

After enabling Identification Services, whenever Forced-Identification users log on to any ObserveIT-monitored server or workstation using the regular Windows logon process, they will be required to provide secondary authentication in the ObserveIT Windows logon screen prompts. For further details, see [Identification Services](#).

If the user enters incorrect credentials, either by mistake or intentionally, they will be presented with the error: "Invalid Credentials or Access Denied". In order to continue, the user must re-enter their credentials.

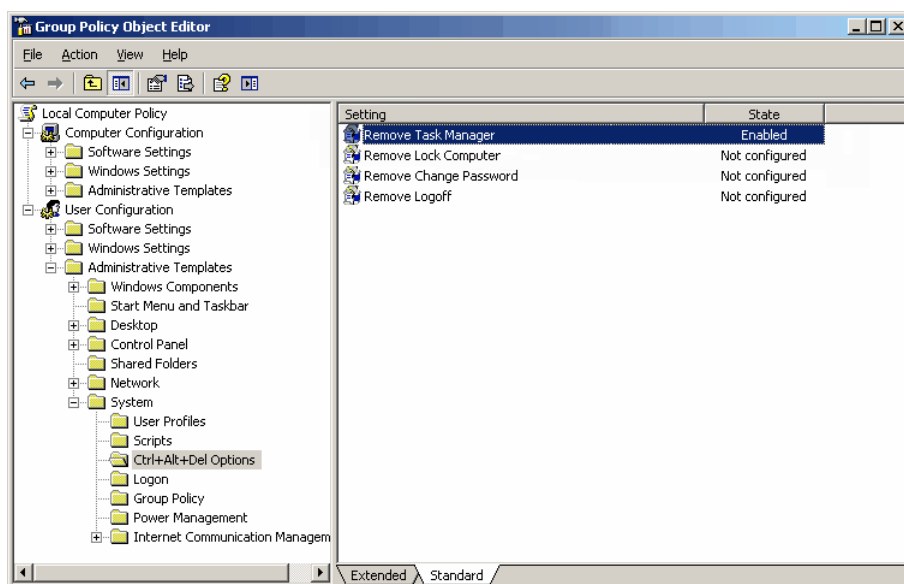
The ObserveIT log on screen or identification prompt is not configured to entirely prevent access to the system; by design, since the user has successfully logged on to the system, the user's identity was already granted the appropriate security token. This means that while the secondary authentication ObserveIT log on screen prompt is still open, waiting for the user's input, the user may be able to press a combination of keys in order to invoke the **Task Manager**. From the **Task Manager**, the user may execute other applications.



Although this may seem like a security flaw, ObserveIT is not designed to work inline with the Windows operating system. It will never prevent a user from logging on to the system, even if they cannot pass the Identification prompt. All the user's actions are still recorded. The only effect is that the user is not identified, for the specific session. Only the Windows log on name is displayed in the **Server** and **User Diaries**, similar to when Identification Services is not enabled.

Session Duration	Login	User	Server	Client	Slides	Video
6/20/2010						
12:31 PM - 12:32 PM	Administrator	n/a	WIN2003-OITSRV	WIN2003-DC	40	
Print this information Print detailed information						
Program Manager						
Windows Task Manager (7)						
Untitled - Notepad (2)						
Create New Task (4)						
My Documents (3)						
C:\Documents and Settings\Administrator\My Documents\Visual Studio 2005 (2)						
Registry Editor						
12:27 PM - 12:31 PM	Administrator	user1	WIN2003-OITSRV (local)		27	

If you need to entirely lock the monitored systems and prevent users from being able to pass the ObserveIT logon screen or identification prompt, you will need to modify the systems security settings and prevent users from being able to run and use the **Task Manager**. This can be done either at the local computer level by using the Local Group Policy, or at the Active Directory domain or Organization Unit (OU) level by using Group Policy Objects (GPOs). For further details, refer to the Microsoft Knowledge Base article: ["Task Manager has been disabled by your administrator" error message](#).



Note: It is beyond the scope of this article to discuss all the security considerations, requirements, best practices and implementation procedures for the system.

Servers

In ObserveIT terminology, servers are the computers on which the ObserveIT Agents are installed, and which are being monitored and recorded.

The **Configuration > Servers** tab displays a list of all the servers and related details.

Server Name	Server Policy	Version	Status	Installation	Last Activity
W2K8-2	Default Windows-based ...	5.8.0.0	OK	12/18/2014	12/18/2014
W2K8-S8-QA10	Default Windows-based ...	5.8.0.0	OK	12/18/2014	12/18/2014
c59-32-7	Default Unix-based Policy		Uninstalled	12/18/2014	12/18/2014

In the **Servers** page, administrators can:

- [View servers](#) and related details including server name, linked Server Policy, version number of the Agent software installed on the server, status of the server, installation date of the Agent software, and date of the last activity reported by the Agent installed on the server.
You can change the Server Policy that is linked to a server, and make manual changes to each server. If the names of physical Windows servers were changed, you can also change the ObserveIT server names to match the new machine names.
- [Filter servers](#) to easily find the server you are looking for, from among the many servers that your organization has.
- [Rename servers](#)
- [Unregister servers](#)
- [Unlink a Server Policy from servers](#)
- [Configure server settings](#)

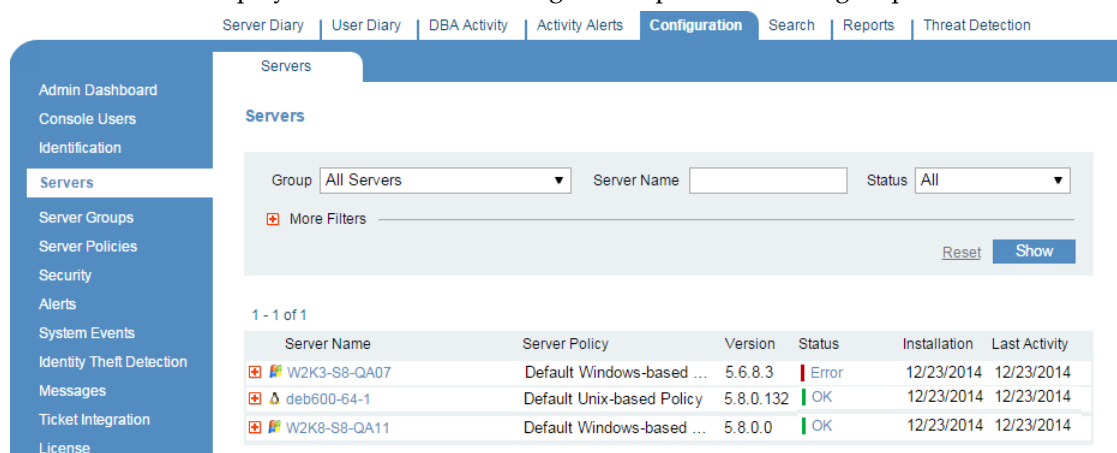
Viewing Servers

In the **Servers** list, you can view a list of servers and details related to the servers and to the Agents installed on the servers.

To view servers

- 1) Navigate to **Configuration > Servers**. (You can also access this page from the **Admin Dashboard** by clicking various links: In the **Agents** portal, the Agent group name, the error number, the **Tampered With** or **Data Loss** icons, and in the **Deployed Agent Versions** portal, the recently **Installed** or **Uninstalled** Agents.)

The **Servers** list displays the servers, according to the specified server group and filter criteria.



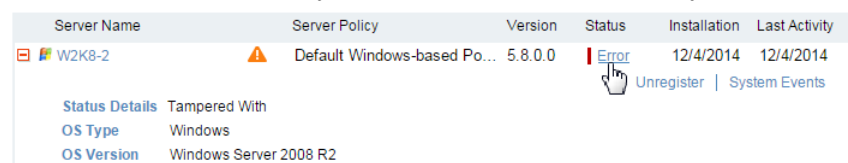
For each server, the **Servers** list displays the following details:

- **Server Name**
- **Server Policy** to which the server is linked
- **Version** of the Agent software installed on the server
- **Status** and **colored severity bar** indicate the event/operational status and severity level (Red (High)=Error, Orange (Medium)=Unreachable/Disabled, Green (Normal/Active)=OK, Blue (Low/Administrative)=Unregistered/Uninstalled). (See also [Colored Severity Levels and Icons](#) in the **Admin Dashboard** section.)
- **Installation** date of the Agent software
- **Last Activity** - date of the last activity that was reported by the Agent installed on the server

2) You can expand a server to view more details.

The details vary per the server status. The **Status Details** field appears only when the status is not "OK". **OS Type** and **OS Version** appear for many statuses.

For example, the following figure displays "Error" status, and **Status Details** displays "Tampered With". The colored severity bars indicate the event severity level (for example, Red=High).



- 3) You can drill down to examine the system events that occurred on the server in order to understand the root cause of the errors and what corrective actions to perform. You can click the **System Events** link to view all system events, or you can click the **Error** link to view the event in the (filtered) **System Events** list where you can view expanded details, including **Additional Info**. For details, see [Investigating System Events](#) and [Viewing System Events](#).
- 4) To unregister the server, you can click the **Unregister** link. For details, see [Unregistering Servers](#).
- 5) You can filter the **Servers** list according to specified criteria (including the server group, name, status, activities which occurred on the server within the past 7 days). For details, see [Filtering Servers](#).

Filtering Servers

You can filter the servers displayed in the **Servers** list per specified criteria.

To filter the servers displayed in the Servers list

- 1) From the **Group** drop-down list (at the top of the **Servers** page), select the server group for which you want to view servers (All Servers, Active Servers, Windows Servers, Unix Servers, Windows Workstation, Windows Gateway, Windows ActiveX, and so on). By default, **All Servers** are displayed.

- 2) From the **Server Name** drop-down list, select the name of the server you want to view.
- 3) From the **Status** drop-down list, select the status of the servers that you want to view (or select **All** to view all).
- 4) Expand the **More Filters** section by clicking  to filter the servers displayed according to additional criteria, as described in the table below.
- 5) When you have finished defining your search criteria, click **Show** to update the server list according to the specified details.

To clear the filter fields, click **Reset**.

More Filters

Filter	Description
Server Policy	To search for servers by policy, select an option from the list or select All to view all servers. Options include: • Manual • Default Metadata Only Policy • Default Recording Disabled Policy • Default Unix-based Policy • Default Windows-based Policy
OS Type	To search for servers by operating system type, select an option from the list (Windows or Unix), or select All to view all servers.
Version	To search for servers by ObserveIT version number or by the Installed version (or select All to view all server versions.
Activities	To search for servers on which particular activities occurred within the past 7 days, select the check box(es) of one or more options from the list: • Data Loss: to search for servers which incurred data loss within the past 7 days • Tampered With: to search for servers that were tampered with within the past 7 days • Installed: to search for servers that were installed within the past 7 days • Uninstalled or Unregistered: to search for servers that were uninstalled or unregistered within the past 7 days
Agent Type	To search for servers by type, select an option from the list (Workstation, Servers, Terminal Services, Site, Unix, ActiveX) or select All to view all servers.
OS Version	To search for servers by operating system version, select an option from the list (CentOS 5.9, Red Enterprise, Windows Server 2008 R2), or select All to view all servers.
Status Details	To search for servers by status details, select an option from the list (Service Stopped, Service Terminated , and so on), or select All to view all servers. For details, see Assessing Agent Statuses and Details .

Renaming Servers

When required, you can rename servers.

To modify a server name

- 1) Navigate to **Configuration > Servers**.
- 2) In the **Servers** list, click the name of the server you want to modify.

- 3) In the server's properties page, in the **Server** section, click the **Modify Name** link next to the server's name.

Server Diary | User Diary | DBA Activity | Activity Alerts | **Configuration** | Search | Reports | Threat Detection

Servers

W2K8-S8-D02 (5.8.0.0)

[Back to Servers List](#) Cancel Save

Currently, server is linked to the Default Windows-based Policy configuration policy.
In order to enable the Save button you must first [unlink the policy](#).

Server

Server ID	1497b10c-4eeb-4512-9b82-4b4ca368770c
Server Name	W2K8-S8-D02 [Modify Name]
Server Policy Template	Default Windows-based Policy [Change Template]
App. Server	http://127.0.0.1:4884/ObserveITApplicationServer
Enable recording	☒
Enable Identity Theft Detection	☐
Enable API	☐

The **Change Server Name** window opens.

Change Server Name

Warning: Changing the Server name has no impact on the actual Windows Server name, but can be used when actual Windows Server name has to be changed, and you wish to match the new name with the ObserveIT data

Server ID 1497b10c-4eeb-4512-9b82-4b4ca368770c

Server Name

Cancel Update

- 4) Type the new **Server Name**.
- 5) Click **Update**.

The server name is modified.

Unregistering Servers

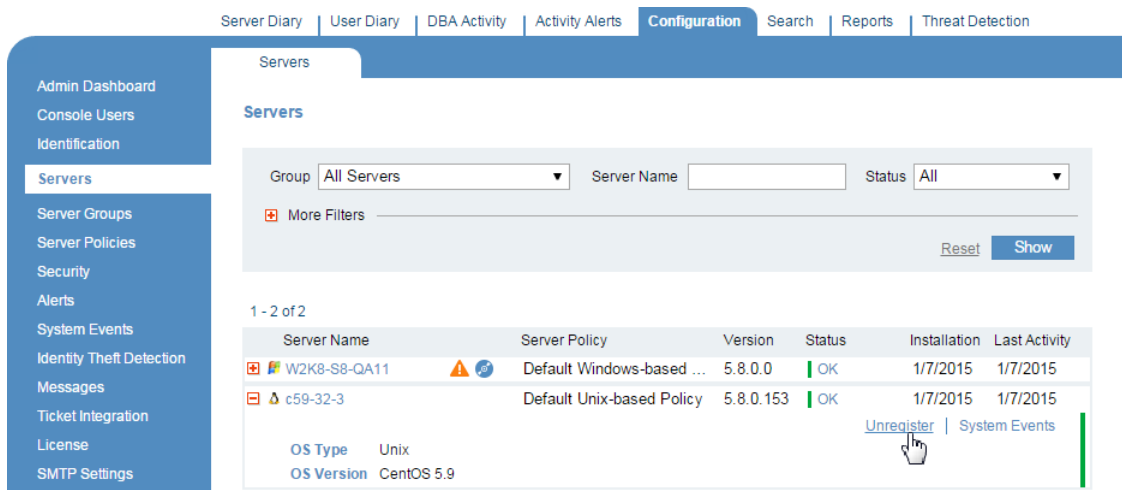
In some cases, an ObserveIT server needs to be uninstalled from specific computers. For example, if the last activity occurred on a server a long time ago, the administrator may decide that a license is no longer required for that server. The correct way to uninstall a server is by using the **Add/Remove Programs** applet in the **Control Panel**. However, there may be times when access to the monitored server is not possible, and you need to stop a specific Agent from working. In addition, you may need to free one or more licenses to be able to install the Agent(s) on additional machines.

In these cases, you can "unregister" the server from the **Servers** list. Unregistering a server will NOT actually uninstall the Agent software on that machine. You will still need to remove the Agent software. Unless you manually uninstall the Agent software, each time a user logs on to the once-monitored machine, the following error message will be displayed: "The ObserveIT Agent was unregistered by the administrator. Please manually uninstall the Agent software from this computer by using the Add/Remove Programs applet in the Control Panel."

The unregistered server's data is still retained inside the database, and you can perform searches and watch recorded sessions from these servers.

To unregister a server

- 1) In the **Configuration > Servers** page, click  next to the server that you want to unregister and click the **Unregister** link (located on the right of the expanded details).



The screenshot shows the ObserveIT Configuration > Servers page. The left sidebar contains navigation links: Admin Dashboard, Console Users, Identification, Servers (selected), Server Groups, Server Policies, Security, Alerts, System Events, Identity Theft Detection, Messages, Ticket Integration, License, and SMTP Settings. The main content area shows the Servers list with filters for Group (All Servers), Server Name, and Status (All). Below the filters is a table with 2 servers. The second server, c59-32-3, is selected, and its details are expanded, showing OS Type (Unix) and OS Version (CentOS 5.9). The Unregister link is highlighted with a mouse cursor.

Server Name	Server Policy	Version	Status	Installation	Last Activity
W2K8-S8-QA11	Default Windows-based ...	5.8.0.0	OK	1/7/2015	1/7/2015
c59-32-3	Default Unix-based Policy	5.8.0.153	OK	1/7/2015	1/7/2015

OS Type: Unix
OS Version: CentOS 5.9

Unregister | System Events

A message is displayed, prompting you to acknowledge your action.

- 2) Click **OK** to proceed.

The Agent version is changed to **Uninstalled** and the status is changed to **Disabled**.

This frees up one license, allowing you to use that license to install an Agent on a new machine.

Unlinking a Server Policy from Servers

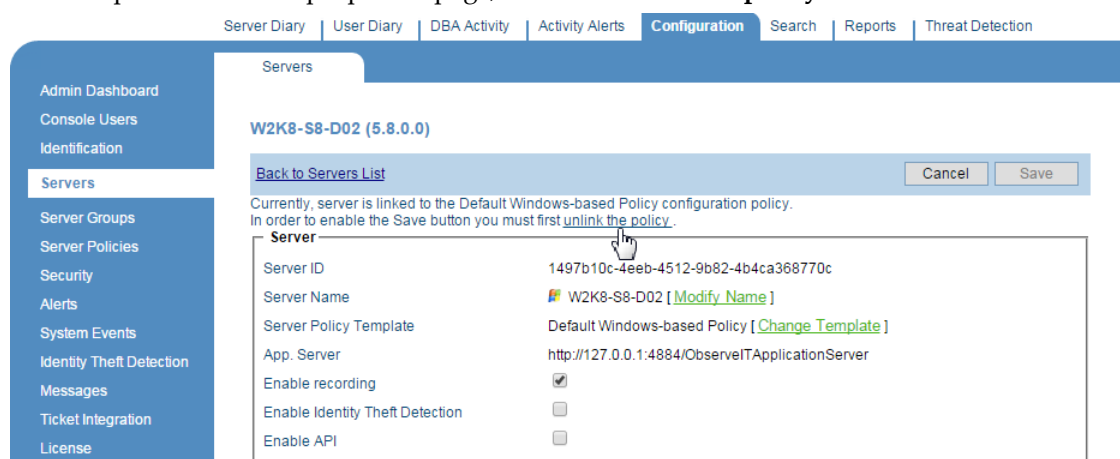
By default, all the servers are automatically configured by the Default Server Policy Template. Any change to that Server Policy will affect all linked servers. You can link a different Server Policy to individual servers or to server groups.

When you are making changes to the configuration of just one server, you may want to manually change the settings on that particular server, and not create a new Server Policy just for that purpose. When doing so, the Server Policy that was previously linked to that server will be unlinked, and the server status will change to "Manual".

When the server is linked to any Server Configuration Policy, the **Save** button is disabled. To enable the **Save** button, you must first unlink the Server Configuration Policy from the server.

To unlink a Server Policy from a server

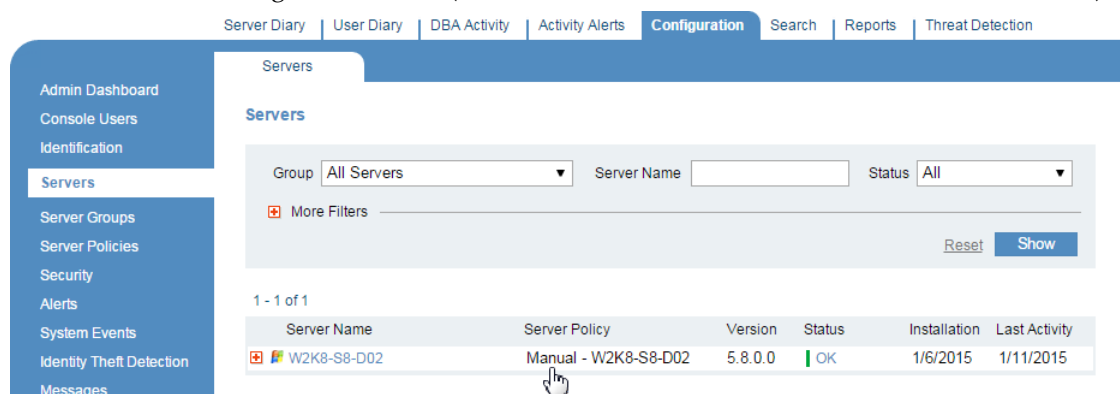
- 1) Navigate to **Configuration > Servers**.
- 2) In the **Servers** list, click the name of the server for which you want to unlink the Server Policy.
- 3) At the top of the server's properties page, click the **unlink the policy** link.



A message is displayed, prompting you to acknowledge your action.

- 4) Click **OK** to proceed.
- 5) After unlinking the policy, you can make changes to the server configuration. When you have finished, click **Save**.

The server mode changes to **Manual** (as shown next to the relevant server in the **Servers** list).



You can link the server to any Server Configuration Policy at any time.

Configuring Server Settings

By default, all servers are automatically configured by one of the default Server Policy Templates. Server Policies are sets of configuration options that control aspects of how a monitored server is configured. Any change to a Server Policy will affect all linked servers. However, you can also manually change server configuration settings for individual servers. To change the configuration settings for an individual server, you must first "unlink" the server from the Server Policy to which it was linked; as a result, the server status will change to "Manual".

As a general rule, it is recommended to use Server Policies, which makes the task of configuration much easier. By using Server Policies, the administrator can configure one set of recording settings, and apply these settings to many monitored servers at the same time.

Server settings can apply to Windows-based server policies, Unix-based server policies, or both Windows and Unix-based server policies.

The following settings can be configured on individual servers or on multiple servers.

Windows-Based Server Policies

- Enabling Agent API
- Showing/Hiding the Agent tray icon
- Restricting recording to RDP sessions
- Enabling hotkeys
- Enabling key logging
- Optimizing screen capture data size
- Setting the image format (recording in color or grayscale)
- Setting keyboard recording frequency
- Setting continuous recording
- Application recording policy

Unix-Based Server Policies

- Data recording policy
- Agent logging and debugging
- Memory management

Windows and Unix-Based Server Policies

- Enabling Agent recording
- Enabling Identity Theft Detection
- Enabling recording notification
- Setting session timeout
- Offline recording policy
- Identification policy
- User recording policy

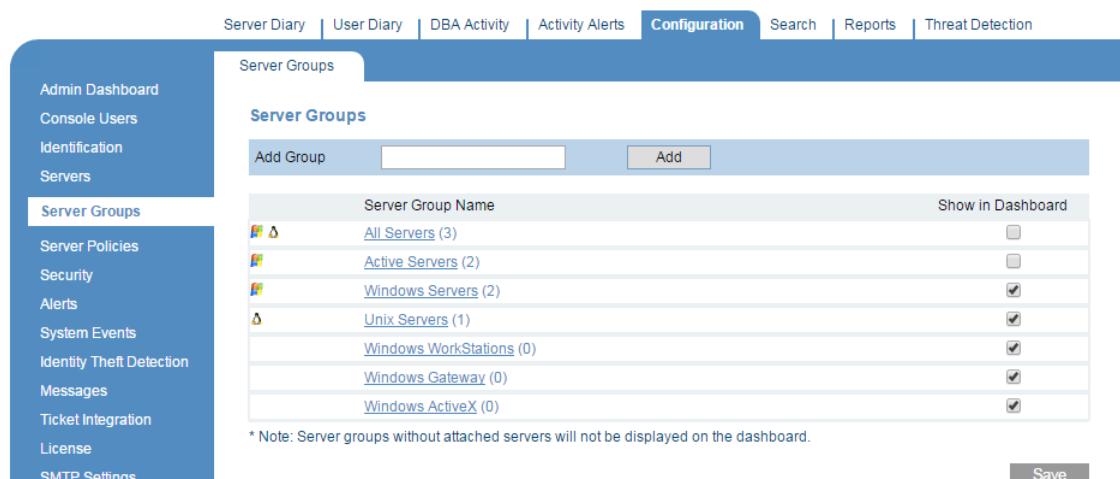
Note: The policy settings that you can configure on an individual server are identical to the policy settings that you can configure for any Server Policy Template. For further details on how to configure policy settings on an individual server or on multiple servers simultaneously, see [Configuring Server Policy Settings](#).

Server Groups

In ObserveIT, you can use server groups to apply management and configuration features simultaneously to several servers.

In ObserveIT terminology, servers are the computers on which the ObserveIT Agents are installed, and which are being monitored and recorded.

In the **Configuration > Server Groups** page, you configure the ObserveIT server groups.



The default server groups include:

- **All Servers:** This group includes all the servers on which the ObserveIT Agent is installed.
- **All Active Servers:** This group includes all servers that are installed with the ObserveIT Agent, but unlike the **All Servers** group, it only includes servers that are currently configured to be active.
- **All Windows Servers:** This group includes all the servers that are running any version of the Microsoft Windows operating system, and that have the ObserveIT Agent installed on them.
- **All Unix Servers:** This group includes all the servers that are running supported versions of the Unix/Linux operating system, and that have the ObserveIT Agent installed on them.
- **Windows Workstations:** This group includes all the servers that are running the Microsoft Windows 8 operating system, and that have the ObserveIT Agent installed on them.
- **Windows Gateway:** This group includes all the servers that are running the Microsoft Windows Server Gateway, and that have the ObserveIT Agent installed on them.
- **Windows ActiveX:** This group includes all the servers that are running the Microsoft Windows ActiveX, and that have the ObserveIT Agent installed on them.

These server groups cannot be deleted, and you cannot modify their members. However, you can create additional server groups.

You can use server groups to configure permissions for Console Users. You can also use server groups to manage Configuration Policies. For further details, see [Server Policies](#).

In the **Configuration > Server Groups** page, you configure the ObserveIT server groups as follows:

- 1) [Create new server groups](#).
- 2) [Modify members of the server groups](#).
- 3) [Assign Console Users permissions for the required server groups](#).
- 4) [Link Server Policies to server groups](#).

You can also delete server groups.

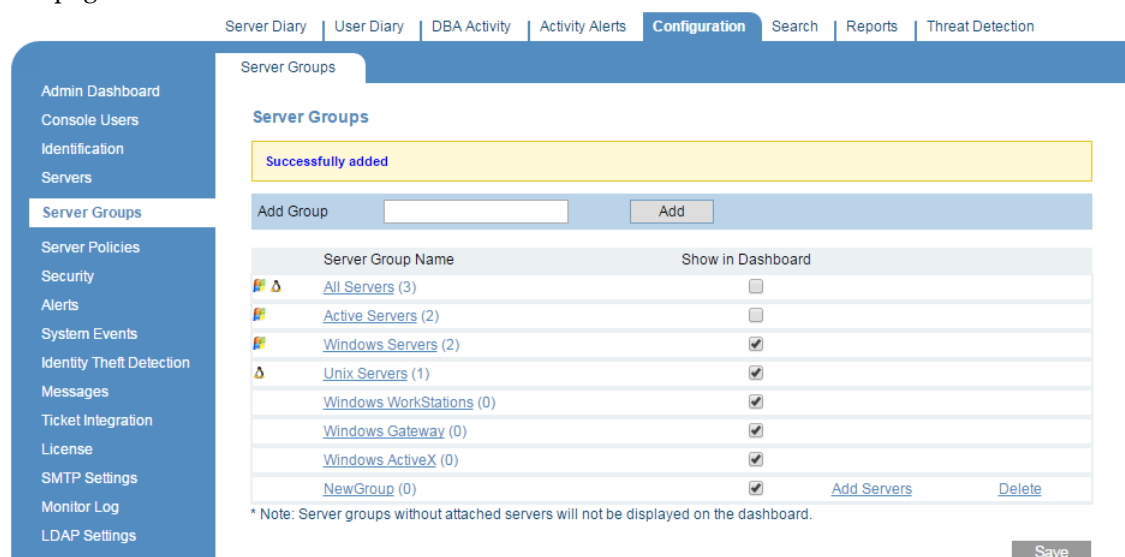
Creating Server Groups

You can use the default built-in server groups. You can also create additional server groups, if required.

To create an additional server group

- 1) Navigate to **Configuration > Server Groups**.
- 2) In the **Add Group** field, type the relevant server group name.
- 3) Click the **Add** button.

The new server group is added to the list. A successful confirmation message appears at the top of the page.



- 4) By default, the **Show in Dashboard** check box is selected, and the new server group is automatically displayed in the **Admin Dashboard** (in the **Agents** portal).

To remove a server group from the **Admin Dashboard**, clear the **Show in Dashboard** check box next to the relevant server group (in the **Server Groups** page).

Modifying Members in Server Groups

You can add and remove servers from server groups, and you can modify group member properties.

To modify the members within a server group

- 1) Navigate to **Configuration > Server Groups**.

Note: The default server groups cannot be deleted, and you cannot modify their members.

- 2) To add servers to a server group, click the **Add Servers** link next to the relevant server group name.

The **Add Servers to Group** window opens.

Server Name	Version	Monitor Status
c59-32-7	Uninstalled	Disabled
W2K8-2	5.8.0.0	Active
W2K8-S8-QA10	5.8.0.0	Active

- 3) Select the relevant check boxes of the servers that you want to add to the server group. You can also use the **Check All** and **Clear All** links.

Note: Servers that are already members of this server group will NOT appear in the **Add Servers to Group** window. Only servers that are currently not members of this server group will be available for selection.

- 4) Click the **Add Checked Servers** button.

- 5) When you have finished, click **Close**.

A message is displayed, prompting you to acknowledge the action.

- 6) Click **OK** to proceed.

The **Server Groups** page displays the number of member servers next to the server group's name.

- 7) To view current members in a server group, click the relevant server group's link.

The **Servers** page opens, filtered to display the relevant server group and its members. (The **Group** field displays the name of the server group, and the **Servers** list displays the group members.) You can manually change the group (in the **Group** drop-down list) to match your requirements to view the relevant servers.

- 8) To modify a member's properties, in the **Servers** list, click the name of the server you want to modify.

- 9) In the server's properties page, edit the relevant fields, and click **Save** to save the changes.

To remove a server from the server group

- 1) In the **Servers** list, click  next to the server that you want to remove, and click the **Remove** link (located on the right of the expanded details).

Server Name	Server Policy	Version	Status	Installation	Last Activity
W2K8-S8-D02	Default Windows-based ...	5.8.0.0	OK	1/6/2015	1/6/2015

A message is displayed, warning that you are about to remove a server from a server group.

- 2) Click **OK** to proceed.

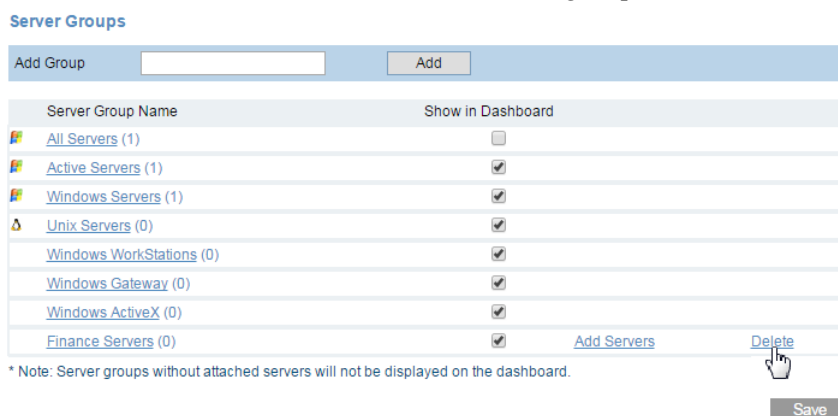
The server is removed from the server group.

Note: Removing servers from a server group may affect the permissions that are assigned to one or more Console Users. In such a case, a Console User might not be able to access these servers anymore.

Deleting Server Groups

To delete a server group

- 1) Navigate to **Configuration > Server Groups**.
- 2) Click the **Delete** link next to the relevant server group name.



A message is displayed, prompting you to confirm the deletion.

- 3) Click **OK** to proceed.

The server group is deleted. The related servers are no longer associated with the group.

Note: The servers that were members of the deleted group will not be deleted. However, deleting a server group may affect the permissions that are assigned to one or more Console Users. In such a case, a Console User might not be able to access these servers anymore.

Server Policies

In ObserveIT terminology, Servers (or Agents) are the computers on which the ObserveIT Agents are installed, and which are monitored and recorded. Servers (or Agents) are configured by using Server Policies. Server Policies are sets of configuration options that control aspects of how the monitored server is configured. By using Server Policies, the administrator can easily configure one set of recording settings, and apply these settings to one or many monitored servers at the same time.

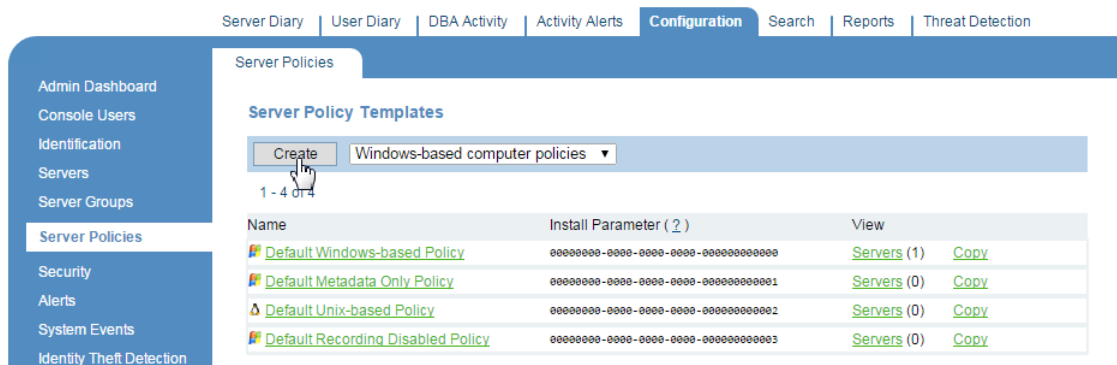
The default Server Policy Templates include:

- Default Windows-based Policy
- Default Metadata Only Policy
- Default Unix-based Policy
- Default Recording Disabled Policy

By default, all the Windows-based Servers (or Agents) are automatically configured by the Default Windows-based Policy, and all Unix/Linux-based Servers (or Agents) are automatically configured by the Default Unix-based Policy. Any changes to these Server Policies will affect all respective linked machines.

The Metadata Only and Recording Disabled Policies were created to ease the deployment of the API-controlled Agents, and to provide an easy method of recording Metadata-only sessions. By default, no Agents are linked to these Policies.

The **Configuration > Server Policies** tab allows you to view all the Server Policy Templates, change settings in policies, copy and delete them, as well as configure and link ObserveIT Servers and Server Groups to these policies.



See the following topics:

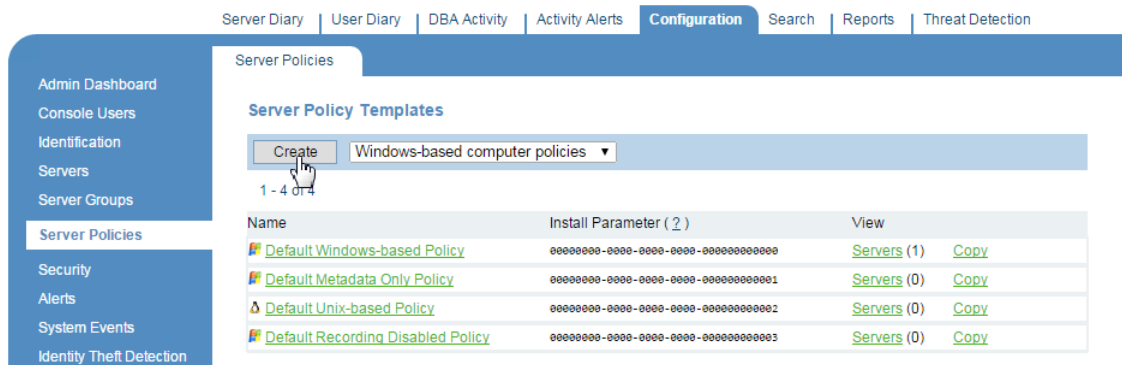
- [Creating Server Policies](#)
- [Modifying Server Policies](#)
- [Deleting Server Policies](#)
- [Linking Servers to Server Policies](#)
- [Linking Server Groups to Server Policies](#)

Creating Server Policies

To create an additional Server Policy

- 1) Navigate to **Configuration > Server Policies**.

The **Server Policy Templates** page opens.

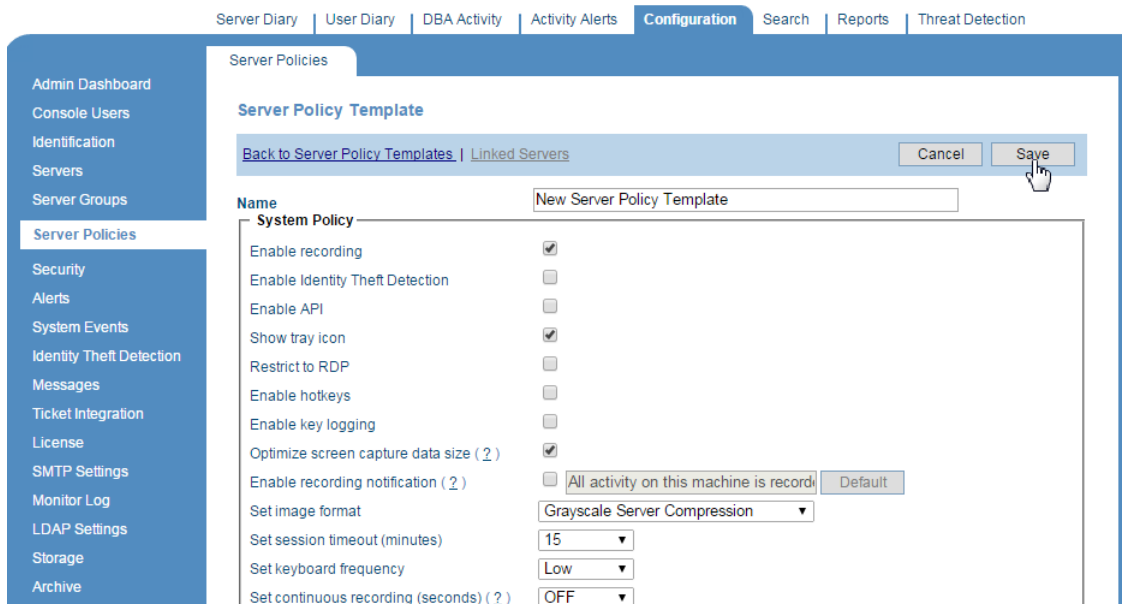


- 2) From the drop-down list, select the type of policy you want to create.
- 3) Click **Create**.

The new Server Policy is created immediately.

Note: You can also copy an existing Server Policy by clicking the **Copy** link next to the policy you want to copy.

The new Server Policy's properties page opens, allowing you to make changes to the new policy.



- 4) Type a descriptive **Name**.
- 5) Configure the fields, as required. (For further details, see [Configuring Server Policy Settings](#).)
- 6) Click **Save**.

The new Server Policy appears in the **Server Policy Templates** list.

Modifying Server Policies

To modify a Server Policy

- 1) Navigate to **Configuration > Server Policies**.
- 2) In the **Server Policy Templates** list, click the **Server Policy Template** name.

The relevant **Server Policy Template** properties page opens.

- 3) Edit the fields, as required. (For further details, see [Configuring Server Policy Settings](#).)
- 4) Click **Save** to save your changes to the Server Policy.

Note: Each Server polls its Application Server at the beginning of each new session or every 15 minutes to check for new configuration settings. To expedite the changes you have made to the linked Server Policies Template, ask the user that is currently logged on to that computer to log off and log on.

Deleting Server Policies

Note: Before deleting a Server Policy, look at the servers' count in the **View** column of the **Server Policies Templates** window. If the count is 0 (zero), this means that no server is linked to this policy. However, if the servers' count is higher than zero, all servers that are linked to the Server Policy you are about to delete will no longer be linked to it, and their status will turn to "Manual". You can view the linked servers by clicking the **Servers** link.

To delete a Server Policy

- 1) Navigate to **Configuration > Server Policies**.
- 2) In the **Server Policy Templates** list, click the **Delete** link next to the Server Policy that you want to delete.

Note: The default policies cannot be deleted.

The screenshot shows the 'Server Policies' section of the configuration interface. On the left is a sidebar with navigation links: Admin Dashboard, Console Users, Identification, Servers, Server Groups, Server Policies (selected), Security, Alerts, System Events, Identity Theft Detection, Messages, and Ticket Integration. The main content area is titled 'Server Policy Templates' and includes a 'Create' button and a dropdown menu set to 'Windows-based computer policies'. Below this is a table listing 6 templates. The first three are default policies (Default Windows-based Policy, Default Metadata Only Policy, Default Unix-based Policy) and the last three are user-defined templates (Default Recording Disabled Policy, New Server Policy Template, Test Server Policy Template). Each row shows the Name, Install Parameter (ID), and View column with links for Servers, Copy, and Delete. A mouse cursor is hovering over the 'Delete' link for the 'Test Server Policy Template'.

Name	Install Parameter (?)	View
Default Windows-based Policy	00000000-0000-0000-0000-000000000000	Servers (1) Copy
Default Metadata Only Policy	00000000-0000-0000-0000-000000000001	Servers (0) Copy
Default Unix-based Policy	00000000-0000-0000-0000-000000000002	Servers (0) Copy
Default Recording Disabled Policy	00000000-0000-0000-0000-000000000003	Servers (0) Copy
New Server Policy Template	0fe9ee2-b6e9-46fa-99c9-22f1d8e93b56	Servers (0) Copy Delete
Test Server Policy Template	060c3fe2-6695-4fbb-870d-b309f529edb1	Servers (0) Copy Delete

Linking Servers to Server Policies

By default, all the Servers (or Agents) are automatically configured by one of Default Server Policies, either the Windows-based Policy or the Unix-based Policy. You can change this and link Servers (or Server Groups) to a different Server Policy Template.

Note: Only one Server Policy Template can be linked to a Server at any given time. If a different Server Policy Template is linked to the same Server, the previous Server Policy Template will be unlinked from the Server immediately, and the new Server Policy Template will be linked to it instead.

There are two ways of linking a Server to a Server Policy Template:

- 1) From the Server Policy Templates list.
- 2) From the Server properties page.

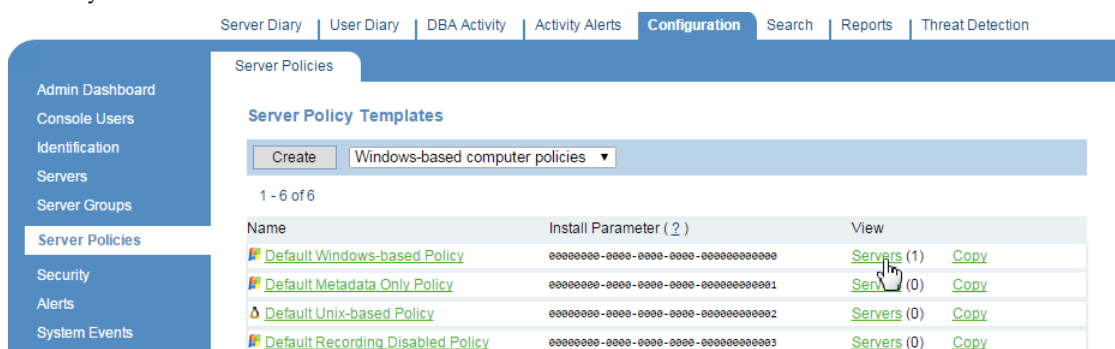
See the following topics:

- [Linking a Server to a Server Policy Template from the Server Policy Templates List](#)
- [Linking a Server to a Server Policy Template from the Server Properties Page](#)

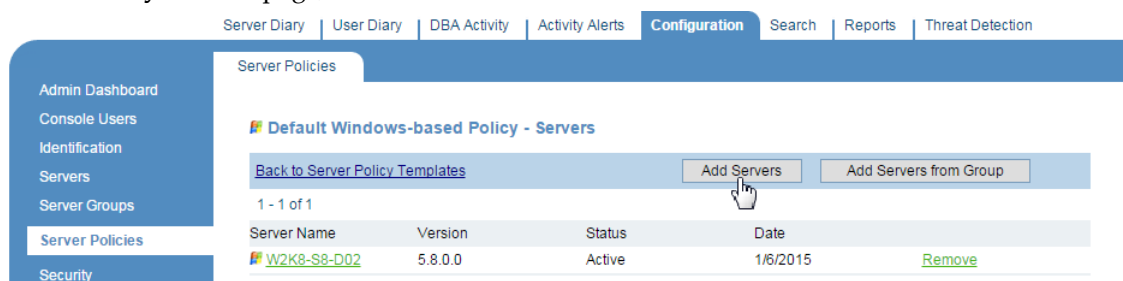
Linking a Server to a Server Policy Template from the Server Policy Templates List

To link Servers to a Server Policy

- 1) Navigate to the **Configuration > Server Policies**.
- 2) In the **Server Policy Templates** list, click the **Servers** link next to the relevant Server Policy to which you want to link the servers.



- 3) In the **Policy Servers** page, click the **Add Servers** button.

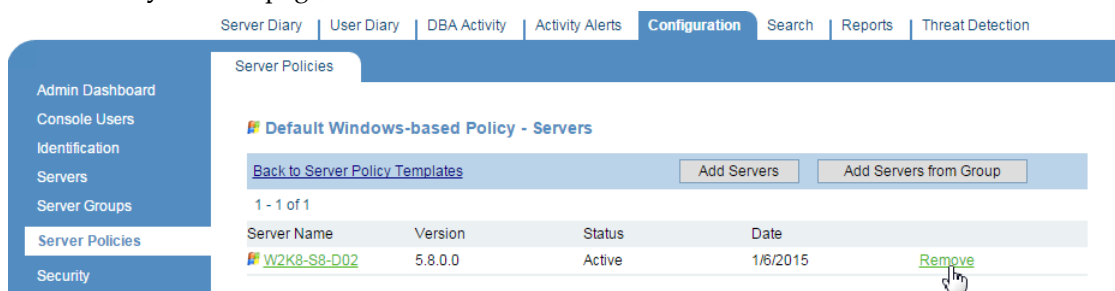


- 4) In the **Servers List Add Servers to Group** window, select the check boxes next to the Servers you want to add to the list. You can also use the **Search** box to find specific Servers.
- 5) Click the **Add Checked Servers** button.
- 6) Click **OK** to proceed.

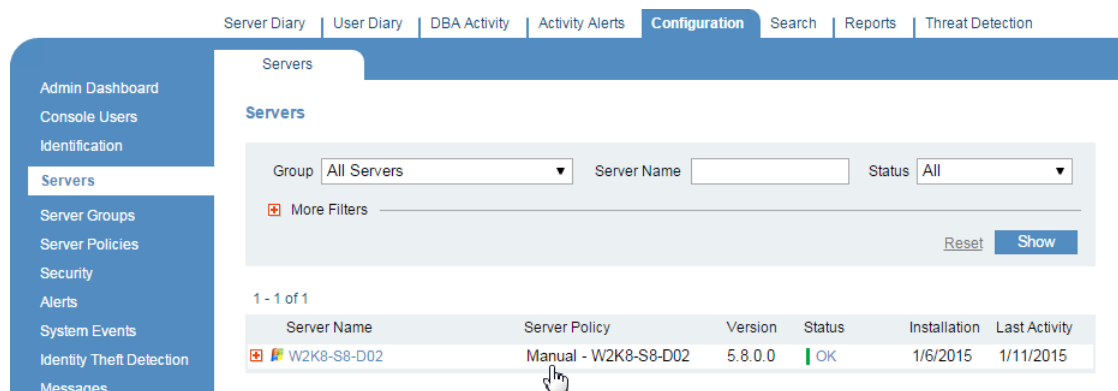
The Server appears in the **Policy Servers** page.

To remove a Server from the list of linked servers

- In the **Policy Servers** page, click the **Remove** link next to the relevant Server name.



Note: Because you are unlinking a Server and not linking it to any other Server Policy Template, the status of the unlinked Server will change to "Manual".

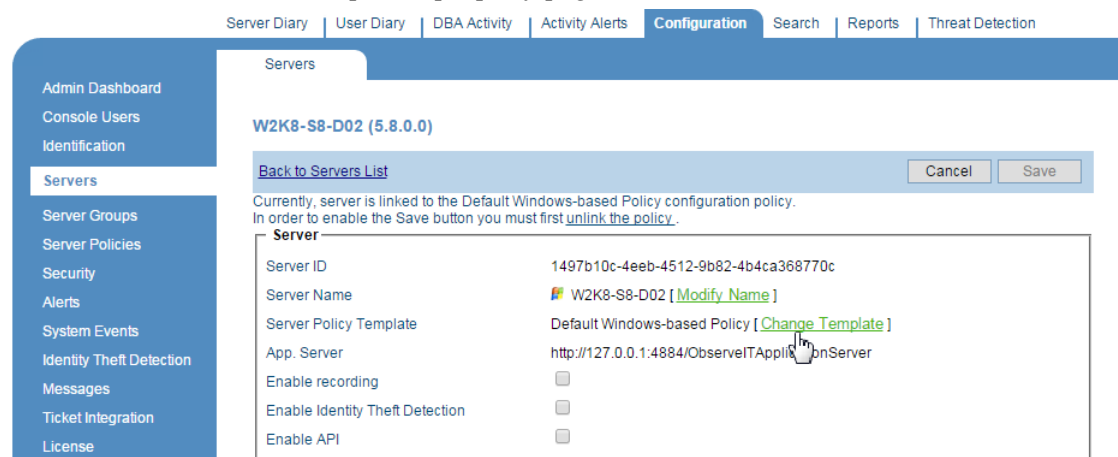


Linking a Server to a Server Policy Template from the Server Properties Page

When a Server is linked to a Server Policy Template, the name of the template is visible in the **Servers** list page, and in the Server's property page.

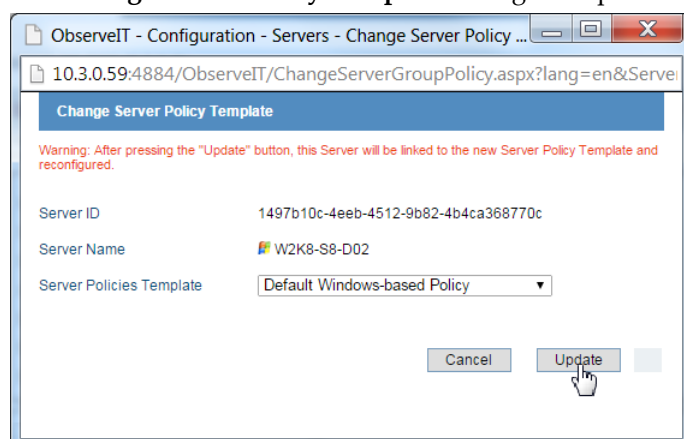
To link a Server to a Server Policy

- 1) Navigate to **Configuration > Servers**.
- 2) Click the relevant server to open its property page.



- 3) Click the **Change Template** link.

The **Change Server Policy Template** dialog box opens.



- 4) From the **Server Policies Template** drop-down list, select the required Server Policy Template.
- 5) Click **Update**.

The server is now linked to the Server Policy.

Linking Server Groups to Server Policies

By default, all the servers (or Agents) are automatically configured by the Default Server Policy Template. However, you can change this and link Servers Groups (or Servers) to a different Server Policy Template.

Note: Only one Server Policy Template can be linked to a server at any given time. If a different Server Policy Template is linked to the same server, the previous Server Policy Template will immediately be unlinked from the server, and the new Server Policy Template will be linked to it instead.

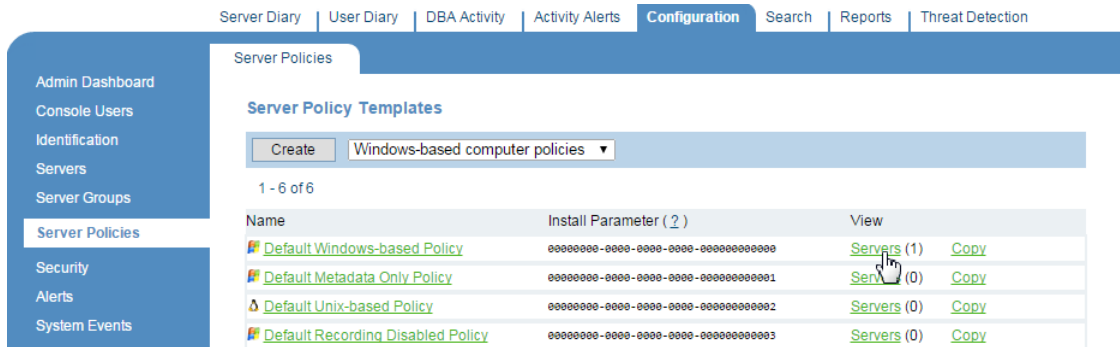
Unlike linking individual servers, by using Server Groups you can perform a mass linking of all the servers that are members of that Server Group.

The process of linking servers to Server Policy Templates by using Server Groups is slightly different than linking specific servers. Unlike linking servers, usage of Server Groups actually performs a batch operation in the background, linking all servers that were members of that Server Group to the Server Policy Template you selected. The Server Group in itself is NOT linked to the Server Policy Template. If, at a later time, you add more servers to that Server Group, they will NOT be linked to the Server Policy Template. To make sure that you have all the servers that are members of that Server Group linked to that Server Policy Template, you will need to repeat this process. Any unlinked servers that are members of that Server Group will then be linked to that Server Policy Template.

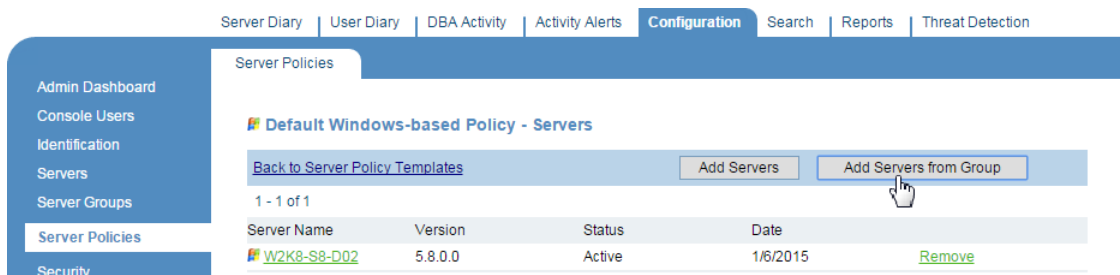
To link a Server Group to a Server Policy

- 1) Navigate to **Configuration > Server Policies**.

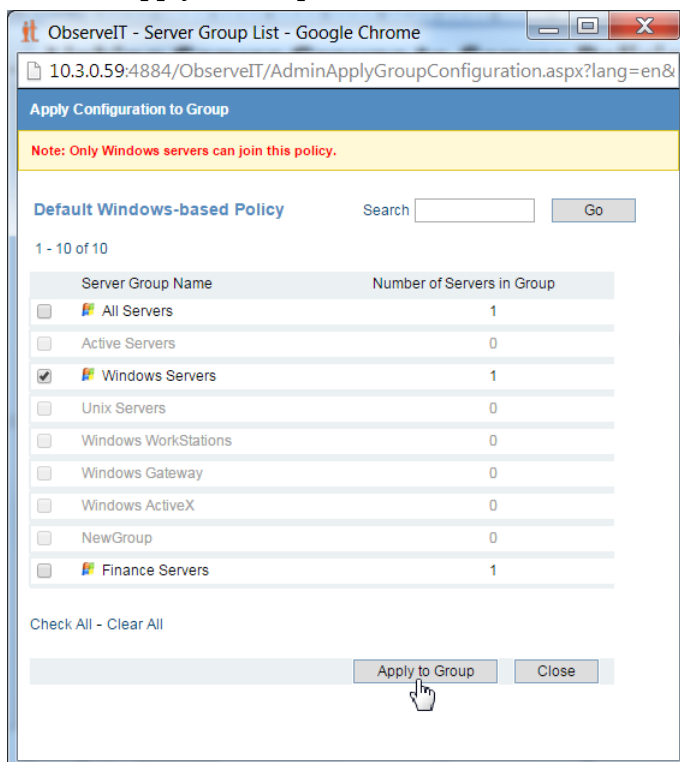
- 2) In the **Server Policy Templates** page, click the **Servers** link next to the Server Policy to which you want to link.



- 3) In the **Policy Servers** page, click the **Add Servers from Group** button.



- 4) In the **Server Group List Apply Configuration to Group** window, select the check box of the required Server Group.
- 5) Click the **Apply to Group** button.



The **Policy Servers** page refreshes, displaying the new linked servers.

Note: You can unlink individual servers from this Server Policy Template, either from the **Server Policy Templates** list, or from the **Server** properties page.

Configuring Server Policy Settings

ObserveIT Servers (or Agents) are configured by using Server Policies. Server Policies are sets of configuration options that control aspects of how the monitored server is configured. By using Server Policies, the task of configuration is simplified since the administrator can configure one set of recording settings, and apply these settings to many monitored servers simultaneously.

Note: You can link a different Server Policy to individual servers or to Server Groups.

Important Notes:

- The policy settings that you can configure on a Server Policy Template are identical to the policy settings that you can configure on an individual server. The topics in this section describe how to configure policy settings using Server Policy templates. Note that setting changes will take effect on new user sessions, after the current sessions are closed. For information about configuring policy settings on an individual server, see [Configuring Server Settings](#).
- Any modifications you make in a server policy can be viewed for auditing purposes in the **Configuration Changes** tab of the Web Console. For further details, see [Auditing Configuration Changes](#).

The following topics in this section describe how to configure the Server Policy settings:

- [Enabling Agent Recording](#)
- [Enabling Identity Theft Detection](#)
- [Enabling Agent API](#)
- [Showing/Hiding the Agent Tray Icon](#)
- [Restricting Recording to RDP Sessions](#)
- [Enabling Hotkeys](#)
- [Enabling Key Logging](#)
- [Optimizing Screen Capture Data Size](#)
- [Enabling Recording Notification](#)
- [Recording in Color or Grayscale](#)
- [Setting Session Timeout](#)
- [Setting Keyboard Recording Frequency](#)
- [Setting Continuous Recording](#)
- [Data Recording Policy](#)
- [Offline Recording Policy](#)
- [Identification Policy](#)
- [User Recording Policy](#)
- [Application Recording Policy](#)
- [Agent Logging and Debugging](#)
- [Memory Management](#)

Enabling Agent Recording

Note: This feature is supported on Windows-based and Unix-based server policies.

By default, as soon as the ObserveIT Agent is installed and the user logs on to the monitored machine, all user actions start to be recorded. However, if required, you can temporarily disable recording without uninstalling the Agent software.

You can control the recording status of the ObserveIT Agent manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To disable the Agent recording status using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (default Windows-based or Unix-based policy).
- 2) In the **System Policy** section of the **Server Policy Template** page, clear the **Enable recording** check box. (By default, this check box is enabled, to allow recording at the start of every session.)

Server Policy Template

- 3) Click **Save** to save the changes.

Setting changes will take effect on new user sessions, after the current sessions are closed.

Enabling Identity Theft Detection

Note: This feature is supported on Windows-based and Unix-based server policies.

When an Identity Theft Detection policy is configured in ObserveIT, users who are logged on to monitored servers can receive notification via email about the specific servers to which they have logged on, and from which client machines they logged in.

To enable users to receive these email notifications from ObserveIT, the **Identity Theft Detection** feature must be enabled.

You can enable this feature manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To enable identity theft detection using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (default Windows-based or Unix-based policy).

- 2) In the **System Policy** section of the **Server Policy Template** page, select the **Enable Identity Theft Detection** check box. By default, this check box is disabled.

Server Policy Template

[Back to Server Policy Templates](#) | [Linked Servers](#) Cancel Save

Name:

System Policy

Enable recording	☒
Enable Identity Theft Detection	☒
Enable API	☐
Show tray icon	☒
Restrict to RDP	☐
Enable hotkeys	☐
Enable key logging	☐
Optimize screen capture data size (?)	☒
Enable recording notification (?)	☐ All activity on this machine is recorded Default
Set image format	Grayscale Server Compression
Set session timeout (minutes)	15
Set keyboard frequency	Low
Set continuous recording (seconds) (?)	OFF

- 3) Click **Save** to save the changes.

Setting changes will take effect on new user sessions, after the current sessions are closed.

Enabling Agent API

Note: This feature is supported only on Windows-based server policies.

The ObserveIT Agent software's Application Programming Interface (API) allows programmers to control the Agent recording status (Enabled, Disabled, Started, or Stopped), which applications or URLs are recorded, and other settings. Although this API is protected, in order to prevent the wrongful usage of this API by malicious users, the API is disabled by default. If you intend to use the API, you must enable it.

You can enable the Agent API manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To enable the Agent API using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (default Windows-based policy).

- 2) In the **System Policy** section of **Server Policy Template** page, select the **Enable API** check box. By default, this check box is disabled.

Server Policy Template

[Back to Server Policy Templates](#) | [Linked Servers](#) Cancel Save

Name: Default Windows-based Policy

System Policy

Enable recording	☒
Enable Identity Theft Detection	☐
Enable API	☒
Show tray icon	☒
Restrict to RDP	☐
Enable hotkeys	☐
Enable key logging	☐
Optimize screen capture data size (?)	☒
Enable recording notification (?)	☐ All activity on this machine is recorded Default
Set image format	Grayscale Server Compression
Set session timeout (minutes)	15
Set keyboard frequency	Low
Set continuous recording (seconds) (?)	OFF

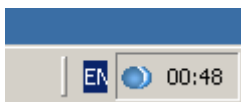
- 3) Click **Save** to save the changes.

Setting changes will take effect on new user sessions, after the current sessions are closed.

Showing/Hiding the Agent Tray Icon

Note: This feature is supported only on Windows-based server policies.

When you install the ObserveIT Agent, an icon is automatically placed in the system tray notification area next to the clock.



This tray icon shows the recording mode at the start of every session. By default, the Agent tray icon is visible. If the icon is grayed-out, then there is a problem with the recording.

ObserveIT lets you configure whether to keep the icon visible, or hide it.

You can configure the visibility of the tray icon manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To configure the ObserveIT Agent icon status using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (default Windows-based policy).

- 2) In the **System Policy** section of **Server Policy Template** page, clear the **Show tray icon** check box to hide the ObserveIT Agent tray icon. By default, this check box is enabled.

Server Policy Template

Back to Server Policy Templates | Linked Servers

Cancel Save

Name: New Server Policy Template

System Policy

Enable recording	☒
Enable Identity Theft Detection	☐
Enable API	☒
Show tray icon	☐
Restrict to RDP	☐
Enable hotkeys	☐
Enable key logging	☐
Optimize screen capture data size (?)	☒
Enable recording notification (?)	☐ All activity on this machine is recorded Default
Set image format	Grayscale Server Compression
Set session timeout (minutes)	15
Set keyboard frequency	Low
Set continuous recording (seconds) (?)	OFF

After the setting changes take effect, no icon will be displayed in the system tray.



Important Notes

- Disabling the **Show tray icon** check box hides the ObserveIT Agent icon, but all recordings on that Server will continue.
- In addition to hiding the tray icon, you might also want to hide the ObserveIT Agent program from the **Add/Remove Programs** applet in **Control Panel**.
- Setting changes will take effect on new user sessions, after the current sessions are closed.

Restricting Recording to RDP Sessions

Note: This feature is supported only on Windows-based server policies.

ObserveIT records all types of user sessions, either local or remote through Remote Desktop or third-party remote management tools, such as VNC, PCAnywhere, NetOP, and others.

By default, all sessions (remote and local) are recorded, but you can configure the Agent to record only when the user session is a remote RDP session. In this case, local log on sessions will not be recorded.

You can configure the recording to RDP only manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To restrict recording to RDP sessions only, using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (default Windows-based policy).

- 2) In the **System Policy** section of the **Server Policy Template** page, select the **Restrict to RDP** check box. By default, this check box is disabled, to allow the recording of all types of user sessions.

Server Policy Template

Back to Server Policy Templates | Linked Servers

Cancel Save

Name: New Server Policy Template

System Policy

- Enable recording ☒
- Enable Identity Theft Detection ☐
- Enable API ☒
- Show tray icon ☒
- Restrict to RDP ☒
- Enable hotkeys ☒
- Enable key logging ☐
- Optimize screen capture data size (?) ☒
- Enable recording notification (?) ☐ All activity on this machine is recorded Default
- Set image format Grayscale Server Compression
- Set session timeout (minutes) 15
- Set keyboard frequency Low
- Set continuous recording (seconds) (?) OFF

- 3) Click **Save** to save the changes.

Setting changes will take effect on new user sessions, after the current sessions are closed.

Enabling Hotkeys

Note: This feature is supported only on Windows-based server policies.

ObserveIT allows you to access the following features by using the F11 and F12 hotkeys:

- F11 enables you to create sticky notes which can be attached to resources and applications on the monitored servers. For further details, see [Sticky Notes](#).
- F12 enables the use of context sensitive searches through the database. For further details, see [Context Sensitive Search](#).

By default, these hotkeys are disabled.

You can configure the hotkeys status manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To enable the use of hotkeys using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (default Windows-based policy).

- 2) In the **System Policy** section of the **Server Policy Template** page, select the **Enable hotkeys** check box.

Server Policy Template

- 3) Click **Save** to save the changes.

Setting changes will take effect on new user sessions, after the current sessions are closed.

Enabling Key Logging

Note: This feature is supported on Windows-based server policies.

ObserveIT's key logger enables the tracking and recording of all on-screen user activity on monitored servers. For further details, see [ObserveIT Key Logging](#) (in the User Guide).

To use the ObserveIT text logger on monitored servers, the key logging feature must be enabled. By default, key logging is disabled.

You can configure key logging manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To configure key logging using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (Windows-based or Unix-based policy).

- 2) In the **System Policy** section of the **Server Policy Template** page, select the **Enable Key Logging** check box.

Server Policy Template

[Back to Server Policy Templates](#) | [Linked Servers](#) Cancel Save

Name:

System Policy

Enable recording	☒
Enable Identity Theft Detection	☐
Enable API	☐
Show tray icon	☒
Restrict to RDP	☐
Enable hotkeys	☐
Enable key logging	☒
Optimize screen capture data size (?)	☒
Enable recording notification (?)	☐ All activity on this machine is recorded Default
Set image format	Grayscale Server Compression ▼
Set session timeout (minutes)	15 ▼
Set keyboard frequency	Low ▼
Set continuous recording (seconds) (?)	OFF ▼

- 3) Click **Save** to save the changes.
Setting changes will take effect on new user sessions, after the current sessions are closed.

Optimizing Screen Capture Data Size

Note: This feature is supported on Windows-based server policies only.

To reduce the overall size of storage required for screenshot data, ObserveIT applies an advanced compression algorithm that optimizes the screen capture storage size. The compression algorithm applies to all ObserveIT screenshots, whether they are stored in the SQL Server database, or in the file system on a local hard drive of the ObserveIT Application Server, or on a file share in the network. This method of optimization can lead to a significant saving in storage size.

Screen data storage optimization is enabled by default. If you want to store images as complete screenshots, you can disable this option.

You can configure the on/off status of screen capture data size optimization manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To configure screen capture data size optimization using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (Windows-based policy).

- 2) In the **System Policy** section of the **Server Policy Template** page, clear the **Optimize screen capture data size** check box to disable this feature. By default, this check box is selected to allow data storage optimization.

Server Policy Template

Back to Server Policy Templates | Linked Servers

Cancel Save

Name: New Server Policy Template

System Policy

- Enable recording ☒
- Enable Identity Theft Detection ☐
- Enable API ☐
- Show tray icon ☒
- Restrict to RDP ☐
- Enable hotkeys ☐
- Enable key logging ☒
- Optimize screen capture data size (?) ☐ (being unselected)
- Enable recording notification (?) ☐ All activity on this machine is recorded and monitored. Default
- Set image format: Grayscale Server Compression
- Set session timeout (minutes): 15
- Set keyboard frequency: Low
- Set continuous recording (seconds) (?) : OFF

- 3) Click **Save** to save the changes.

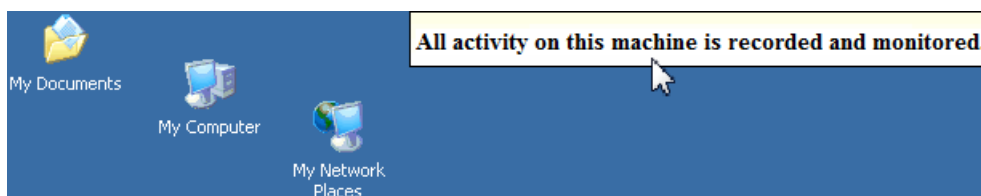
Setting changes will take effect on new user sessions, after the current sessions are closed.

Enabling Recording Notification

Note: This feature is supported on both Windows and Unix-based server policies.

ObserveIT enables you to notify users that their actions are being recorded during recording sessions on the server. This is most useful on management workstations in which there are privacy issues.

When actions are being recorded, and the notification message feature is enabled, a yellow recording notification bar appears on the desktop on each recording session, clearly notifying the user that their actions are being recorded and monitored. The default message displays "All activity on this machine is recorded and monitored".



You can configure the display of the recording notification message manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To configure the recording notification message using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (Windows-based or Unix-based policy).

- 2) In the **System Policy** section of the **Server Policy Template** page, select the **Enable recording notification** check box. By default, this check box is disabled.

Server Policy Template

[Back to Server Policy Templates](#) | [Linked Servers](#) Cancel Save

Name

System Policy

Enable recording	☒	
Enable Identity Theft Detection	☐	
Enable API	☐	
Show tray icon	☒	
Restrict to RDP	☐	
Enable hotkeys	☐	
Enable key logging	☒	
Optimize screen capture data size (?)	☐	
Enable recording notification (?)	☒	All activity on this machine is recorded Default
Set image format		Grayscale Server Compression ▼
Set session timeout (minutes)		15 ▼
Set keyboard frequency		Low ▼
Set continuous recording (seconds) (?)		OFF ▼

- 3) If required, you can edit the default recording notification message that is displayed next to the check box. To revert to the default message, click the **Default** button.
- 4) Click **Save** to save the changes.

Enabling the recording notification message configures the yellow recording notification bar that appears on the desktop on each recording session, clearly notifying the user that their actions are being recorded and monitored. When disabled (the default), recording continues on the server but the notification bar on the desktop will not be displayed.

Setting changes will take effect on new user sessions, after the current sessions are closed.

Recording in Color or Grayscale

Note: This feature is supported only on Windows-based server policies.

By default, all ObserveIT session images are recorded in grayscale. However, it is possible to change the recording settings to full color. The recording color affects the ObserveIT Agent performance depending on the format of the collected screenshots, the database storage required, and network utilization.

Session image colors can be compressed on the ObserveIT Client-side or Server-side. On the Client-side, the Agent captures the images in color and compresses them to grayscale images. On the Server-side, the Agent sends the captured colored images to the Application Server, which compresses them either to grayscale or color.

Note the following:

- By default, the images are compressed using "Grayscale Server Compression". However, if more than two monitors are connected to your computer, or if the monitor size is larger than 1680x1050 pixels, the image format switches to "Grayscale Client Conversion".
- When the Agent is in offline mode, even if you are recording the images in color, all the images will be saved as grayscale regardless of the server policy configuration. In the Session Player however, the images might be colored and grayscale; that is, colored when the Agent is online, and grayscale when the Agent is offline.
- The default setting "Grayscale Server Compression" requires normal CPU resources on the ObserveIT Agents and normal network bandwidth utilization.
- "Grayscale Client Compression" requires additional CPU resources on the ObserveIT Agents for the conversion, but utilizes less network bandwidth.
- The "Color" setting requires no additional CPU resources for compression; however, more data storage is required per screenshot on the SQL Server database, and there is a much higher network bandwidth utilization (up to 10 times greater than the default grayscale). This setting is not recommended unless it is absolutely essential.

You can configure the recording color manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To configure the recording color using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (default Windows-based policy).

- 2) In the **System Policy** section of the **Server Policy Template** page, from the **Set image format** drop-down list, select the required image format (**Color**, **Grayscale Server Compression**, or **Grayscale Client Compression**).

Server Policy Template

[Back to Server Policy Templates](#) | [Linked Servers](#)
Cancel Save

Name

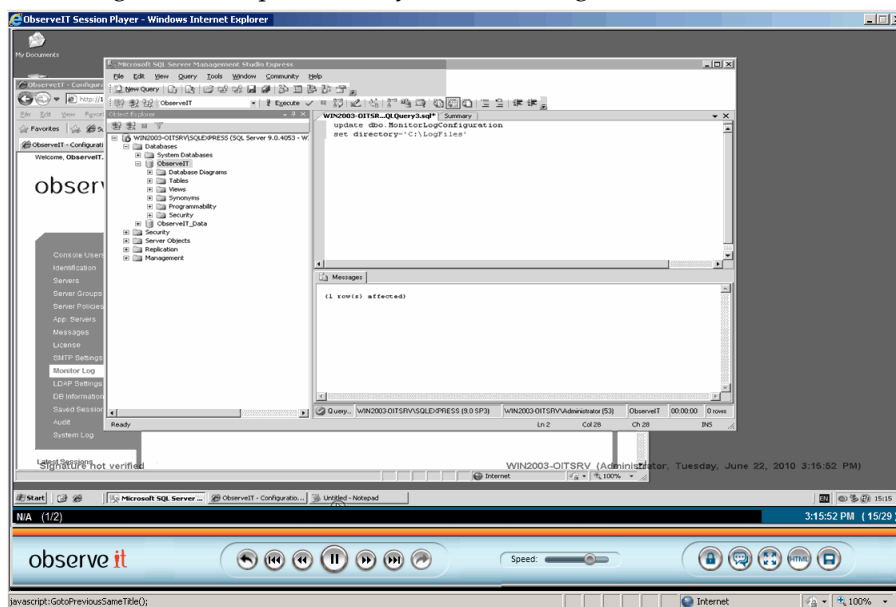
System Policy

- Enable recording ☒
- Enable Identity Theft Detection ☐
- Enable API ☐
- Show tray icon ☒
- Restrict to RDP ☐
- Enable hotkeys ☐
- Enable key logging ☒
- Optimize screen capture data size (?) ☐
- Enable recording notification (?) ☒ All activity on this machine is recorded Default
- Set image format

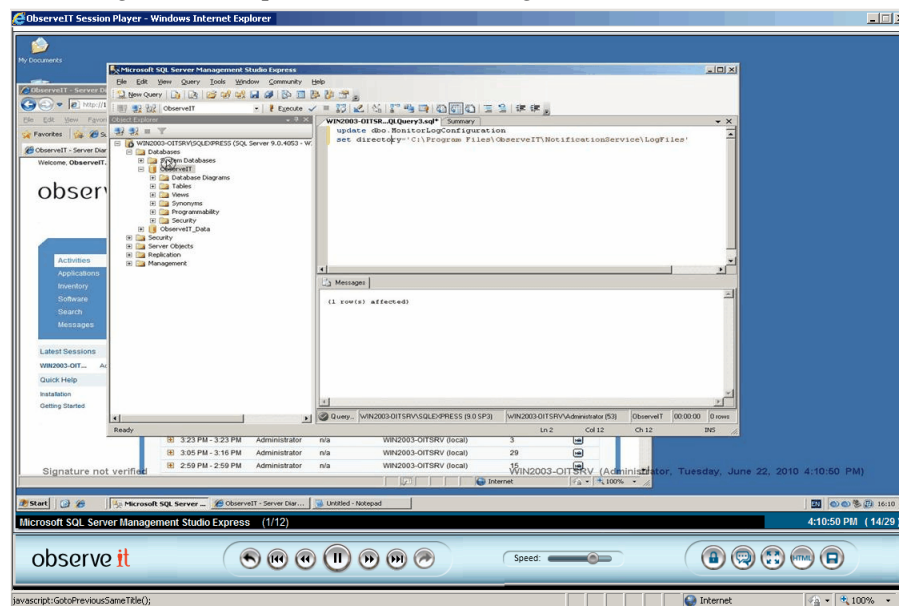
Grayscale Server Compression
Color
Grayscale Server Compression
Grayscale Client Compression
- Set session timeout (minutes)
- Set keyboard frequency
- Set continuous recording (seconds) (?)

OFF

Following is an example of a Grayscale recording:



Following is an example of a color recording:



- 3) Click **Save** to save the changes.

Setting changes will take effect on new user sessions, after the current sessions are closed.

Setting Session Timeout

Note: This feature is supported on Windows-based and Unix-based server policies.

ObserveIT tracks session idle time, which is the period of inactivity in the session. When a session times out, ObserveIT will no longer wait for the user input, and closes the session. When a user performs an action such as clicking on a mouse key or typing on the keyboard, ObserveIT will create a new session. This will result in two or more user sessions in the **Server Diary** or **User Diary**, although from a Windows perspective there was just one long user session.

Server Diary

User Diary

DBA Activity

Activity Alerts

Configuration

Search

Reports

Threat Detection

Activities

Applications

Inventory

Software

Search

Messages

Latest Sessions

W2K8-S8-D02 Admini...

Quick Help

Installation Guide

User Guide

Configuration Guide

Activity View

Server: W2K8-S8-D02 Go Server statistics Print this information

Period: Last 1 Months Start Date: Jan 6 2015 End Date: Jan 14 2015

Filter by login/user: -All-

1 - 12 of 12

Session Duration	Login	User	Server	Client	Slides	Video
1/8/2015						
11:06 AM - 11:08 AM	Administrator	n/a	W2K8-S8-D02	OIT-DAVID	9	📺
10:31 AM - 10:35 AM	Administrator	n/a	W2K8-S8-D02	OIT-DAVID	4	📺
9:46 AM - 9:49 AM	Administrator	n/a	W2K8-S8-D02	OIT-DAVID	1	📺
9:16 AM - 9:17 AM	Administrator	n/a	W2K8-S8-D02	OIT-DAVID	2	📺

By default, all idle sessions time out at 15 minutes.

You can configure the session timeout manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To configure the session timeout using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (default Windows-based or Unix-based policy).
- 2) In the **System Policy** section of the **Server Policy Template** page, from the **Set session timeout (minutes)** drop-down list, select the required period of user inactivity after which the ObserveIT Agent will stop monitoring. The default is 15 minutes.

Server Policy Template

[Back to Server Policy Templates](#) | [Linked Servers](#)

Cancel
Save

Name

System Policy

Enable recording	☒
Enable Identity Theft Detection	☐
Enable API	☐
Show tray icon	☒
Restrict to RDP	☐
Enable hotkeys	☐
Enable key logging	☐
Optimize screen capture data size (?)	☒
Enable recording notification (?)	☐ All activity on this machine is recorded Default
Set image format	Grayscale Server Compression
Set session timeout (minutes)	15
Set keyboard frequency	Low
Set continuous recording (seconds) (?)	OFF

- 3) Click **Save** to save the changes.

Setting changes will take effect on new user sessions, after the current sessions are closed.

Setting Keyboard Recording Frequency

Note: This feature is supported only on Windows-based server policies.

The ObserveIT key logger enables the tracking and recording of all user activity on monitored servers, including every key press and mouse click. Any keyboard activity is a trigger for the ObserveIT Agent to perform a screen and metadata capture. For further details, see ObserveIT Key Logging (in the User Guide).

ObserveIT monitors the rate at which the user types on the keyboard. The frequency of the character typing will determine how often a screen capture is performed. For example, if a user types just one or two words in the command prompt window, in a leisurely manner, it will probably trigger one or two screenshots. However, if the same user types a 500 character email or Word document, many screenshots will be captured, but not every single typed character will invoke a screen capture.

It is possible to change the settings of the keyboard stroke recording frequency.

Important: Changing the keyboard stroke recording frequency will result in many more captured images and metadata, resulting in a lot more bandwidth usage plus extra storage usage on the SQL Server database. This setting is not recommended unless it is absolutely essential.

You can configure the keyboard stroke recording frequency manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To configure the keyboard stroke recording frequency using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (default Windows-based policy).
- 2) In the **System Policy** section of the **Server Policy Template** page, from the **Set keyboard frequency** drop-down list, select the required keyboard stroke frequency.

Server Policy Template

Back to Server Policy Templates | Linked Servers

Cancel Save

Name: Default Windows-based Policy

System Policy

- Enable recording: ☒
- Enable Identity Theft Detection: ☐
- Enable API: ☐
- Show tray icon: ☒
- Restrict to RDP: ☐
- Enable hotkeys: ☐
- Enable key logging: ☐
- Optimize screen capture data size (?): ☒
- Enable recording notification (?): ☐ All activity on this machine is recorded Default
- Set image format: Grayscale Server Compression
- Set session timeout (minutes): 15
- Set keyboard frequency: Low
- Set continuous recording (seconds) (?): OFF

Options include:

- **Low:** Every 1 second (default)
- **Medium:** Every 0.5 second
- **High:** Every key stroke

- 3) Click **Save** to save the changes.

Setting changes will take effect on new user sessions, after the current sessions are closed.

Setting Continuous Recording

Note: This feature is supported on Windows-based server policies only.

In Continuous Recording mode, ObserveIT records the user's screen even when no user activity is detected. This feature is useful when the user is watching a video with lengthy screen output, or long output from a running application. ObserveIT records the screen every x seconds, as configured in the server policy. By default, this feature is turned OFF.

When this feature is enabled and when no user activity occurs within the specified time interval (number of seconds), the screen which is in focus will be recorded, but only if it differs from the previous screen (in graphic or metadata).

If a recording policy was configured specifying applications or URLs and users or user groups that should not be recorded, these will not be recorded if they are in focus during the idle time. However, if a "metadata only" recording policy is preconfigured, this feature will be disabled automatically.

Important: You must be aware when using Continuous Recording mode, since it could cause a considerable increase in the database size. It is CPU intensive and it should not be used for Terminal Services or Citrix servers that host many concurrent sessions.

You can configure Continuous Recording mode manually per server (Agent) from the **Configuration > Servers** page, or by using **Server Group Policies** in order to configure many servers (Agents) simultaneously.

To configure continuous recording using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (default Windows-based policy).
- 2) In the **System Policy** section of the **Server Policy Template** page, the **Set continuous recording** check box is set to **OFF** by default.

Server Policy Template

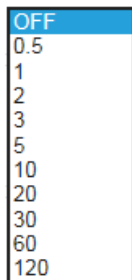
[Back to Server Policy Templates](#) | [Linked Servers](#) Cancel Save

Name:

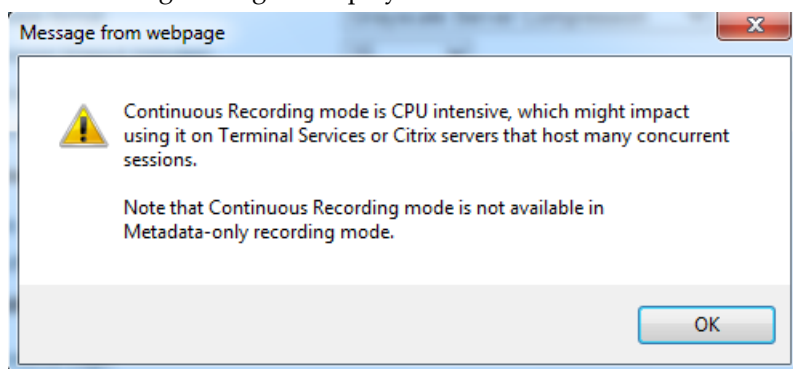
System Policy

Enable recording	☒
Enable Identity Theft Detection	☐
Enable API	☐
Show tray icon	☒
Restrict to RDP	☐
Enable hotkeys	☐
Enable key logging	☐
Optimize screen capture data size (?)	☒
Enable recording notification (?)	☐ All activity on this machine is recorded Default
Set image format	Grayscale Server Compression
Set session timeout (minutes)	15
Set keyboard frequency	Low
Set continuous recording (seconds) (?)	OFF

- 3) To set continuous recording, from the drop-down list, select the required interval (in seconds) during which time you want to continue recording even when no user activity occurs.



The following message is displayed.



- 4) Click **OK** to continue.
- 5) Click **Save** in the **Server Policy Template** page to save your setting changes.

Note: Setting changes will take effect on new user sessions, after the current sessions are closed.

Data Recording Policy

The following features enable you to configure a data recording policy which controls how much data is recorded during user sessions:

- Recording in Basic or Extended mode
- Limiting Output Data Recording

Note: These features are supported on Unix-based server policies only.

Recording in Basic or Extended Mode

On Unix/Linux-based operating systems, the ObserveIT Agent records:

- All interactive shell logins to the system, whether via SSH, Telnet, or local console.
- Each command line activity on the system.
- Every activity displaying screen output is visually recorded.
- System functions that were executed by commands or scripts that were executed by the user.

Recording on Unix/Linux-based operating systems can be handled in two modes:

- **Basic** mode is used to record commands and terminal output. This is the default mode.
- **Extended** mode is used to record all system functions metadata in addition to commands and terminal output. It is recommended that you select this option only if you require detailed inspection of system functions performed by executables, as a large volume of system function data can create heavy load on the Application Server. To reduce the load of system function data, you can select just the specific functions that you want to record.

In the ObserveIT Web Console, you can configure the recording mode manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To configure the recording mode using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (Unix-based policy).
- 2) In the **Data Recording Policy** section of the **Server Policy Template** page, select the required recording mode: **Basic** or **Extended**.

Server Policy Template

Back to Server Policy Templates | Linked Servers Cancel Save

Name

System Policy

Enable recording ☒

Enable Identity Theft Detection ☐

Enable recording notification ☐ Default

Set session timeout (minutes)

Data Recording Policy

☒ Basic (record commands and terminal output)

☐ Extended (record commands, terminal output and system functions)

☒ Stop recording session output beyond until new user input is detected

☒ Stop recording command output beyond until a new command or user input is detected

- 3) If you selected **Extended** mode, select the specific functions that you want to record, as shown below. By default, they are all selected.

Data Recording Policy

☐ Basic (record commands and terminal output)

☒ Extended (record commands, terminal output and system functions)

- ☒ File opened for read
- ☒ File created or opened for write
- ☒ File renamed
- ☒ File deleted
- ☒ File permissions changed
- ☒ Child process or shell created
- ☒ Process killed

☒ Stop recording session output beyond until new user input is detected

☒ Stop recording command output beyond until a new command or user input is detected

- 4) Click **Save** to save the changes.

Setting changes will take effect on new user sessions, after the current sessions are closed.

Limiting Output Data Recording

During ObserveIT session recording in a Unix/Linux environment, if there is no user input and the volume of output exceeds the defined limit, the recording of output data will stop. For session output, only upon new user input will a new session be created and recording resume. For command output, recording will resume upon a new command. By limiting output data recording, you can control the volume of recorded output data for an ObserveIT session when there is no user activity (for example, when running the "tail -f" command on the OS messages/syslog file and a high volume of logging messages are written to that file).

In the ObserveIT Web Console, on Unix and Linux-based server policies, you can configure a recording policy for limiting output data recording, by specifying a maximum output data size that is allowed to be recorded before a session is closed when there is no user input.

You can configure output data recording thresholds per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To configure thresholds for output data recording using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (Unix-based policy).
- 2) In the **Data Recording Policy** section of the **Server Policy Template** page, select one or both of the check boxes next to the required **Stop recording session/command** options. (By default, both options are selected.)

Data Recording Policy

☒ Basic (record commands and terminal output)

☐ Extended (record commands, terminal output and system functions)

☒ Stop recording session output beyond until new user input is detected

☒ Stop recording command output beyond until a new command or user input is detected

- **Stop recording session output beyond:** Select this option to define a limit (in KB or MB) for the session output data recording size before new user input is received. The default size is 1000 kilobytes; zero means that there is no data size limit.
 - **Stop recording command output beyond:** Select this option to define a limit (in KB or MB) for the volume of command output, before a new command or user input is received. This output limit applies to each command; a new command will start a new session for recording. The default size is 500 kilobytes; zero means that there is no data size limit.
- 3) Click **Save** to save the changes.
- Setting changes will take effect on new user sessions, after the current sessions are closed.

Offline Recording Policy

Note: This feature is supported on Windows-based and Unix-based server policies.

ObserveIT Agents transmit recorded data to the ObserveIT Application Server. When offline mode is disabled, in the event of a network malfunction or disconnection between the Agents and the Application server, no recording nor local data will be stored on the monitored machines.

When offline mode is enabled, and a network malfunction or disconnection occurs between the Agents and the Application server, the Agents will cache a local copy of the recorded data. When the network is back online, the Agents will transmit the local cached content back to the Application server, and the local copy will be removed. ObserveIT lets you configure the amount of local cache content to use.

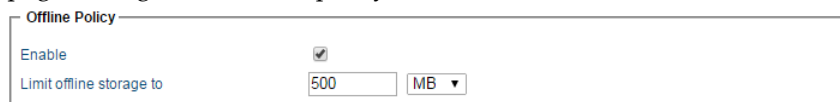
Important: Although the locally cached files cannot be used other than by viewing them through the ObserveIT system, the locally stored files might still be deleted or moved by a local malicious administrator. In this case, make sure you use proper NTFS file-level permissions and apply auditing on the Queue folder, and monitor any access and change to that folder.

On Unix-based server policies, you can configure an offline storage location for recorded ObserveIT sessions. By default, recorded data on Unix/Linux Agents is stored under the directory `/opt/observeit/agent/run`. If connectivity with the ObserveIT Application Server is lost when offline recording is enabled, user activity data will be temporarily stored in the file system of the client machine until connectivity is restored and the data can be transferred to the Application Server. You may specify the file system path where the recorded data will be temporarily stored, or you can store the data in the "Default product path" which is a folder under the directory of the installed ObserveIT Agent. On Unix-based server policies, you can also define limits for the size of the offline storage for each recorded machine and/or each recorded session.

You can configure an offline recording policy manually per server (Agent) from the **Configuration > Servers** page, or by using **Server Group Policies** in order to configure many servers (Agents) simultaneously.

To enable offline mode recording using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (Windows-based or Unix-based policy).
- 2) If the server policy is Windows-based, in the **Offline Policy** section of the **Server Policy Template** page, configure an offline policy as follows:



Offline Policy

Enable ☒

Limit offline storage to MB

- a) Select the **Enable** check box.
- b) In the **Limit offline storage to** field, specify (in MB/GB) the maximum volume of data that can be stored offline. The default is 500 megabytes. If the maximum volume of data is exceeded, content will be overwritten from the beginning.

Or

- 3) If the server policy is Unix-based, in the **Offline Recording Policy** section, configure an offline policy as follows:



- a) Select the **Enable offline recording** check box. (By default, this check box is selected.)
- b) You can change the **Offline storage location** default directory `/opt/observeit/agent/run` which stores the offline data for recorded Unix/Linux sessions. You must provide a valid full path to the new offline storage location (that is, no spaces, no forbidden characters, it must start with a "/", and so on); otherwise you will receive an error message and the location will revert to the default.

Note: If connectivity with the ObserveIT Application Server is lost when offline recording is enabled, user activity data will be temporarily stored in the file system of the client machine until connectivity is restored and the data can be transferred to the Application Server. For the **Offline storage location**, you may specify the file system path where the recorded data will be temporarily stored, or you can click **Default** to store the data in the **[Default product path]** which is a folder under the directory of the installed ObserveIT Agent.

- c) If required, you can define limits for the size of the offline storage per recorded machine and/or per recorded session:
 - **Limit per recorded machine:** Select this option to specify (in MB/GB) the maximum volume of data that can be stored in the offline storage folder for each recorded machine, regardless of the number of sessions. The default size limit is 10 gigabytes. Note that if you do not select this option, the offline storage per recorded machine is unlimited.
 - **Limit per recorded session:** Select this option to specify (in MB/GB) the maximum volume of data that can be stored in the offline storage folder for each recorded session. The default size limit is 100 megabytes. Note that if you do not select this option, the offline storage per recorded session is unlimited.
- 4) Click **Save** to save the changes.

Setting changes will take effect on new user sessions, after the current sessions are closed.

Identification Policy

Note: This feature is supported on both Windows and Unix-based server policies.

When ObserveIT's Identification Services are enabled and configured, Forced-Identification users are required to identify themselves by a secondary log on prompt when logging on to any ObserveIT-monitored server. For further details, see [Identification Services](#).

This topic describes how to configure identification policy settings for Forced-Identification users.

You can configure these policy settings manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To configure identification policy settings using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (Windows or Unix-based policy).
- 2) In the **Identification Policy** section of the **Server Policy Template** page, select the **Enforce Login** check box. By default, this check box is selected.

Note that selecting this check box when no Forced-Identification users have been defined will have no effect.

If required, you can edit the text of the default message that will be displayed to the user when requested to provide secondary authentication. For further details, see [Enabling Recording Notification](#).

- 3) Select **All Users** to enforce a secondary login on *all the users* who are logged in to the monitored servers.

Or

Select **User** to enforce a secondary login on a *specific user*, enter the required **Domain** name or select it from the list, and specify the user's **Login** name. Click the **Add** button.

The **Domain** drop-down list displays all the domains in the Active Directory forest in which the ObserveIT Application Server is a member. You can select "*" to select all domains.

Note: ObserveIT easily integrates with your Active Directory forest, enabling you to use user and group objects from any domain in the forest in which the ObserveIT server-side components are installed, and in which the ObserveIT Agents are deployed (if different). Cross forest trusts can also be used. Although using groups from Active directory domains is possible with any group scope (domain local, global, or universal), it is recommended that you follow Microsoft's best practices on group object usage. For further details, see [Active Directory Best Practices](#).

- 4) Select the **Save last used login** check box if you want to auto-populate the **User Name** box of the secondary ObserveIT logon screen with the last logged-on user name.

Note: If you select this setting, the next user that logs on will be able to see which user was previously logged on to the system. For security reasons, it is recommended that you do *not* select this setting.

- 5) Click **Save** to save the changes.

Setting changes will take effect on new user sessions, after the current sessions are closed.

User Recording Policy

Note: This feature is supported on Windows-based and Unix-based server policies.

By default, ObserveIT is configured to record all the users that log on to any monitored computer. However, if you do not want to record all users that log in, ObserveIT lets you configure a recording policy that specifies which users and/or user groups to include/exclude from being recorded. If required, you can record just metadata for users/groups that you want to exclude from being recorded.

Note: ObserveIT easily integrates with your Active Directory forest, enabling you to include (or exclude) user and groups from any domain in the forest in which the ObserveIT server-side components are installed, and in which the ObserveIT Agents are deployed (if different). Cross forest trusts can also be used. Although using groups from Active directory domains is possible with any group scope (domain local, global, or universal), it is recommended that you follow Microsoft's best practices on group object usage. For further details, refer to [Active Directory Best Practices](#).

You can configure a user recording policy manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies in the **Server Policy Template** page to configure many servers (Agents) simultaneously.

To configure the ObserveIT Server to record all user sessions, except for a few specific users or groups, using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (Windows-based or Unix-based policy).
- 2) In the **User Recording Policy** section of the **Server Policy Template** page, select **Record all users**.

User Recording Policy

☒ **Record all users**

To exclude any user from being recorded, please enter the login (e.g. "administrator" or "OBSERVEIT\danielp") and click Add. You can add multiple users to this list.

Exclude: User Domain (* for all) Login Add

Domain\User	Created Date	Type

Remove

☐ **Record only the following users**

To activate recording (video & metadata) for only specific users, please enter the login (e.g. "administrator" or "OBSERVEIT\danielp") and click Add. You can add multiple users to this list.

Include: User Domain (* for all) Login Add

Domain\User	Created Date	Type

Remove

- 3) To exclude specific users from being recorded:
 1. In the **Exclude** drop-down list, select **User**, type the domain for the user or select it from the list, and type the user's **Login** name. Click the **Add** button.

Note: The **Domain** list displays all the domains in the Active Directory forest in which the ObserveIT Application Server is a member. You can select "*" to select all domains.

2. Repeat the above step for each user that you want to exclude. The specified users are displayed in the list.

Or

- 4) To exclude specific groups from being recorded:
 1. In the **Exclude** drop-down list, select **Group**, select the domain for the group from the **Domain** drop-down list, and type the **Group Name**. Click the **Add** button.
 2. Repeat the previous step for each group that you want to exclude.
- 5) If you want to allow textual metadata to be recorded for the excluded users/groups, select the **Record metadata for excluded users** check box.

Note: You can remove users/groups from the list by selecting them and clicking the **Remove** button.

- 6) Click **Save** to save the changes.

To configure the ObserveIT Server to record video and metadata for only specific users or groups

- 1) In the **User Recording Policy** section of **Server Policy Template** page, select **Record only the following users**.

User Recording Policy

☐ Record all users

To exclude any user from being recorded, please enter the login (e.g. "administrator" or "OBSERVEIT\danielp") and click Add. You can add multiple users to this list.

Exclude: Domain (* for all) Group Name

Group * \ Add

Domain\User	Created Date	Type

☐ Record metadata for excluded users Remove

☒ Record only the following users

To activate recording (video & metadata) for only specific users, please enter the login (e.g. "administrator" or "OBSERVEIT\danielp") and click Add. You can add multiple users to this list.

Include: Domain (* for all) Login

User * \ Add

User Domain\User Created Date Type

Group

Domain\User	Created Date	Type

☐ Record metadata for all users Remove

- 2) From the **Include** drop-down list, select **User**, select the domain name, and type the user's **Login** name. Click the **Add** button. Repeat this step for each user you want to include.

The specified users are displayed in the list.

Note: The **Domain** drop-down list displays all the domains in the Active Directory forest in which the ObserveIT Application Server is a member. You can select "*" to select all domains.

Or

- 3) From the **Include** drop-down list, select **Group**, select the domain name from the **Domain** drop-down list, and type the **Group Name**. Click the **Add** button. Repeat this step for each group you want to include.

- 4) If you want to allow textual metadata to be recorded for any user, even though visual data will only be available for specific users, select the **Record metadata for all users** check box. This option is only available if there are one or more users/groups in the **Include** list.

Note: You can remove users/groups from the list by selecting them and clicking the **Remove** button.

- 5) Click **Save** to save the changes.

Setting changes will take effect on new user sessions, after the current sessions are closed.

Application Recording Policy

Note: This feature is supported only on Windows-based server policies.

By default, ObserveIT is configured to record all the applications that are used by users that log on to any monitored computer. The list of applications is dynamically generated, which means that when a user loads an application for the first time, it will be registered in the applications list.

However, if you do not want to record all the applications that are used, ObserveIT lets you configure a recording policy that specifies which applications to include or exclude from being recorded. You can also configure a recording policy to record just metadata for applications, in which case no video will be captured.

You can configure an application recording policy manually per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To configure an application recording policy using Server Policies

- 1) In the **Configuration > Server Policies** page, click **Create** or select a server policy template (Windows-based policy).

- 2) In the **Application Recording Policy** section of the **Server Policy Template** page, you can select options for creating an application recording policy.

Application Recording Policy

☒ **Record all applications**

To de-activate recording (video & metadata) for a specific application, please select the process name from the list and click Add. You can add multiple applications to this list.

Exclude:

Exclude URL: ☐ Exact Match

☐ Also Record metadata for Exclude applications. No video will be recorded.

☐ **Record only the following applications**

To activate recording (video & metadata) for a specific application, please select the process name from the list and click Add. You can add multiple applications to this list.

Applications:

Record URL: ☐ Exact Match

☐ Record metadata for all applications regardless of whether they appear in the list. Video will be recorded only for applications that appear in the list.

☐ Record metadata only. Only metadata will be recorded for all applications. No video will be recorded.

- 3) To create a recording policy for all applications, do the following:

- Select the **Record all applications** option.
- To deactivate recording video and metadata for a specific application, select its name in the **Exclude** list, and enter the application's URL in the text box. You can specify part of the URL path, or the exact URL by selecting the **Exact Match** check box. Note that although the application will be added, it will only be recorded when the user accesses the specified URL.

Note: URL filtering is supported on Internet Explorer, Firefox, and Chrome applications.

- Click **Add**. Repeat the above step for each application that you want to exclude. The ObserveIT Server will record all applications except for those in the **Exclude** list.
- To record textual metadata for the excluded applications, select the **Also Record metadata for Excluded applications** check box. Note that no video will be recorded.

Note: To remove applications from the list, select them and click the **Remove** button.

- 4) To activate recording (video and metadata) for specific applications do the following:

- Select the **Record only the following applications** option.

☒ **Record only the following applications**

To activate recording (video & metadata) for a specific application, please select the process name from the list and click Add. You can add multiple applications to this list.

Applications:

Record URL: ☐ Exact Match

☐ url: *www.google.com*

☐ Record metadata for all applications regardless of whether they appear in the list. Video will be recorded only for applications that appear in the list.

- b) From the **Applications** list, select an application for which you want to enable recording, and enter the application's URL in the text box. You can specify part of the URL path, or the exact URL by selecting the **Exact Match** check box. Note that although the application will be added, it will only be recorded when the user accesses the specified URL.
 - c) Click **Add**. Repeat step 2 for each application that you want to include in the list.
 - d) For example, by typing "www.google.com" and clicking **Add**, *www.google.com* will be added to the list of recorded applications, recording any variation to that URL as long as the base string exists in the URL. If you also select **Exact Match** before clicking **Add**, "www.google.com" will be added to the list of recorded applications and any variation of that URL will NOT be recorded.
-
- Note: To remove applications from the list, select them and click the **Remove** button.
-
- e) To record metadata for all applications, select the check box, **Record metadata for all applications regardless of whether they appear in the list**. Note that a video is recorded only for applications that appear in the list.
- 5) To configure ObserveIT to record *only metadata* for the applications accessed during a user's session, select the **Record metadata only** option. Note that when this option is selected, no graphic information will ever be recorded.
 - 6) Click **Save** to save the changes.
- Setting changes will take effect on new user sessions, after the current sessions are closed.

Agent Logging and Debugging

Note: This feature is supported on Unix-based server policies only.

This feature enhances Agent logging and debugging by enabling users to dynamically control the level of detailed logs, at the policy level.

By default, after ObserveIT installation, the Unix/Linux Agent creates a directory named `/opt/observeit/agent/run`, which is used to store the log files of all recorded sessions. Unix/Linux Agent logs are stored in the `obit.log` file. When the `obit.log` file reaches its predefined limit, rotation occurs; that is, the file content is moved to a renamed backup file, and new log and debug data is stored in the `obit.log` file.

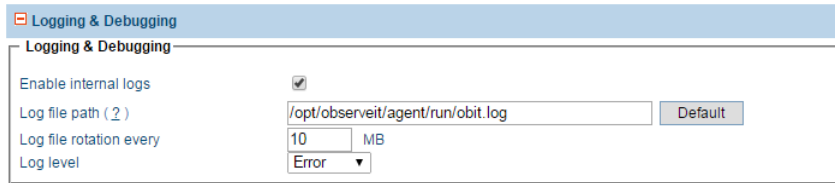
Four log level options can be configured at the policy level to trace Agent activities: **error**, **warning**, **info**, or **debug**. In earlier versions of ObserveIT, all internal messages and debug information were written to the syslog. The syslog is now used to store only critical system (**error** log level and above) errors; all other events are written, by default, to the `obit.log` file, or can be configured at the policy level.

In the ObserveIT Web Console, you can configure a server policy for session logs, per server (Agent) from the **Configuration > Servers** page, or by using **Server Group Policies** to configure many servers (Agents) simultaneously.

To configure session logs with session level information using Server Policies

- 1) In the **Configuration > Server Policies** page, select the required server policy template (Unix-based policy) or click **Create** to create a new server policy.

- 2) In the **Server Policy Template** page, expand the **Logging & Debugging** section by clicking the  icon.



- 3) To enable a new logging policy, select the **Enable internal logs** check box. (By default, this check box is selected.) If it is not selected, errors will still be reported in the syslog.
- 4) In **Log file path**, accept the default log file path or enter a new path for storing the log files.

Note: You can specify the file system path where the log data (and optionally, session debug data) will be stored, or you can click the **Default** button to store the log data in the **[Default product path]** which is a folder under the directory of the installed ObserveIT Agent.

- 5) Specify a threshold (in MB) for the **Log file rotation**. Permitted values are in the range of 1-100 MB; the default is 10 MB.
- 6) Select the required **Log level** from the drop-down list:
- **Error**: includes only error conditions (default setting)
 - **Warning**: includes all warning conditions (plus **error** messages)
 - **Info**: informational messages (plus **error** and **warning** messages)
 - **Debug**: debug-level messages (plus **error**, **warning** and **info** messages)
- 7) Click **Save** to save the settings.

Note: The log level changes automatically without the need to restart the Agent.

Memory Management

Note: This feature is supported on Unix-based server policies only.

ObserveIT provides an advanced feature that enables a more efficient way of managing recorded data that has accumulated in the Agent's memory, before it is sent to the Application Server. Offloading data from the Agent's memory prevents the Agent from consuming too much main memory that, in extreme cases, could cause the logger to fail or the session itself to fail due to memory problems.

In addition, sending the offloaded data of a session can be done while a session is still ongoing (live), instead of having to wait until the end of the session.

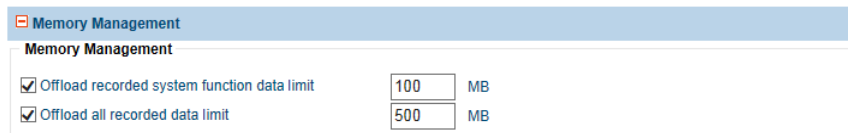
In the ObserveIT Web Console, on Unix and Linux-based server policies, you can configure a policy for offloading from the Agent's memory, recorded system function data and/or all recorded data when they reach predefined thresholds. Data is offloaded to the "offline storage location" (the default is `/opt/observeit/agent/run`) which stores the data for recorded Unix/Linux sessions.

You can configure a server policy for offloading recorded data, per server (Agent) from the **Configuration > Servers** page, or by using Server Group Policies to configure many servers (Agents) simultaneously.

To configure an offload data recording policy

- 1) In the **Configuration > Server Policies** page, select the required server policy template (Unix-based policy) or click **Create** to create a new server policy.

- 2) In the **Server Policy Template** page, expand the **Memory Management** section by clicking the  icon.



Memory Management	
☒ Offload recorded system function data limit	100 MB
☒ Offload all recorded data limit	500 MB

- 3) To configure an offload data recording policy for **recorded system function data**, select the check box, and specify a threshold (in MB) at which recorded system function data will be offloaded. The default is 100 MB.
- 4) To configure an offload data recording policy for **all recorded data**, select the check box, and specify a threshold (in MB) at which all recorded data will be offloaded. The default is 500 MB.

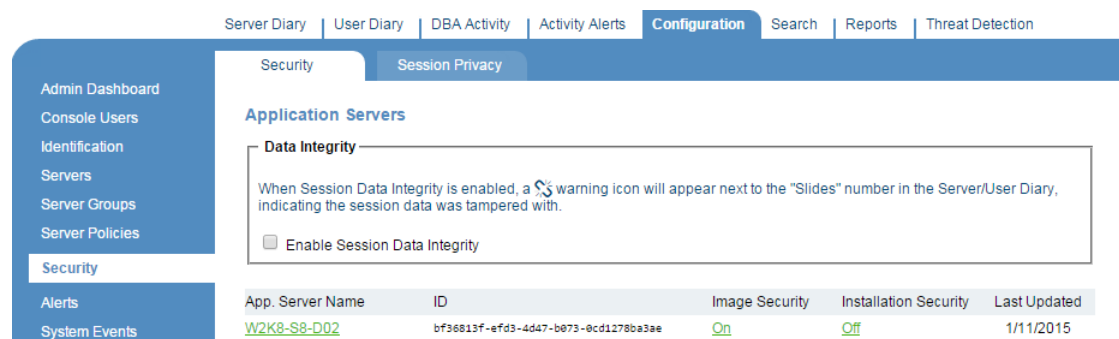
Note: These options are enabled by default.

- 5) Click **Save** to save the changes.
- Setting changes will take effect on new user sessions, after the current sessions are closed.

Implementing Security

ObserveIT is designed to be deployed within a secure network and accessed by administrators, and as such, is secure. Out-of-the-box deployment is designed to be simple, however security features such as digital signing and encryption can be optionally configured.

You can configure security in the **Configuration > Security** page.



On this page, you can make the following configuration changes:

- [Rename Application Servers](#)
- [Enable Image Security](#)
- [Enable Installation Security](#)

Note: Any modifications you make when configuring Application Server, Image, or Installation security, can be viewed for auditing purposes in the **Configuration Changes** tab of the Web Console. For further details, see [Auditing Configuration Changes](#).

General Security Best Practices

Following are some best practice recommendations that you should consider:

- Ensure that the servers running ObserveIT components are physically secure. If possible, lock these computers in a secure room to which only authorized personnel have direct access.
- Ensure that administrative rights to the Windows operating system are given only to those users that currently need them as part of their job description, and remove outdated users from administrative groups such as the default Administrators, Domain Admins, and Enterprise Admins groups.
- Change the default ObserveIT Admin password frequently and control access to that account.
- Strictly limit who is authorized to manage ObserveIT and view recorded session.
- Enable Agent-to-Application Server traffic security.
- Enable Database encryption and digital signing.
- Enable Installation Security to prevent rough Agent installation.
- Install digital certificates and set up SSL communications in IIS.
- Prevent the usage and execution of specific applications, programs or file types by using Group Policy Objects (or GPO). If required, refer to the Microsoft articles:
 - [Using Software Restriction Policies to Protect Against Unauthorized Software](#)
 - [How to Use Software Restriction Policies in Windows Server 2003](#)

- Protect traffic to and from critical servers by implementing IPsec Policies. If required, refer to the Microsoft article: [IPsec](#).

Read and implement well-documented security guidelines.

Renaming Application Servers

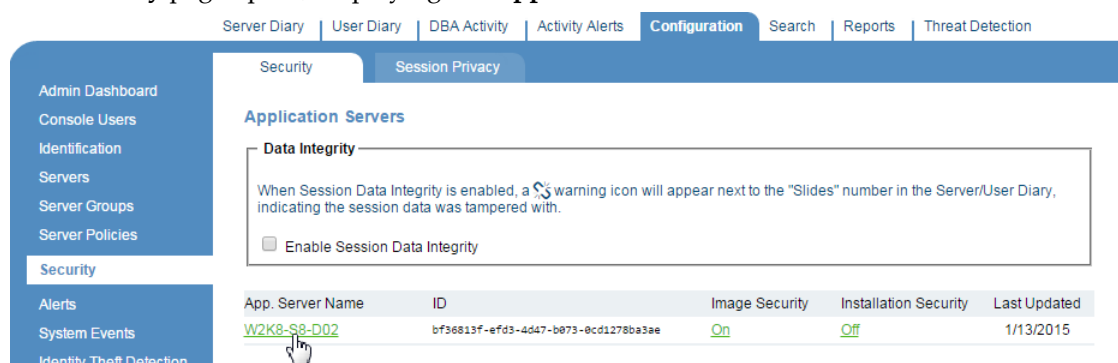
You can rename the ObserveIT Application Servers in case their computer names were changed and you want to maintain their new name in the application.

The ObserveIT Application Servers are listed in the **Configuration > Security** page, and thus can be renamed there.

To rename an Application Server

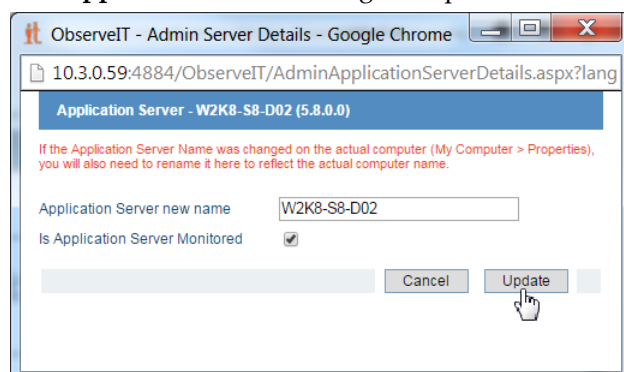
- 1) Navigate to **Configuration > Security**.

The **Security** page opens, displaying the **Application Servers** list.



- 2) Click the relevant **Application Server Name**.

The **Application Server** dialog box opens.



- 3) In the **Application Server new name** field, type the new name.
- 4) Click **Update**.

The new server name appears in the **Application Servers** list (in the **Configuration > Security** page).

Enabling Image Security

When Image Security is enabled, the ObserveIT Application Server uses a PKI-based mechanism to encrypt and digitally sign all session data.

Note: There may be some performance impact issues and database size increases when using image security.

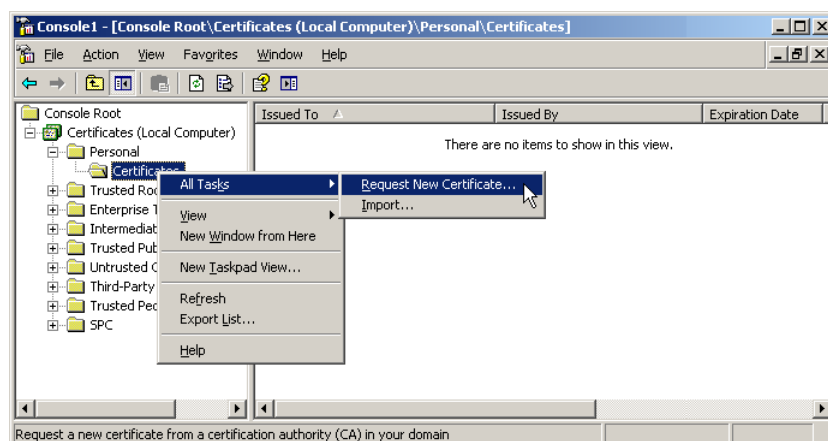
The following steps are required to enable image security:

- 1) Obtain a digital certificate.
- 2) Install the digital certificate.
- 3) Enable Image Security on the Application Server.

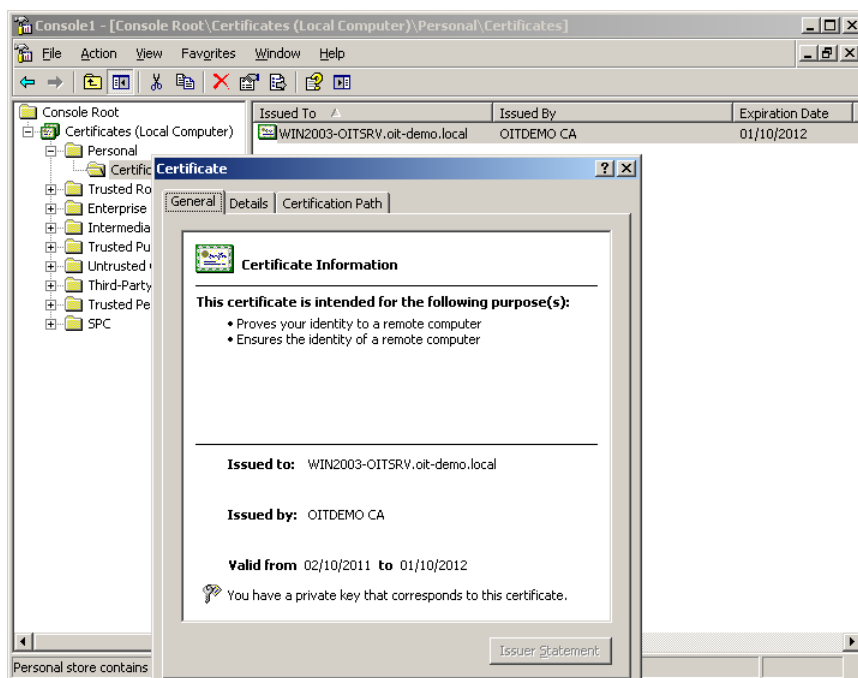
Step 1 - Obtaining a Digital Certificate

The first step in enabling image security is to obtain a Digital Certificate for each Application Server. A Digital Certificate is the digital equivalent of an ID card used with a public key encryption system. Also called digital IDs, digital certificates are issued by trusted third parties, known as certification authorities (CAs). The process of obtaining a digital certificate is beyond the scope of this documentation. This guide assumes that the reader holds prior knowledge of PKI and its related terminology. For further details, refer to the Microsoft Knowledge Base article: [Certificate Autoenrollment in Windows Server 2003](#).

There are several ways you can obtain a Digital Certificate; from a self-signed source, from an internal Certificate Authority (CA), or from a 3rd-party commercial CA. The following screen provides an example of a Digital Certificate request from a Windows Server 2003 machine to an internal Enterprise Certificate Authority.



You should provide a "friendly" name for the certificate such as "ObserveIT Certificate".



Alternatively, if you do not have an online CA or simply want to test this configuration without obtaining a trusted certificate, you can also use the MAKECERT utility from Microsoft which can be downloaded separately or as a part of the Microsoft Windows SDK from the Microsoft Download Center: [Microsoft Window SDK for Windows 7 and .NET Framework 4](#).

After you have obtained the MAKECERT utility, run the following command to obtain a self-signed certificate:

```
makecert -n "CN=ObserveIT Certificate" -sr LocalMachine -ss My -a sha1 -sky exchange -pe -r -m 12 -sp "Microsoft Strong Cryptographic Provider" -sy 1 -len 2048
```

Note: Use this procedure only for testing purposes.

After the Digital Certificate is obtained, it will be used in the process of encrypting and decrypting the images.

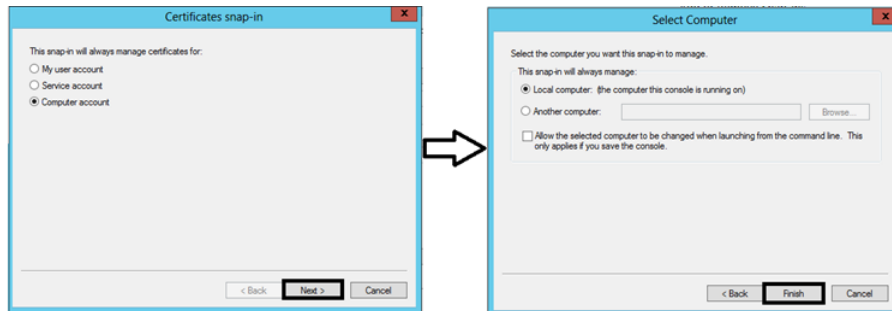
Important: It is very important that you maintain a proper backup of this Digital Certificate and the associated Private Key. This can be done by exporting it to a .PFX file and keeping it in a safe place. The .PFX file is also used to import the Digital Certificate and the associated Private Key to additional Application Servers.

Step 2 - Installing the Digital Certificate

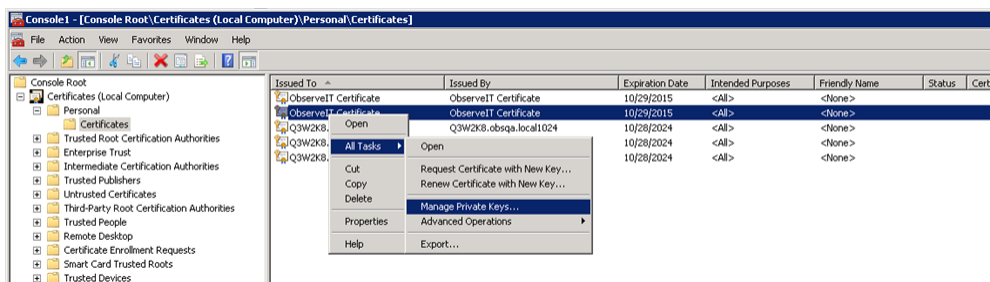
To install the certificate using the Internet Information Services (IIS) Manager Microsoft Management Console (MMC).

- 1) Go to **Start > run** and enter **mmc**.
- 2) In the **Console** window, select **File > Add/Remove Snap-in**.

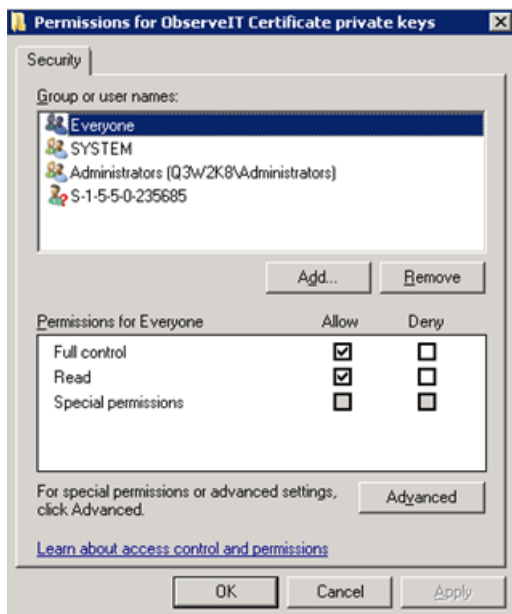
- 3) Select the **Certificates** snap-in, click **Add**, and assign it to the local computer account (**Computer Account -> Local Computer**).



- 4) In the MMC, under **Local Computers > Personal**, right-click the certificate and select **All Tasks > Manage Private Keys**.



- 5) Grant the certificate full privileges for the **Everyone** group.



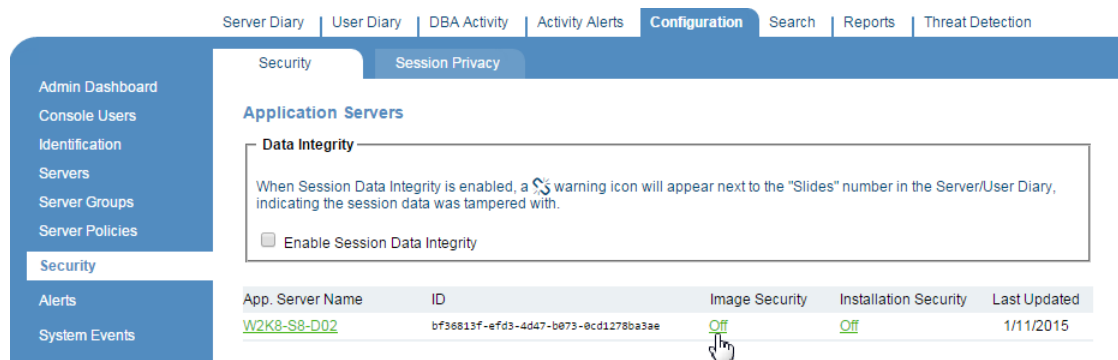
Step 3 - Enabling Image Security on the Application Server

To enable image security on the Application Server

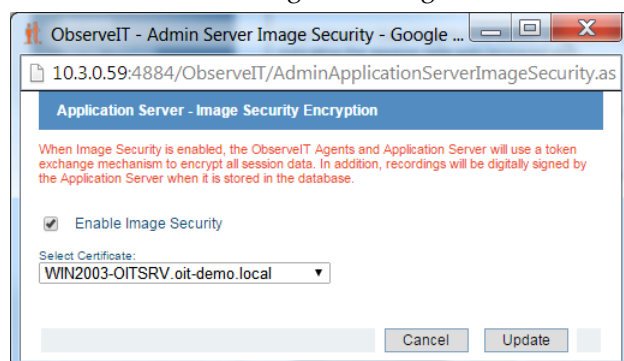
- 1) Navigate to **Configuration > Security**.
- 2) In the **Security** tab, if required, select the **Enable Session Data Integrity** check box.

Important: By default, the **Enable Session Data Integrity** check box is disabled. When this check box is enabled, a security check is run on all sessions in the database. If the security check finds any sessions that may have been tampered with and could therefore be corrupted, a  warning icon will appear next to the relevant sessions in the **Server Diary** or **User Diary**, or in the video replay of the **Session Player**.

- 3) Under **Image Security**, click the **Off** link.

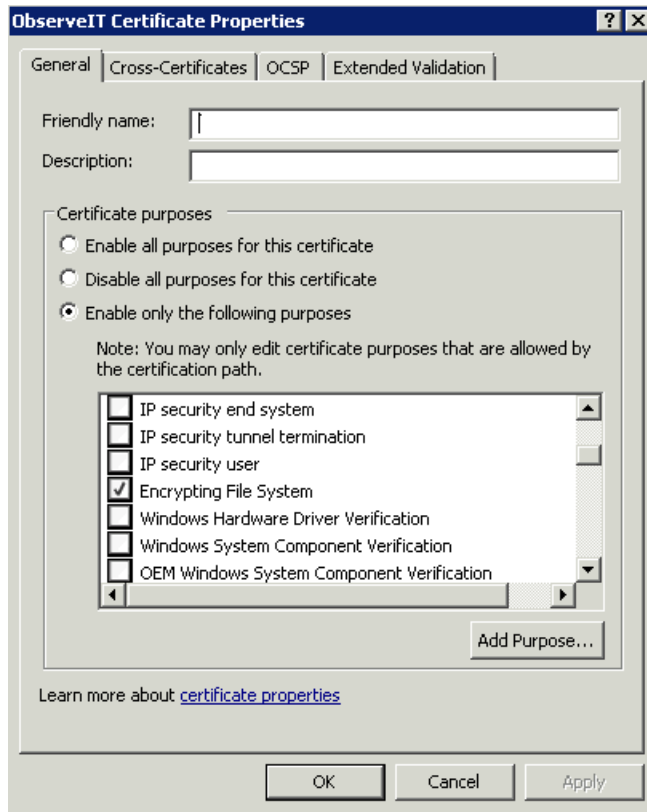


- 4) In the **Application Server - Image Security Encryption** window, select the **Enable Image Security** check box. Make sure the Digital Certificate listed matches the one you have obtained for the Application Server. If no Digital Certificate is listed, the image security cannot be enabled.
- 5) Click the **Update** button.
- 6) Click **OK** to acknowledge the changes.



The images will now be protected in the database.

Important: If you have previously set SSL for communicating with the ObserveIT Management console or the ObserveIT Application Server (see Enabling SSL on the Web Console and Configuring an ObserveIT Windows Agent to Use SSL in the Installation Guide), you CANNOT use the same SSL certificate for the encryption of images. The certificate MUST be configured for at least **Encrypting File System** purposes.



Enabling Installation Security

Installing ObserveIT Agents can be performed by any user with local administrative permissions on a computer, and with sufficient knowledge about the name or IP address of the ObserveIT Application Server. Some customers may want to enable an additional layer of security that will prevent unauthorized installations or uninstallations of the ObserveIT Agent software.

By default, installation security is disabled.

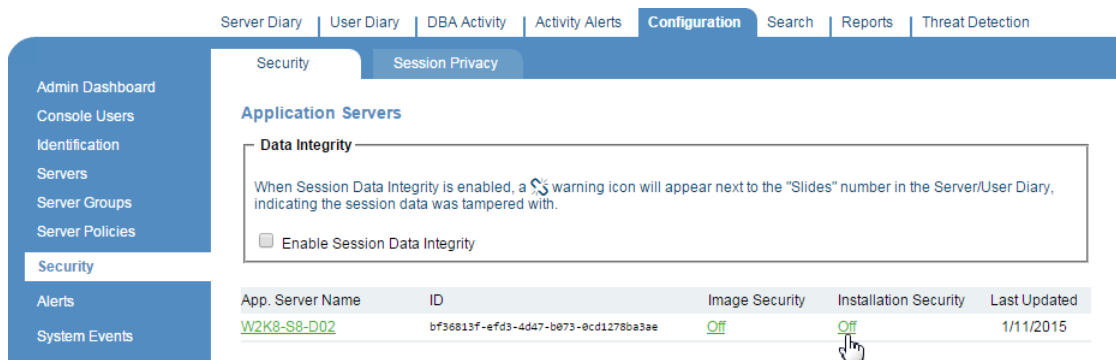
By enabling installation security, only users with knowledge of the installation security password can proceed with the Agent installation (or uninstallation). The ObserveIT Agent installation (or uninstallation) UI will prompt the user to enter the installation security password.

To enable installation security

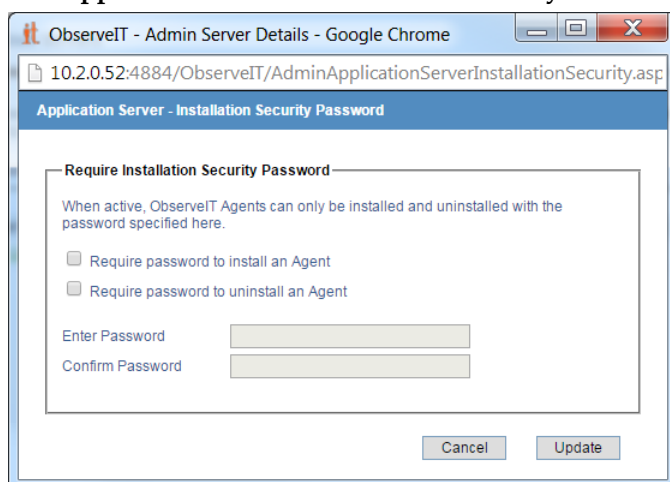
- 1) Navigate to **Configuration > Security**.
- 2) In the **Security** tab, if required, select the **Enable Session Data Integrity** check box.

Important: By default, the **Enable Session Data Integrity** check box is disabled. When this check box is enabled, a security check is run on all sessions in the database. If the security check finds any sessions that may have been tampered with and could therefore be corrupted, a  warning icon will appear next to the relevant sessions in the **Server Diary** or **User Diary**.

- 3) Under **Installation Security**, click the **Off** link.



The **Application Server - Installation Security Password** dialog box opens.



- 4) Select one or both check boxes to require a password on installation and/or uninstallation of the Agent.
- 5) Enter the installation password twice to confirm.
- 6) Click **Update**.
- 7) Acknowledge the message to confirm the change.

After the configuration changes are made, the **Installation Security** status changes to:

- **On** if passwords are required on both install and uninstall options.
- **On (Install only)** if a password is required only on Agent installation.
- **On (Uninstall only)** if a password is required only on Agent uninstallation.

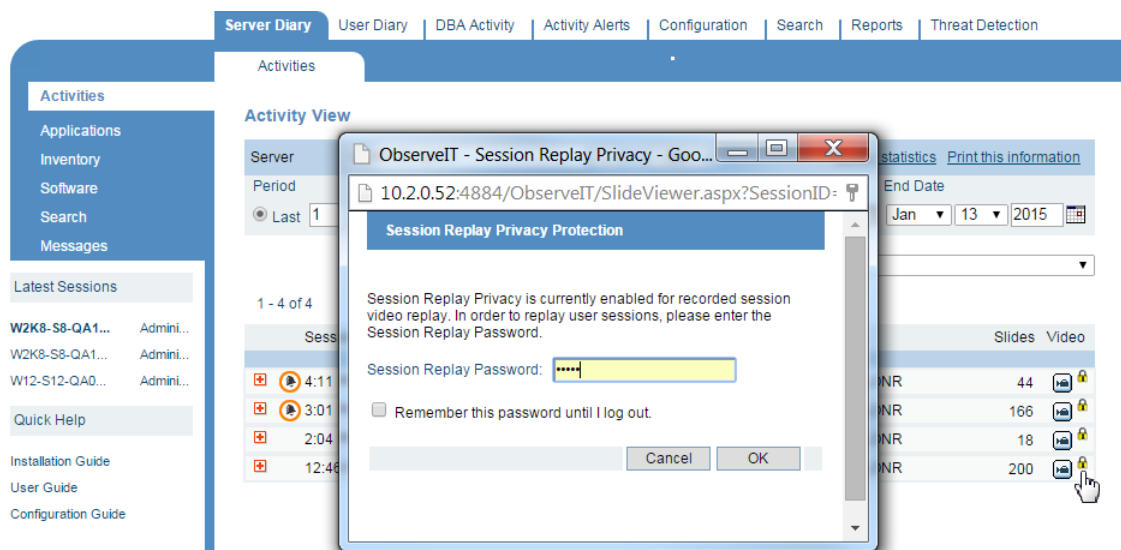
Note: You can always change the installation password, or cancel it entirely, by clicking the **On** link, and making the required changes.

Enabling Session Replay Privacy

ObserveIT is designed to allow Console Users proper roles and permissions to replay any session for which they have permissions. However, some customers may require additional replay security measures to protect the privacy of the recorded sessions.

The **Session Replay Privacy** option allows the customer to assign a master password that must be entered each time that a Console User wants to replay sessions.

After Session Replay Privacy Protection is enabled, each time a Console User needs to replay a recorded session, a lock icon appears next to the replay button. When the replay button is clicked, a message is displayed prompting the user to enter the Replay Privacy Protection password.



The Console User must enter the correct password, and click the **OK** button. If required, the user can select the **Remember this password until I log out** check box, to prevent the need to re-enter the password for each session they want to replay.

Note: If privacy is important, make sure that the Console User logs out of the Web Console after replaying the required sessions.

Note: The password is not required for making changes to the ObserveIT configuration settings. However, if the client wants to remove the Session Replay Privacy Protection, they will also need to know the master password. This is in order to prevent the client's Console Users with Admin role permissions from temporarily disabling the Session Replay Privacy Protection without the proper authorization.

Note: Session Replay Privacy Protection also applies to Saved Sessions and Reports.

To enable Session Replay Privacy Protection

- 1) Navigate to **Configuration > Security** and click the **Session Privacy** tab.

The screenshot shows the ObserveIT web console interface. The top navigation bar includes 'Server Diary', 'User Diary', 'DBA Activity', 'Activity Alerts', 'Configuration' (selected), 'Search', 'Reports', and 'Threat Detection'. The left sidebar lists various menu items, with 'Security' selected under the 'Configuration' section. The main content area is titled 'Session Privacy' and contains the 'Session Replay Privacy Protection' settings. A message states: 'When Session Replay Privacy is enabled, any attempt to replay a user session will require a password.' There is a checked checkbox for 'Enable Session Replay Privacy Protection'. Below it are two password input fields labeled 'Enter Password' and 'Confirm Password', both containing masked characters. A note next to the 'Enter Password' field indicates '(max. 14 characters)'. At the bottom right of the form is a 'Save' button.

- 2) Select the **Enable Session Replay Privacy Protection** check box.
- 3) Enter the Session Replay Privacy password twice to confirm.
- 4) Click **Save**.

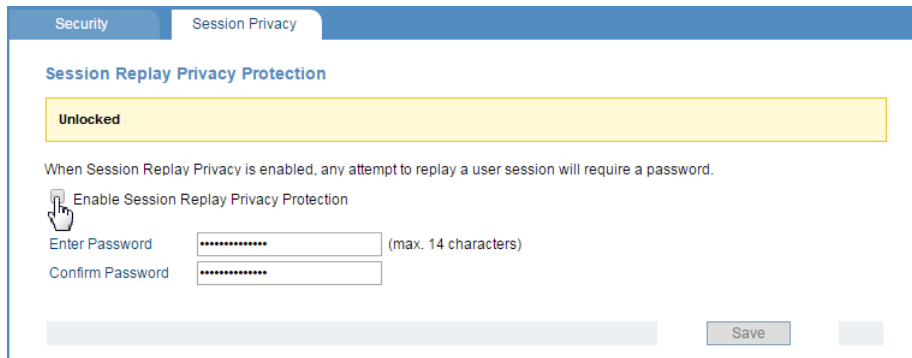
To disable Session Replay Privacy protection and/or change the password

- 1) In the **Configuration > Security > Session Privacy** tab, enter the Session Replay Privacy password, and click the **Unlock** button.

The screenshot shows the same ObserveIT web console interface as the previous one, but now the 'Session Privacy' tab displays a password unlock screen. A message at the top says: 'This page is password protected: Enter the session replay password to unlock this page.' Below this is a single password input field with masked characters. To the right of the input field is an 'Unlock' button, which is being clicked by a mouse cursor. Below the unlock section, the same 'Session Replay Privacy Protection' settings are visible, including the checked 'Enable Session Replay Privacy Protection' checkbox and the 'Enter Password' and 'Confirm Password' fields. A 'Save' button is at the bottom right.

After the correct password has been entered, you can disable Session Replay Privacy protection or change the password.

- 2) Clear the **Enable Session Replay Privacy Protection** check box.
- 3) Enter and confirm the new password, as required.
- 4) Click **Save**.



The screenshot shows a web interface for configuring session privacy. At the top, there are two tabs: 'Security' and 'Session Privacy', with 'Session Privacy' being the active tab. Below the tabs, the title 'Session Replay Privacy Protection' is displayed. A yellow box with the text 'Unlocked' indicates the current status. Below this, a message states: 'When Session Replay Privacy is enabled, any attempt to replay a user session will require a password.' There is a checkbox labeled 'Enable Session Replay Privacy Protection' which is currently unchecked. Below the checkbox are two password input fields: 'Enter Password' and 'Confirm Password', both containing masked characters (dots). To the right of the 'Enter Password' field, it says '(max. 14 characters)'. At the bottom right of the form, there is a 'Save' button.

Activity Alerts

Alerts (also known as "activity alerts") are user-defined notifications which are generated when suspicious login events or user activity occurs during a session. Alert rules, configured by ObserveIT administrators, define the conditions under which an alert will be triggered.

The **Activity Alerts** feature provides ObserveIT with a proactive, real-time detection and defense mechanism.

This feature enables ObserveIT administrators to configure fully customizable and flexible rules which define the conditions in which user actions will cause alerts to be generated. Alerts are based on suspicious login events or user activities that occur during a session. By highlighting suspicious user activity events in real-time, administrators, and IT security personnel can respond quickly and effectively to any deliberate or inadvertent threats to system integrity, IT security, regulatory compliance, or company policy.

Note: The ObserveIT installation package includes a list of sample alert rules which can be used as a basis for customizing alert rules.

ObserveIT administrators can view and manage activity alerts from the **Activity Alerts** tab in the ObserveIT Web Console. Generated activity alerts are also highlighted in the **User Diary**, **Server Diary**, and **Search** pages, as well as in the session video player. ObserveIT administrators can create and manage alert rules from the **Activity Alert Rules** page in the ObserveIT Web Console (by selecting **Configuration > Alerts > Activity Alert Rules**). After defining an alert rule, the administrator can configure an alert notification policy for users who will receive email notification about the alert. An alert notification policy defines which alerts are sent to which email addresses and at what frequency (for example, as every alert happens, as a digest once every x minutes, or as a daily digest).

Activity alerts can also be easily integrated into an organization's existing SIEM system.

Activity Alert Examples

Following are some examples of login and user activities that might trigger alerts:

- Irregular access to a company's financial servers, during non-working hours.
- External vendor login to database servers during non-working days.
- A non-administrator user accessing a sensitive system file (for example, `hosts` file).
- A Unix user attempting to change credentials to privileged user.
- Users browsing illegal Websites from work.

Example of an Alert Management Process

- 1) An ObserveIT administrator defines a rule that will trigger an alert when suspicious activity occurs (for example, a suspicious command, window, or text appears in a command line or on the screen).
- 2) An alert is triggered.
- 3) ObserveIT user/administrator receives an email notification about the alert.
- 4) Via a link in the email, the user opens the alert in the Web Console's **Activity Alerts** page for further investigation.
- 5) User can view the alert details in list, full details, or slideshow mode. Users can also search for the alert by its ID.

- 6) User can click the **Video** icon  next to the alert to launch the **ObserveIT Session Player**, which will replay all the slides of the session in which the alert occurred.
- 7) If required, upon reviewing the slide(s) which triggered the alert, user can navigate back to the alert in the **Activity Alerts** page, and flag it for follow up.

Viewing and Managing Activity Alerts

The following sections describe how to view and manage activity alerts and alert rules:

- [Managing Activity Alerts](#): describes how to filter alerts according to specified criteria, view alerts in different modes in the Web Console, flag alerts for follow-up, print and export alerts, delete alerts, and receive alert notification emails.
- [Viewing Alert Indications in the Web Console](#): describes how to view sessions that have alerts, view alerts in recorded session videos (in the Session Player), and search for sessions according to an alert ID.
- [Managing Alert Rules](#): describes how to view alert rules in different modes, create, edit, duplicate, and delete alert rules, and how to define alert notification policies.
- [Integrating Alerts in SIEM Products](#): describes how to integrate alerts into your organization's existing SIEM system.

Managing Activity Alerts

The **Activity Alerts** page provides information about alerts enabling administrators to view and manage activity alerts in the Web Console.

Important: Alerts are triggered by alert rules which define the conditions that could signify suspicious activity on ObserveIT monitored servers. ObserveIT administrators can create and manage alert rules from the **Activity Alert Rules** page (by selecting **Configuration > Alerts > Activity Alert Rules** in the ObserveIT Web Console). For further details, see [Managing Alert Rules](#).

To open the **Activity Alerts** page, click the **Activity Alerts** tab in the ObserveIT Web Console. The **Activity Alerts** page opens in List view which is the default mode, displaying a list of alerts according to the specified severity and filter criteria.

Activity Alerts

Period: ☐ Last 6 months ☐ Between 1/1/2014 and 2/28/2014

Severity: Alert rule:

Show:

1 - 20 of 1955 1 2 ... 84 85 Next > Last >>

Time	Alert	Login	User	Server	Video
2/9/2014					
2:19 PM	After-hours Login to DB server...	administrator	lan	OITHostedDem...	Video
7:56 AM	Opened Hosts file	administrator	lan	OITHostedDem...	Video
5:18 AM	After-hours Login to DB server...	administrator	lan	OITHostedDem...	Video
2/6/2014					
8:31 PM	After-hours Login to DB server...	administrator	lan	OITHostedDem...	Video
8:24 PM	Opened Hosts file	administrator	lan	OITHostedDem...	Video
1:48 PM	After-hours Login to DB server...	administrator	ami	OITHostedDem...	Video
1:17 PM	Opened Regedit	administrator	lan	OITHostedDem...	Video
12:27 PM	After-hours Login to DB server...	administrator	dpetri	OITHostedDem...	Video

Alert Viewing Modes

You can view alerts in different modes. To switch between modes, click the required icon:

	List view	In this view, you can see at a glance all the alerts that are already configured according to the specified filter criteria.
	Details view	In this view, you can see for each alert exactly Who? Did What? On Which Computer? When? and From Which client?
	Gallery view	The Gallery view provides a slideshow of the screenshots for each alert alongside the alert's details. By viewing alerts in this mode, you can see clearly the user environment and the context of exactly what the user was doing when an alert was triggered.

Activity Alert Tasks

The tasks you can perform on activity alerts include:

- [Filtering Alerts](#): Display the alerts according to your own specified criteria.
- [Viewing a List of Alerts](#): View the alerts that were generated during a specified time period and according to specified criteria.
- [Viewing Alert Details \(Who? Did? What?...\)](#) : View exactly Who? Did what? On which computer? From which client? When? for each alert.
- [Viewing Alerts in Gallery Mode](#): Browse through the screenshots of each alert while showing the full details near each screen.
- [Flagging Alerts for Follow-Up](#): Highlight alerts that require more attention by flagging them.
- [Printing and Exporting Alerts](#): Print the **Alerts** list and export it to Excel.
- [Deleting Alerts](#): Delete alerts that are no longer required.
- [Receiving Alert Notifications by Email](#): Receive email alerts to quickly identify alerts and respond accordingly.
- [Viewing Sessions with Alerts](#): View recorded sessions which contain alerts (marked alert indications) in the **Server Diary**, **User Diary**, and/or **Search** lists
- [Viewing Alerts in the Session's Video](#): Replay videos of sessions with alerts in the **Session Player**.
- [Searching for Sessions by Alert ID](#): From the **Activity Alerts Details** view, click an **Alert ID** link to open the **Search** page filtered to display a session according to a particular alert ID, in order to view additional information about the session and the context of the activity that caused the alert with that ID.

Filtering Alerts

In the **Activity Alerts** page, you can filter the alerts displayed in the **Alerts** list per specified criteria.

To filter the alerts displayed in the Alerts list

- 1) In the **Period** field, specify the time period (**Last**) or a date range for your search (**Between**).

Period: ☒ Last Months ☐ Between and

Severity: Alert rule:

More Filters

Server: Login:

Server group: User (secondary):

Client: Flagged:

Alert ID:

[Reset](#) [Show](#)

- 2) From the **Severity** drop-down list, select the alert severity level that you want to view (**High**, **Medium**, **Low**, or select **All** to view all).
- 3) From the **Alert rule** drop-down list, select the alert rule that you want to view (or select **All** to view all).
- 4) Expand the **More Filters** section by clicking to filter the alerts displayed according to additional criteria, as described in the table below.
- 5) In the **Alert ID** text box, type the ID of the particular alert that you want to view. (Note that "search" is enabled only according to the *exact* alert ID.)
- 6) When you have finished defining your search criteria, click **Show** to update the **Alerts** list according to the specified details.

To clear the filter fields, click **Reset**.

More Filters

Filter	Description
Server	To search for alerts by the servers on which the alerts occurred, select a specific server from the list, or select All to view all alerts.
Server group	To search for alerts by the server group which includes the servers on which the alerts occurred, select a specific server group from the list, or select All to view all alerts.
Client	To search for alerts by the client computer from which the user who ran the session logged in, select a specific client from the list, or select All to view all alerts.
Login	To search for alerts by the login name of the user who ran the session in which the alerts occurred, select a specific login name from the list, or select All to view all alerts.
User (secondary)	To search for alerts by the secondary identification of the user who ran the session in which the alerts occurred, select a specific user name from the list, or select All to view all alerts.
Flagged	To search for alerts by whether they were flagged or not flagged select Yes (flagged) or No (not flagged), or select All to view all events.

Viewing a List of Alerts

In the **Activity Alerts** page, you can view the names and severities of all generated alerts, with the newest alerts at the top (organized by date/time and color coded per severity level). You can expand an alert row to view more details (including the conditions which triggered the alert).

To view a list of alerts

- 1) Click the **Activity Alerts** tab.

The **Activity Alerts** page opens in List view which is the default mode.

- 2) To switch to **List** mode from another viewing mode, click the **List**  icon in the **Show** area of the **Activity Alerts** page.

In **List** mode, you can view a list of alerts that are already configured according to the specified filter criteria. One line of information is shown about each alert.

Note: You can print the **Alerts** list and/or export it to Excel (see [Printing and Exporting Alerts](#)). Alerts can be deleted **ONLY** by ObserveIT Administrators (see [Deleting Alerts](#)).

For each alert, the following information is displayed according to the "filtered" details (see [Filtering Alerts](#)):

	Click to show details of the alert.
Time	Time that the alert was triggered. Alerts are generated as close as possible to the time they occur. In case of a delay between the alert generation and the time of reporting it (such as, Agent offline, communication issues, and so on), the date and time of the alert reflects the time it was generated, regardless of the delay.
Flag icon	Indication of whether the alert is currently flagged for follow-up.
Alert	Name of the alert that was triggered. For example, "After-hours login to DB server".
Login	Login name of the user who ran the session in which the alert occurred.
User	Secondary identification of the user who ran the session in which the alert(s) occurred.
Server	Server on which the alert occurred.
Video icon	When clicked, opens the Session Player at the screen location where the alert was generated.

Viewing Alert Details (Who? Did? What?...)

In **Details** mode, you can view details of the conditions that contributed to the generation of the alert. You can see exactly "Who?" "Did what?" "On which computer?", "From Which client?" and "When?".

For details of the conditions and instructions on how to configure them, see [Creating Alert Rules](#).

To view the alerts in Details mode

- 1) In the **Show** area of the **Activity Alerts** page, click the **Details**  icon.

The **Details** mode displays the expanded details for each alert (same as if you clicked  to expand each list view item).

Activity Alerts

Period: ☒ Last 1 Months ☐ Between 07/15/2014 and 07/23/2014

Severity: All Alert rule: All

More Filters

Server: All Login: All

Server group: All User (secondary): All

Client: All Flagged:  All

Alert ID: [Reset](#) [Show](#)

Show:   

1 - 11 of 11

Time	Alert	Login	User	Server	Video
7/21/2014					
03:05 PM	Browsing SETTINGS pages	micky	n/a	OBSERVEIT-PM	
	OBSERVEIT-PM/micky View rule details				
	Opened window: Microsoft SQL Server Management Studio				
	OBSERVEIT-PM				
	OIT-MICKY (10.1.100.100)				
	Monday, 7/21/2014 3:05 PM Alert ID: 10000010				
01:27 PM	Unix privileged deletion or copy	micky	n/a	oit-pm-linux	
	(none)/micky View rule details				
	Executed command with permission level root and other than own Executed command: /rm Executed command: rm				
	oit-pm-linux				
	localhost (:::1)				
	Monday, 7/21/2014 1:27 PM Alert ID: 10000009				

- 2) In **Details** mode, you can view the details of the conditions that contributed to the generation of the alert, as described in the following table.

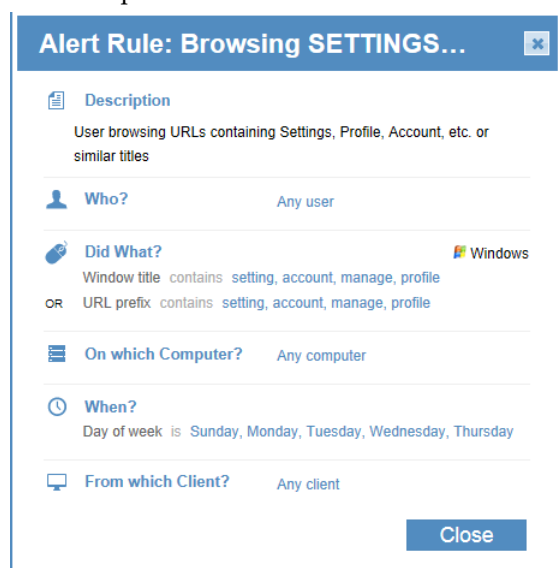
Who?	Who is the user on which the alert will be generated?
Did What?	What actions did the user do? For example, you can see which URLs the user visited, which applications they ran, and so on.
On Which Computer?	Name of the computer on which the action occurred.
From Which Client?	Name of the client domain\name or client IP address.
When?	What day/date/time did the action occur. In case of a delay between the alert generation and the time of reporting it (such as, Agent offline, communication issues, and so on), the date and time of the alert reflects the time it was generated, regardless of the delay.
View rule details	Click the View rule details link to view alert rule details (as described in the procedure below).
Alert ID	ID number of the alert. Click the Alert ID link to open the Search tab showing the session that contains the alert. (For further details, see Searching for Sessions by Alert ID.)

From the **Details** mode, you can view the alert rule details.

To view alert rule details

- Click the **View rule details** link.

A popup window opens, displaying the configured alert rule conditions that triggered the alert. For example:



Note: You can print the **Alerts** list and/or export it to Excel (see [Printing and Exporting Alerts](#)). Alerts can be deleted **ONLY** by ObserveIT Administrators (see [Deleting Alerts](#)).

Viewing Alerts in Gallery Mode

In **Gallery** mode, you can browse through the screenshots of each alert while viewing the full alert details next to each screen. Viewing alerts in **Gallery** mode provides a view of the user environment, enabling you to see the context of exactly what the user was doing when an alert was triggered.

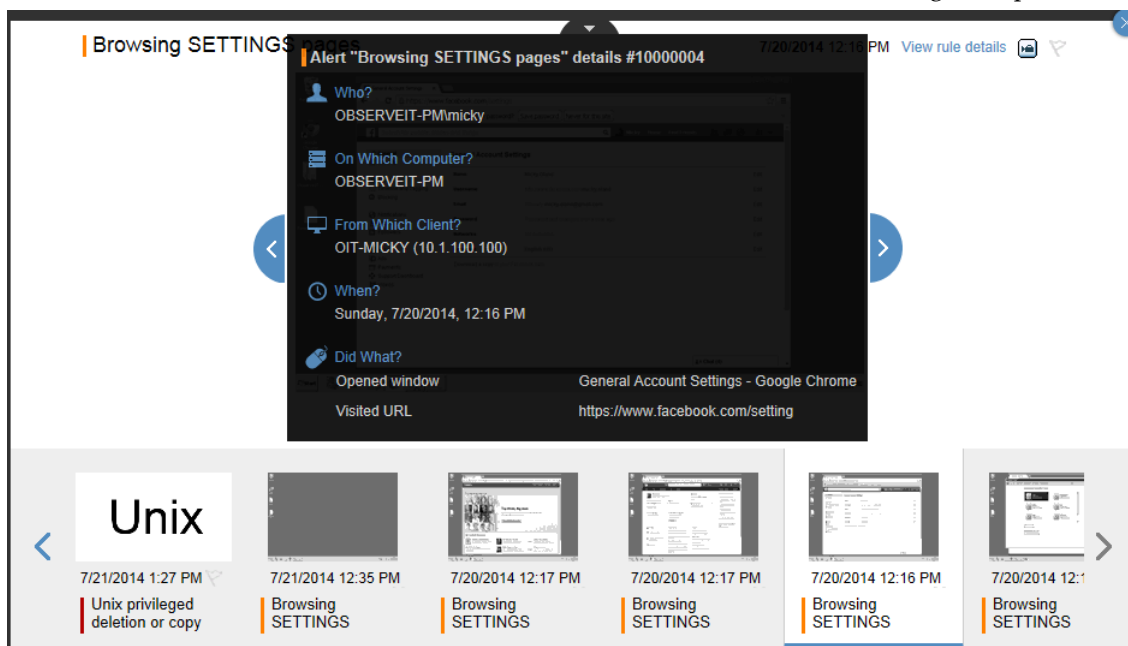
To view alerts in Gallery mode

- 1) In the **Activity Alerts** page, click the  icon in the **Show** area.

The **Gallery** mode displays screenshots of each alert.

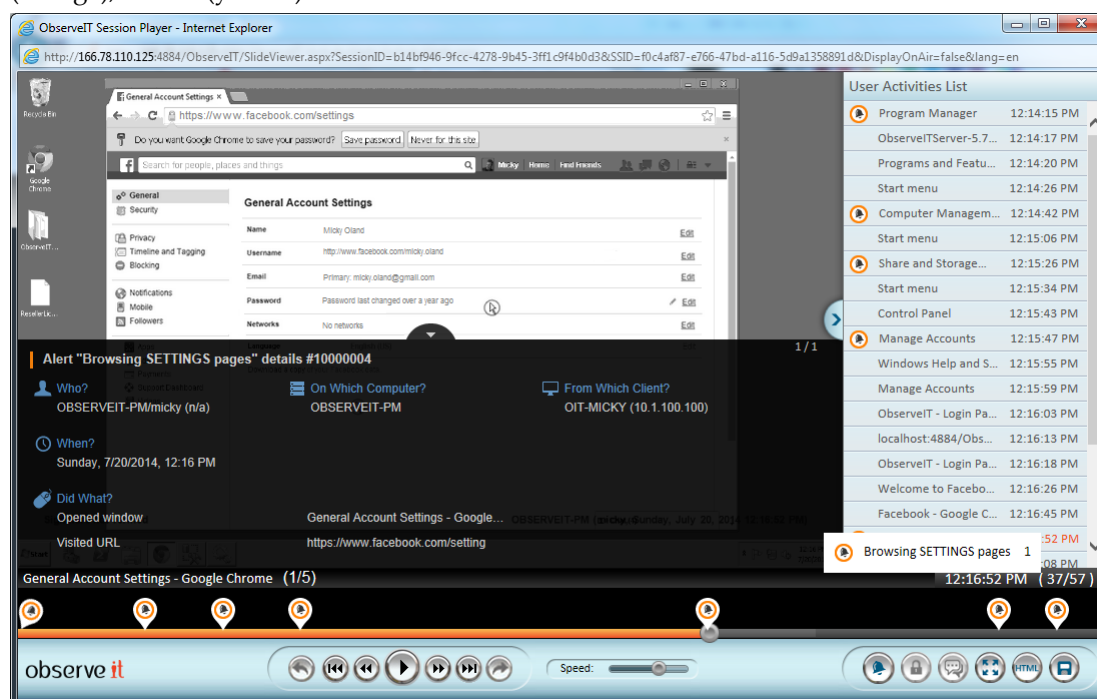
- 2) Browse through the screenshots by clicking the **Next**  or **Previous**  buttons. The alert details change accordingly.

- 3) Click the **Video**  icon to open the **Session Player** at the screen location where the alert was generated.
- 4) Click the  icon to maximize the screenshots view, as shown in the following example:



- 5) In maximized view, you can see a slideshow of the alert screenshots, with alert details emphasized.
- 6) Use the  and  buttons to move through the slideshow.
- 7) Select a slide in the slideshow to see the details of an alert maximized.
- 8) Click the **Video**  icon to open the **Session Player** at the screen location where the alert was generated.

The following shows an example of a video replay of a session during which a number of alerts occurred. The color of the ring around the alert icon shows the alert severity; high (red), medium (orange), or low (yellow).



For further details about viewing alerts in the **Session Player**, see [Viewing Alerts in the Session's Video](#).

For further details about how to use the ObserveIT **Session Player**, see [Windows Session Player](#) or [Unix Session Player](#) (in the User Guide).

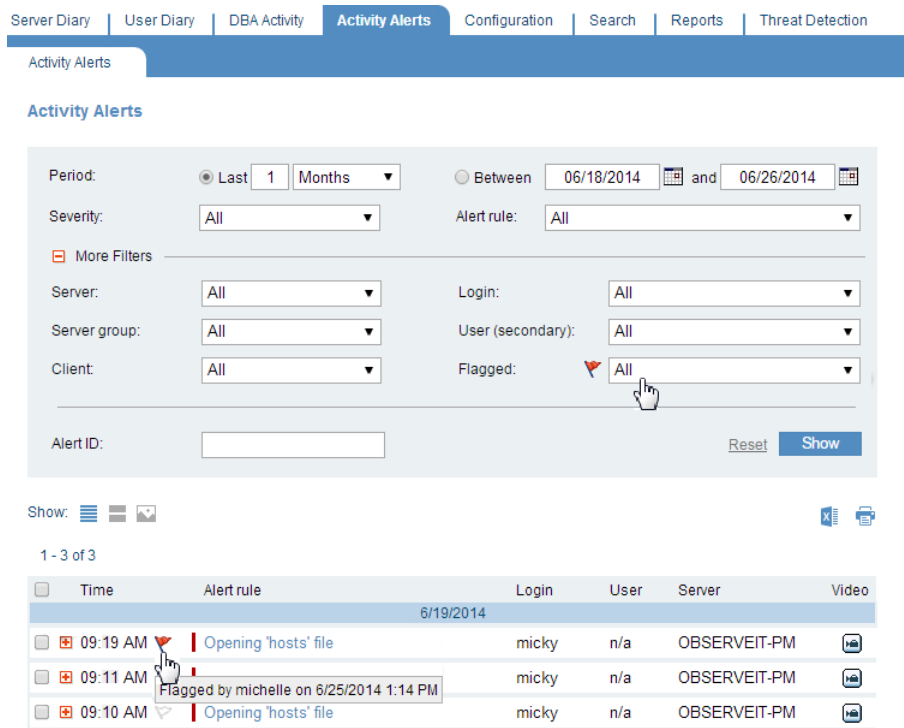
Note: You can print the **Alerts** list and/or export it to Excel (see [Printing and Exporting Alerts](#)). Alerts can be deleted **ONLY** by ObserveIT Administrators (see [Deleting Alerts](#)).

Flagging Alerts for Follow-Up

Flagging an alert enables you to highlight an event that requires further attention. After flagging an alert, it cannot be archived or deleted from the system.

To flag alerts for follow-up

- 1) In the **Activity Alerts** page, click the **Flag**  icon next to the alert to flag/un-flag it.



Activity Alerts

Period: ☐ Last 1 Months ☐ Between 06/18/2014 and 06/26/2014

Severity: All Alert rule: All

More Filters

Server: All Login: All

Server group: All User (secondary): All

Client: All Flagged: All

Alert ID: Reset Show

Show: ☐ ☐ ☐

1 - 3 of 3

Time	Alert rule	Login	User	Server	Video
09:19 AM	Opening 'hosts' file	micky	n/a	OBSERVEIT-PM	
09:11 AM	Opening 'hosts' file	micky	n/a	OBSERVEIT-PM	
09:10 AM	Opening 'hosts' file	micky	n/a	OBSERVEIT-PM	

- 2) You can filter the list of alerts based on the flagged/not-flagged status.

Note the following:

- When flagging an alert, the system stores the Console user name and the time that the alert was flagged (this information is also shown in a tooltip).
- Only the user who flagged an alert (or the administrator) can un-flag it. The system stores the user name and time of the un-flagging (this information also shown in a tooltip).
- The same user can flag/un-flag an alert as many times as required, without any message interruption.

Printing and Exporting Alerts

ObserveIT allows you to export the **Alerts** list as displayed in HTML format to an external window for easier printing and for usage in Microsoft Excel.

To export the Alerts list

In the **Activity Alerts** page, click the following icons:

- Click  to open the **Alerts** list in a **Report To Export** browser window from which you can view or save the details as an Excel file.
- Click  to open the **Alerts** list in a **Report To Export** browser window, from which you can print the report as you would any browser window. From this window, you can click the **Excel** link to open the information as an Excel file.

Deleting Alerts

ObserveIT administrators can delete alerts that are no longer relevant, thus reducing the **Alerts** list to show only alerts that are flagged as important, and high severity alerts.

Note: Only an "Admin" user can delete alerts (that is, not any user with administrative permissions).

To delete an alert

- 1) In the **Activity Alerts** page, select the alerts you want to delete, and click the **Delete**  icon.
A confirmation dialog box opens.
- 2) Click **OK** to confirm the deletion.
The **Alerts** list refreshes.

Receiving Alert Notifications by Email

Alert notification policies enable ObserveIT administrators to define the email notifications that will be created when an alert is generated. These policies define to whom and how often emails will be sent in the event of an alert. By using configurable policies for alert notifications, they can be easily edited (for example, by changing the email address) and applied to multiple alert rules. Every Alert rule is associated with a single notification policy.

Note: Notification policies are available for selection in the **Activity Alert Rules** page.

When defining an alert notification policy (see [Defining Alert Notification Policies](#)), administrators can specify when and how often recipients will receive the email notification, by selecting one of the following options:

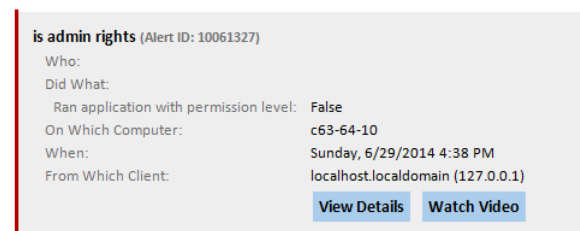
- Email on every alert (default frequency).
- Send digest email no more than once every X minutes.
- Send a daily digest email at a fixed time every day (for example, 08:00 AM).

The following examples show the email notification that users might receive when an alert is generated.

Note the following:

- The severity of the alert is indicated by a colored bar on the left (Red=High, Orange=Medium, Yellow=Low).
- Clicking the **View Details** button opens the maximized view of the alert in slideshow mode with the alert's details expanded.
- Clicking the **Watch Video** button launches the video player for this session at the time stamp of this alert.

Example of Individual Alert Email



Example of Alert Digest Emails

There are two types of alert digest emails:

- **Daily Alert Digest** email is sent at the designated time every 24 hours even if no alerts were generated in the prior 24 hours. If no alerts occurred, the subject remains the same (showing "0 alerts") and the body will contain only, "No alerts generated in the past 24 hours."
- **Alert Digest** email is sent every x minutes if new alerts were recently generated. The Alert Digest email is sent only when at least one alert was generated since the last digest was sent *and* the specified number of minutes passed since the last digest email.

Activity Alert Summary

High-severity Alerts

432 [UrlDomainNotEndsWithCom](#)

132 [GTWen](#)

1 [happy hippo 60](#)

Low-severity Alerts

1 [Load Test Rule](#)

1 [Load Test Complex Rule](#)

Activity Alert Details (10 of 567 shown here | [view all](#))

High-severity Alerts (10 of 565 shown here)

UrlDomainNotEndsWithCom (Alert ID: 10060230)

Who: observeit-sys.local\lili
On Which Computer: OIT-LILI
When: Monday, 1/1/1753 12:00 AM
From Which Client: local (127.0.0.1)

[View Details](#)[Watch Video](#)

UrlDomainNotEndsWithCom (Alert ID: 10060500)

Who: observeit-sys.local\lili
On Which Computer: OIT-LILI
When: Monday, 1/1/1753 12:00 AM
From Which Client: local (127.0.0.1)

[View Details](#)[Watch Video](#)

UrlDomainNotEndsWithCom (Alert ID: 10060212)

Who: (none)\lili (ObserveIT.Authentication\al)
On Which Computer: localhost.localdomain
When: Monday, 1/1/1753 12:00 AM
From Which Client: oit-liliya.observeit-sys.local (10.1.100.114)

[View Details](#)[Watch Video](#)

UrlDomainNotEndsWithCom (Alert ID: 10060412)

Who: observeit-sys.local\lili
On Which Computer: OIT-LILI
When: Monday, 1/1/1753 12:00 AM
From Which Client: local (127.0.0.1)

[View Details](#)[Watch Video](#)

UrlDomainNotEndsWithCom (Alert ID: 10060430)

Who: observeit-sys.local\lili
On Which Computer: OIT-LILI
When: Monday, 1/1/1753 12:00 AM
From Which Client: local (127.0.0.1)

[View Details](#)[Watch Video](#)

Viewing Alert Indications in the Web Console

Activity alerts that are generated on a session are also indicated in the ObserveIT **Server Diary**, **User Diary**, **Search** tab, and in the session's video player.

The topics in this section describe how to:

- [View alert indications in recorded sessions](#)
- [View alert indications in the Session Player](#)
- [Search for sessions with alerts according to alert IDs](#)

Viewing Sessions with Alerts

A recorded session that has one or more alerts, shows an alert indication in the **Server Diary**, **User Diary**, and/or **Search** lists.

To view sessions with alerts and related details

- 1) Click the relevant tab (**Server Diary**, **User Diary**, or **Search**).

Following is an example of the **Server Diary** showing medium severity alert indications next to some sessions.

The screenshot shows the 'Server Diary' tab selected in the top navigation bar. Below the navigation bar, there's a section for 'Activity View' with filters for Server (OBSERVEIT-PM), Period (Last 1 Month), and Start/End Date (Jul 22, 2014 to Jul 30, 2014). A table lists sessions with columns for Session Duration, Login, User, Server, Client, Slides, and Video. Four sessions are shown, each with an alert icon (a bell with an exclamation mark) next to the duration. The sessions are for 7/21/2014 and 7/20/2014.

Session Duration	Login	User	Server	Client	Slides	Video
3:05 PM - 3:05 PM	micky	n/a	OBSERVEIT-PM	OIT-MICKY	1	[icon]
12:35 PM - 12:38 PM	micky	n/a	OBSERVEIT-PM	OIT-MICKY	29	[icon]
12:14 PM - 12:17 PM	micky	n/a	OBSERVEIT-PM	OIT-MICKY	57	[icon]
11:25 AM - 11:45 AM	micky	n/a	OBSERVEIT-PM	OIT-MICKY	11	[icon]

- 2) Click the alert indication  icon next to a session.

A popup window opens showing the alerts (and the number of alert instances) that were generated during that session.

For example:

The screenshot shows a popup window with two alert entries. Each entry has an icon (a bell with an exclamation mark), a description, and a count in parentheses. The first entry is 'Browsing SETTINGS pages (7)' and the second is 'Accessing sensitive data (1)'. At the bottom, there are 'Close' and 'View all' buttons.

	Browsing SETTINGS pages	(7)
	Accessing sensitive data	(1)

Close View all

- 3) In the popup window, click an alert to open a maximized screenshot displaying the alert's details.

- 4) In the popup window, click **View all** to jump directly to the **Activity Alerts** page showing all the session alerts with all their details.

Server Diary | User Diary | DBA Activity | **Activity Alerts** | Configuration | Search | Reports | Threat Detection

Activity Alerts

Activity Alerts

Period: ☒ Last 1 Months ☐ Between 07/22/2014 and 07/30/2014

Severity: All Alert rule: All

More Filters

Alert content keyword: [Reset](#) [Show](#)

Show:

1 - 7 of 7

Time	Alert	Login	User	Server	Video
7/20/2014					
12:17 PM	Browsing SETTINGS pages	micky	n/a	OBSERVEIT-PM	
Who? OBSERVEIT-PM/micky View rule details					
Did What? Signed Out LinkedIn - Google Chrome Opened window Visited URL https://www.linkedin.com/uas/logout?session_full_logout=&csrftoken=ajax%3A8109911951292998364&trk=nav_account					
On which Computer? OBSERVEIT-PM					
From which Client? OIT-MICKY (10.1.100.100)					
When? Sunday, 7/20/2014 12:17 PM Alert ID: 10000006					
12:17 PM	Browsing SETTINGS pages	micky	n/a	OBSERVEIT-PM	
Who? OBSERVEIT-PM/micky View rule details					
Did What? Account & Settings LinkedIn - Google Chrome Opened window Visited URL https://www.linkedin.com/setting					
On which Computer? OBSERVEIT-PM					
From which Client? OIT-MICKY (10.1.100.100)					
When? Sunday, 7/20/2014 12:17 PM Alert ID: 10000005					
12:16 PM	Browsing SETTINGS pages	micky	n/a	OBSERVEIT-PM	
Who? OBSERVEIT-PM/micky View rule details					
Did What? General Account Settings - Google Chrome Opened window Visited URL https://www.facebook.com/setting					
On which Computer? OBSERVEIT-PM					
From which Client? OIT-MICKY (10.1.100.100)					
When? Sunday, 7/20/2014 12:16 PM Alert ID: 10000004					
12:15 PM	Browsing SETTINGS pages	micky	n/a	OBSERVEIT-PM	
Who? OBSERVEIT-PM/micky View rule details					
Did What? Manage Accounts Opened window					
On which Computer? OBSERVEIT-PM					
From which Client? OIT-MICKY (10.1.100.100)					
When? Sunday, 7/20/2014 12:15 PM Alert ID: 10000003					
12:15 PM	Browsing SETTINGS pages	micky	n/a	OBSERVEIT-PM	
Who? OBSERVEIT-PM/micky View rule details					
Did What? Share and Storage Management Opened window					
On which Computer? OBSERVEIT-PM					
From which Client? OIT-MICKY (10.1.100.100)					
When? Sunday, 7/20/2014 12:15 PM Alert ID: 10000002					
12:14 PM	Browsing SETTINGS pages	micky	n/a	OBSERVEIT-PM	
Who? OBSERVEIT-PM/micky View rule details					
Did What? Computer Management Opened window					
On which Computer? OBSERVEIT-PM					
From which Client? OIT-MICKY (10.1.100.100)					
When? Sunday, 7/20/2014 12:14 PM Alert ID: 10000001					
12:14 PM	Browsing SETTINGS pages	micky	n/a	OBSERVEIT-PM	
Who? OBSERVEIT-PM/micky View rule details					
Did What? Program Manager Opened window					
On which Computer? OBSERVEIT-PM					
From which Client? OIT-MICKY (10.1.100.100)					
When? Sunday, 7/20/2014 12:14 PM Alert ID: 10000000					

Viewing Alerts in the Session's Video

While replaying a recorded session using the **Session Player**, you can watch the session video for alert(s). If any alerts occurred on the session an alert indication  will be displayed. Note that the color of the ring around the alert icon shows the alert severity; high (red), medium (orange), or low (yellow).

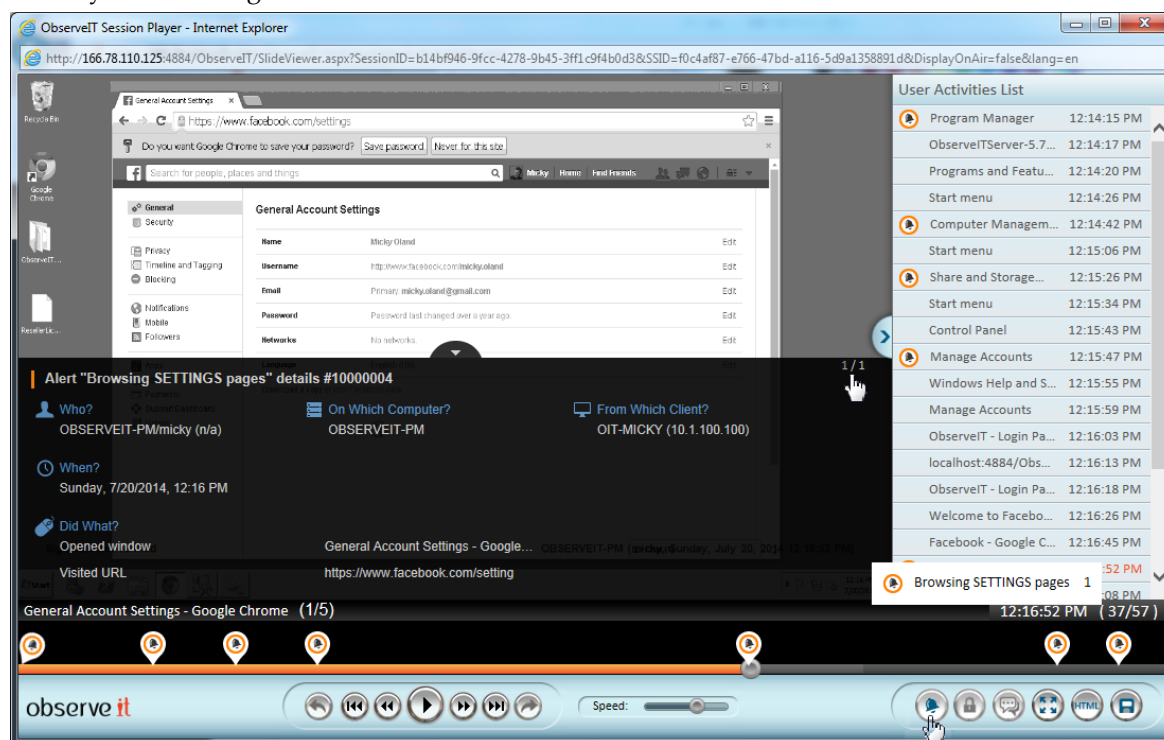
For instructions on how to use the ObserveIT **Session Player**, see Windows Session Player or Unix Session Player (in the User Guide).

To open a session's video for viewing alerts

- 1) In the **Activity Alerts List** view, **Details** view, or **Gallery** view, click the **Video**  icon next to the alert.

The **Session Player** opens. Details for each alert are displayed as the replay progresses.

Following is an example of a video replay of an ObserveIT session on which a number of medium severity alerts were generated.



- 2) In the **Alert Details Panel**, you can view a summary of the alert activity including alert name, severity, conditions, and the number of alerts in the session (in the upper right corner, for example, 1/1 in the above example).
- 3) Click the **Bell** icon  in the lower right part of the screen to toggle between showing or hiding the alert details, as required.
- 4) On the replay timeline bar, you can view alert indication icons, and hover over an alert icon to view the alert rule name.
- 5) In the **User Activities List** (on the right), you can view alert indications on the suspicious activities.

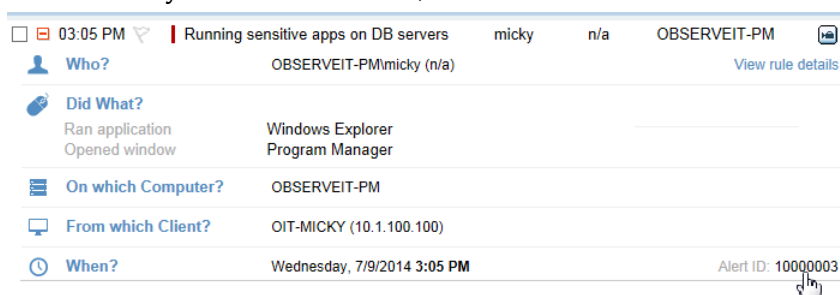
Searching for Sessions by Alert ID

In the **Search** page, you can search for sessions by alert ID. When viewing alerts in **Details** mode (see Viewing Alert Details (Who? Did? What? ...)), you can open the **Search** page filtered to display a session according to a particular alert ID.

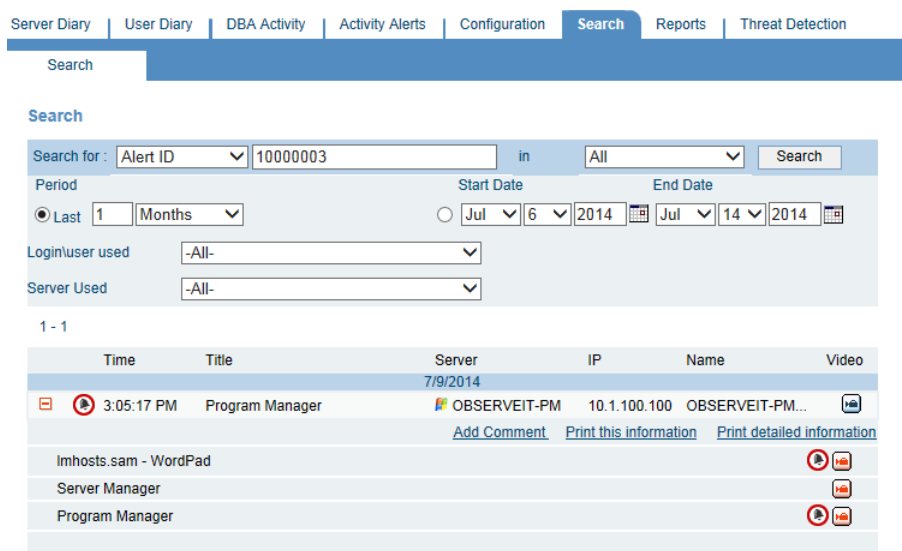
The **Search** page enables you view other information about the session that is not available in the **Activity Alerts Details** view (such as metadata, ticketing, and application information). This additional information could help you better understand the context of the activity that caused the alert. For further details about the ObserveIT **Search** feature, see Free Text Search (in the User Guide).

To search for a session by alert ID

- 1) In the **Activity Alerts Details** view, click the relevant **Alert ID** link.



The **Search** page opens, displaying the session with an alert of that ID, and marked with an alert indication .



- 2) Click  to expand the session to see exactly which slide has the alert.
- 3) Click the **Video**  icon next to the slide to open the **Session Player** for replaying the video of the session on which an alert was generated.

Managing Alert Rules

Alert rules define the conditions under which an alert will be triggered. Alert rules are configured by ObserveIT administrators, according to conditions which could signify suspicious activity on monitored servers. After defining an alert rule, the administrator can configure an alert notification policy which defines whom should be notified when the alert is generated, and how they will be notified.

Note: The ObserveIT installation package includes a list of sample alert rules which you can use as a basis to customize your own alert rules.

An alert rule comprises conditions that answer the following criteria:

- **Who?** - Who was logged in to the session when the alert was triggered?
- **Did what?** - What was the user doing when the alert was triggered?
- **On which computer?** - On which computer was the user logged in?
- **When?** - At what time was the alert triggered?
- **From which client?** - Which client computer was being used when the alert was triggered?

Managing and configuring alert rules is done from the **Activity Alert Rules** page in the ObserveIT Web Console. You can navigate to this page via **Configuration > Alerts > Activity Alert Rules**.

The screenshot displays the 'Manage Alert Rules' interface in the ObserveIT Web Console. The left sidebar contains navigation links for various system components. The main content area is divided into a filter section and a table of alert rules. The filter section includes dropdowns for Status, Severity, Notification policy, History, and Updated on, along with a date range selector. The table lists alert rules with their names, status, update dates, and update users. The 'SAMPLE - After-hours access to sensitive servers' rule is highlighted, and its details are expanded on the right. The details section provides a comprehensive overview of the rule's configuration, including its description, the user who triggered it, the action performed, the computer used, the time of day, and the client from which the alert was generated.

Alert Rule Name	Status	Updated on	Updated by
SAMPLE - Access from outside the organization	Inactive	1/4/2015	Admin
SAMPLE - After-hours access to sensitive servers	Inactive	1/4/2015	Admin
SAMPLE - Unix - User trying to remove a sensitive directory	Inactive	1/4/2015	Admin

Alert Rule Details:

- Description:** Remote vendors try to log in to servers belong to sensitive groups not during regular business hours, during weekends or holidays
- Who?** Login account [domain\name] is member of group RemoteVendor, Contractors
- Did What?** Logged in
- On Which Computer?** ObserveIT server group name is DBServers, FinanceServers
- When?** Day of week is Sunday, Saturday
OR Specific date is 01/09/2014,13/10/2014,31/10/2014
OR Time of day is not between 08:00 and 18:00
- From Which Client?** Any client

Alert Rule Tasks

The tasks you can perform from the **Activity Alert Rules** page include:

- [Viewing Alert Rules](#): View a list of alert rules that were generated during a specified time period and according to the criteria that you specify.
- [Filtering Alert Rules](#): Filter the alert rules displayed in the **Alert Rules** list per specified criteria
- [Creating Alert Rules](#): Define the alert rule criteria for creating new alert rules.
- [Defining the "Who?" Conditions](#): Define the alert rule "condition" that shows who was the logged in user on which an alert was triggered.
- [Defining the "Did What?" Conditions](#): Define the alert rule "condition" that shows exactly what the user was doing when the alert was triggered.
- [Defining the "On Which Computer" Conditions](#): Define the alert rule "condition" that shows on which computer the user was logged in when the alert was triggered.
- [Defining the "When?" Conditions](#): Define the alert rule "condition" that shows at what time/date the alert was triggered?
- [Defining the "From Which Client" Conditions](#): Define the alert rule "condition" that shows which client computer was being used when the alert was triggered.
- [Defining Alert Notification Policies](#): Define Alert Notification policies to determine who gets notified by email, and at what frequency.
- [Editing and Duplicating Alert Rules](#): Edit and duplicate alert rules, as required.
- [Deleting Alert Rules](#): Delete alert rules that are no longer required.

Viewing Alert Rules

In the **Activity Alert Rules** page, you can view and manage all the currently configured alert rules.

To view alert rules

- 1) Navigate to **Configuration > Alerts**.

The **Activity Alert Rules** tab opens by default in **List** view which is the default mode.

The screenshot displays the ObserveIT Configuration Guide interface. The top navigation bar includes links for Server Diary, User Diary, DBA Activity, Activity Alerts, Configuration (selected), Search, Reports, and Threat Detection. The left sidebar contains a menu with categories like Admin Dashboard, Console Users, Identification, Servers, Server Groups, Server Policies, Security, Alerts, System Events, Identity Theft Detection, Messages, Ticket Integration, License, SMTP Settings, Monitor Log, LDAP Settings, Storage, Archive, Saved Sessions, Audit, and System Log. The main content area is titled 'Activity Alert Rules' and 'Alert Notification Policies'. It features a 'Manage Alert Rules' section with a '+ Create New Alert Rule' button. Below this are filters for Status (All) and Severity (All), with a 'More Filters' button and 'Reset' and 'Show' buttons. A 'Show:' section indicates '1 - 17 of 17' items. A table lists three alert rules, all with a status of 'Inactive' and updated on '12/29/2014' by 'Admin'. The first rule is 'SAMPLE - Access from outside the organization', the second is 'SAMPLE - After-hours access to sensitive servers', and the third is 'SAMPLE - Unix - User trying to remove a sensitive directory'. Below the table, a 'Description' section states 'Removing sensitive data can cause data lose and may jeopardize system stability'. Other sections include 'Who?' (Any user), 'Did What?' (Executed Command: Command name is rm, AND Executed Command: Argument contains etc, bin, usr, AND Executed Command: Switch is -r, -f), 'On Which Computer?' (Any computer), 'When?' (Any time), and 'From Which Client?' (Any client).

- 2) You can filter the alert rules displayed in the **Alert rules** list, see [Filtering Alert Rules](#).
- 3) You can switch between **List** and **Details** modes, as described in the following procedures.

To view alert rules in List mode

- 1) In the **Show** area of the **Activity Alert Rules** page, click the **List**  icon.
The **List** mode displays one line of information is shown about each alert rule. This is the default mode.
Alert rules are presented by date in reverse chronological order so that the most recently defined rules appear at the top of the list.

For each alert rule in the list, the following information is displayed according to the "filtered" details, including the specified status (**All**, **Active**, or **Inactive**) and alert severity (**All**, **High**, **Medium**, **Low**):

Severity bar	A colored bar representing the severity of the alert rule: - Red: High severity - Orange: Medium severity - Yellow: Low severity
Alert Rule Name	A unique name that describes the alert rule. For example: "Opening 'hosts' file".
Status	Active or Inactive. When an Alert Rule is inactive, new alerts are not generated but old alerts are fully accessible. The default status for new rules is 'Inactive'.
Updated on	Date the rule was last updated.
Updated by	User who last updated this rule.

To view more details, you can click  next to an alert rule in the list, or you can switch to **Details** mode, as described below.

To view alert rules in Details mode

- In the **Show** area of the **Activity Alert Rules** page, click the **Details**  icon to view details for all alert rules on the page.

The **Details** mode displays a description, and a textual summary of the rules' parameters (that is, Who? Did what? On which computer? From which client? When?) for all the rules in the list.

In **Details** mode, you can view details of the alert rules including a description and details of exactly "Who? Did what? On which computer? From which client? When?".

Description	A description that provides a motivation for the alert rule. For example: "Alert if user views 'hosts' file in typical editors."
Who?	Who is the user on which the alert was generated?
Did What?	What actions did the user do?
On Which Computer?	Name of the computer on which the action occurred.
From Which Client?	Name of the client domain\name or client IP address.
When?	What day/date/time did the action occur.

Alert Rule Tasks

From the **Alert Rules** page, the tasks you can perform on activity alert rules include:

- Creating Alert Rules:** Create a new alert rule by clicking the **Create New Alert Rule** button to open the **Create Alert Rule** page where you can create the new alert rule.
- Editing and Duplicating Alert Rules:** Edit the rule by clicking the name of the relevant rule in the list to open the **Edit Alert Rule** page where you can edit the parameters currently defined for the selected alert rule. Duplicate the alert rule by clicking the **Duplicate** link next to the relevant rule to open the **Edit Alert Rule** page with a new Alert Rule initialized to the exact content of the selected item, named **Copy of <selected alert rule name>**, and edit this duplicate rule, as required.
- Deleting Alert Rules:** Delete an alert rule that is no longer required by clicking the **Delete** link next to the relevant rule in the list. The select alert rule is deleted, after confirmation.

Filtering Alert Rules

In the **Activity Alert Rules** tab, you can filter the alert rules displayed in the **Alert Rules** list per specified criteria.

To filter alert rules

- 1) From the **Status** drop-down list, select the status of the alert rules that you want to view (**Active**, **Inactive**, or select **All** to view both active and inactive rules).

- 2) From the **Severity** drop-down list, select the alert severity level that you want to view (**High**, **Medium**, **Low**, or select **All** to view all severities).
- 3) Expand the **More Filters** section by clicking  to filter the alert rules displayed according to additional criteria, as described in the table below.
- 4) When you have finished defining your search criteria, click **Show** to update the **Alert Rules** list. To clear the filter fields, click **Reset**.

More Filters

Filter	Description
Notification Policy	To search for alert rules by assigned notification policy (which specifies who receives alert notifications when an alert is generated and at what frequency), select a specific notification policy from the list, or select All to view all alert rules.
Alert rule keyword	To search for alert rules by alert rule keywords, type the relevant text in the text box. This enables you to search in the following fields in the Alert Rules list: • Alert Rule Name • Description (if there is no description, you cannot search on this field) • All rule content fields (for example server names, programs) • Updated by (for example, Console user name)
History	To search for alert rules by whether they were previously used, select Generated at least one alert , Never generated an alert , or select All to view all alert rules.
Last updated	To search for alert rules by the time period they were last updated, specify the specific time period (During last) or specify a date range for your search (Between).
Last updated by	To search for alert rules by the user who last updated them, select a specific user from the list, or select All to view all.

Creating Alert Rules

This topic describes how to create alert rules. For information about editing or duplicating existing alert rules, see [Editing and Duplicating Alert Rules](#).

The ObserveIT installation package includes a list of sample alert rules which can be used as a basis for customizing alert rules.

Note: Before you begin to create or edit alert rules, it is recommended that you read the topic [Understanding the Logic for Triggering Alerts](#), which describes the logic for defining alert conditions.

To create a new rule

- 1) In the **Activity Alert Rules** tab, click the **Create New Alert Rule** button.

The **Create Alert Rule** page opens without any defined content, enabling you to define the parameters and conditions required for your alert rule.

The screenshot shows the 'Create Alert Rule' page in the ObserveIT configuration interface. The page is titled 'Create Alert Rule' and is part of the 'Alert Notification Policies' section. It features a sidebar with navigation links like 'Admin Dashboard', 'Console Users', 'Identification', 'Servers', 'Server Groups', 'Server Policies', 'Security', 'Alerts', 'System Events', 'Identity Theft Detection', 'Messages', 'Ticket Integration', 'License', 'SMTP Settings', 'Monitor Log', 'LDAP Settings', 'Storage', 'Archive', 'Saved Sessions', 'Audit', and 'System Log'. The main content area includes fields for 'Name', 'Description', and 'Notification policy'. There are also sections for 'Who?' (Currently: Any user), 'Did What?' (on: Windows and Unix, Logged in), 'On Which Computer?' (Currently: Any computer), 'When?' (Currently: Any time), and 'From Which Client?' (Currently: Any client). At the bottom right, there are 'Cancel' and 'Save' buttons.

2) Define the alert rule details, as follows:

Field	Description
Name	Specify the name for the alert rule. For example: "Suspicious Unix activity after working hours".
Description	Provide a description for the rule that explains its meaning or motivation. For example: "Warn about irregular access to database servers and suspicious activity over the weekend."
Notification Policy	Select a notification policy that defines who should receive email notifications when an alert from this rule is triggered, and how often. For example: "Daily digest for Division Managers". To define the policy, click the  icon. For details, see Defining Alert Notification Policies . There is no default notification policy. New Alert Rules are created with no policy, which means that newly generated alerts will not trigger any email.

Status	Select the status of the alert rule: Active or Inactive .
Severity	Select the severity of the alert rule: High , Medium , or Low . The default severity for new rules is Medium . The severity of newly generated alerts is the severity of the rule that triggered the alert (that is, this field).

3. Define the conditions for the rule that will trigger the alert, as follows:

Condition	Description	For details, see
"Who?"	Who is the user on which the alert will be generated?	Defining the "Who?" Conditions
"Did What?"	What actions did the user do?	Defining the "Did What?" Conditions
"On Which Computer?"	Name of the computer on which the action occurred.	Defining the "On Which Computer" Conditions
"When?"	Name of the client domain\name or client IP address.	Defining the "When?" Conditions
"From Which Client?"	What day/date/time did the action occur.	Defining the "From Which Client" Conditions

4. When you have finished creating your alert rule, click **Save** to save your settings.

The newly configured alert rule is displayed in the **Activity Alert Rules** page.

Understanding the Logic for Triggering Alerts

An alert rule comprises conditions that define the criteria/logic for triggering an alert.

This topic describes the logic behind the alert conditions and the expected behavior of the system when defining alert rules. You should read this topic before you attempt to create or edit alert rules.

About Conditions

Each condition is evaluated as part of the rule. Each condition comprises:

- Field (that is being tested). For example: "Server name".
- Operator (for example, "is, is not, contains, ...").
- Value(s) (to test against). For example: "SRV, DB, LAP". Note that you can enter multiple values, separated by commas.

Rules for Configuring Alert Conditions

- For each of the "Who-Did What-....." sections, you can configure a number of alert conditions.
- To define an additional condition, click the  icon.
- To delete a condition, click the adjacent  icon.
- You can sort the order of your conditions by clicking the  icon.
- The "Who-Did What-....." sections always relate to each other with the "AND" logic. For example:

	Who?	User is John
--	------	--------------

AND	Did what?	Ran application Regedit
AND	On which computer?	Computer is DBSVR1
AND	When?	Day is Sunday

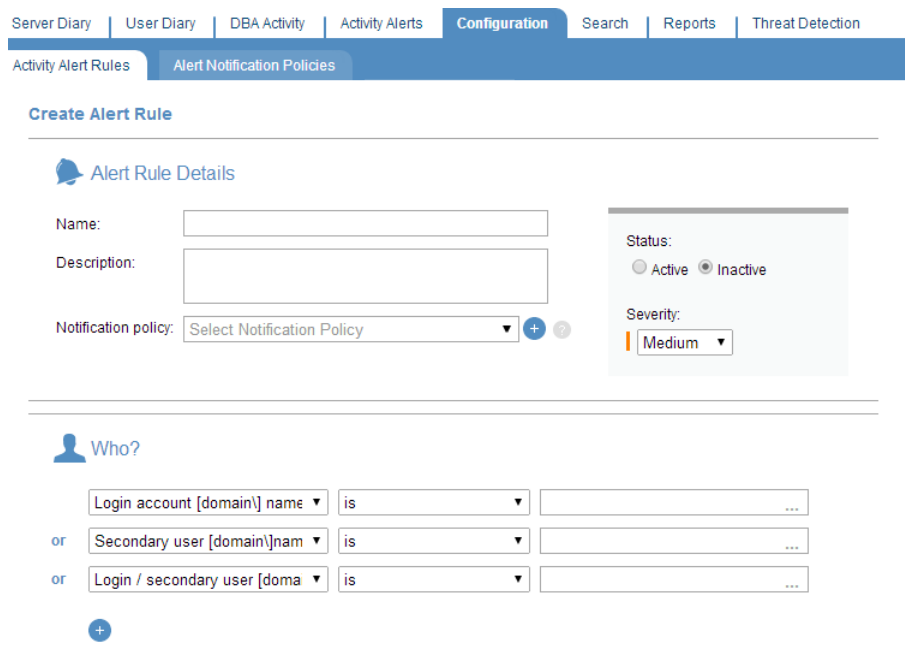
- You can choose whether all conditions within a "Who-Did What-....." section must match (by using the "AND" logic), or whether any of the conditions may apply (by using the "OR" logic). You cannot configure "AND" and "OR" conditions within the same criteria section. To switch between "AND" and "OR", simply click on the text.
- A negative condition, for example, "Window title does not contain x, y, z", means that the Window title does not contain "x", nor "y", nor "z".
- The system should trigger a new alert if any of the matched conditions are different from previously triggered alerts. For example, when the condition "User ran application Regedit, SQL Manager, or CMD" is defined, an alert is triggered if the user runs "Regedit" or "CMD".

Defining the "Who?" Conditions

In the **Who?** section of the **Create Alert Rule** page, you can define (or edit) the individual(s) or groups of users who performed the activity on which an alert will be generated.

To define the "Who?" conditions

- Open the **Who?** section by clicking  or the **Edit**  icon.



The screenshot shows the 'Create Alert Rule' page. At the top, there are tabs for 'Server Diary', 'User Diary', 'DBA Activity', 'Activity Alerts', 'Configuration', 'Search', 'Reports', and 'Threat Detection'. Below these is a sub-header 'Activity Alert Rules' with a tab for 'Alert Notification Policies'. The main section is titled 'Create Alert Rule' and contains 'Alert Rule Details'. This section includes fields for 'Name', 'Description', and 'Notification policy' (a dropdown menu). To the right, there are 'Status' (radio buttons for 'Active' and 'Inactive') and 'Severity' (a dropdown menu set to 'Medium'). Below this is the 'Who?' section, which has a header with a user icon and the text 'Who?'. It contains three rows of conditions, each with a dropdown menu for the user type, a logical operator (is), and a text input field for the value. The rows are: 'Login account [domain] name', 'Secondary user [domain] name', and 'Login / secondary user [domain] name'. There is a plus icon at the bottom left of the 'Who?' section to add more conditions.

Important: Before you begin, make sure that you have read the "Rules for Configuring Alert Conditions" described in [Understanding the Logic for Triggering Alerts](#).

- To define the individual(s) or groups of users who performed the activity on which an alert will be generated, select the relevant user type options, as described in the following table.

Options for Defining the "Who" Conditions

Field Option	Operators	Usage Examples
Login account [domain\]name	• is • is not • contains • does not contain • starts with • does not start with • ends with • does not end with • is member of group • undefined	Use this option to specify the name (and optionally, the domain) of regular users who are logged in. Examples: • If the required user belongs to a specific domain (for example, "observeit"), you can define the condition: "Login account [domain\]name is observeit.com\john, observeit.com\root" • If you do not want to specify a domain for the user, you can define the condition: "Login account [domain\]name is john, root, any user"
Secondary user [domain\]name		Use this option to specify the name (and optionally, the domain) of users for whom secondary authentication is required. For example: "Secondary user [domain\]name is observeit-sys\james"
Login/Secondary user [domain\]name		Use this option if the required user could be a regular or secondary authentication user. For example: "Login/Secondary user [domain\]name contains observeit.com\john"

Defining the "Did What?" Conditions

In the **Did What** section of the **Create Alert Rule** page, you can define conditions of suspicious user activities which would trigger an alert, based on recorded ObserveIT metadata for Windows and Unix/Linux operating systems.

On Windows, you can search for users who logged in, ran a specific application, viewed a specific window's title, visited a URL, or executed an SQL command containing keywords (for example, a table name).

On Unix/Linux, you can search for users who logged in, executed a specific command (based on command name, full path, arguments, command switches) or acted under a different user's permissions.

Numerous options are available to help you configure the exact conditions that must be met in order for the alert rule to be active. Example scenarios are provided in subsequent topics to help you understand how to configure **Did What?** conditions, using the group and field options in the **Create Alert Rule** page.

Note: You can use the **Logged in** option to generate an alert when a user logs in to either a Windows or Unix/Linux computer. It is the default activity that appears when creating a new alert rule, and it cannot be combined with any other **Did What** activity. **Without specifying some additional criteria related to this activity, countless alerts will be generated—in fact every time someone logs in to any monitored computer!** Therefore, it is important to specify particular users, servers, days/times, and so forth—so that you receive only relevant alerts.

The following procedure describes the steps required for defining the **Did What?** conditions, how to define the frequency of alert generation, and the available group and field options.

To define the "Did What?" conditions

- 1) Open the **Did What** section by clicking  **Did What?** or the **Edit**  icon.

The following figure provides an example of some configured **Did What?** conditions.

Edit Alert Rule

Alert Rule Details

Name: Opening 'hosts' file

Description: Alert if user views 'hosts' file in typical editors

Notification policy: Immediate email

Status: ☒ Active ☐ Inactive

Severity: High

Who? Currently: Any user

Did What? Alert only once: Per session on: Unix

Executed Co... : Command name is rm

and Executed Co... : Argument is /var/run/observeit

and Executed Co... : Switch is -f, -f

Important: Before you begin, make sure that you have read the "Rules for Configuring Alert Conditions" described in [Understanding the Logic for Triggering Alerts](#).

2) Define the alert frequency.

Note: The alert frequency applies to all the **Did-What** options (except for the **Logged-In** option since it is not relevant). You must take the alert frequency into account when defining conditions.

An alert can be triggered by a specific event (for example, a Window title containing "host"), which may repeat itself for succeeding screenshots (for example, if the user keeps working in Notepad the word "hosts" is triggered from almost every recorded screen). In this case, generating an alert for every screen is not feasible, and it would probably be sufficient to generate an alert only once in a user session. To prevent too many alerts from being generated for the same event, ObserveIT lets you define the frequency of alert generation which controls the number of times an alert can be triggered.

From the **Alert only once** drop-down list, select an option to prevent alerts from being generated more than once per session, once per application/process, or once per the specified number of minutes:

Alert only once: Per session

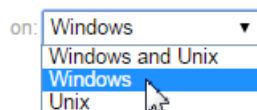
Per session

Per process

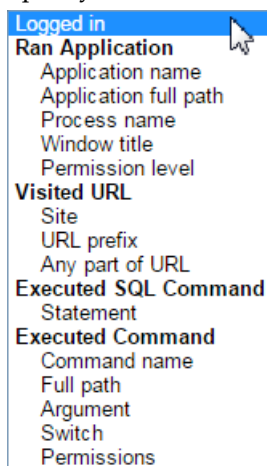
Every x minutes:

- **Per session** (default): Generate an alert only on the first occurrence of every unique match of the rule in each user session.
- **Per process**: Generate an alert on the first occurrence of every unique match of the rule per application/process (based on process ID) within each session. For example, you could select this option to generate an alert each time that an unauthorized user accesses a specific sensitive file (such as, "regedit.exe") during a session.

- **Every x minutes:** Do not generate an alert if the same conditions trigger within X minutes of the last alert generated with the same conditions. If you select this option, specify the number of minutes in the adjacent field box. For example, you might select this option if you do not want to be alerted every time the user browses an illegal Website, but only at specific time intervals.
- 3) From the **On:** drop-down list, select **Windows and Unix** or **Windows** or **Unix** depending on the required operating system.



- 4) Specify the field to be tested by selecting an option from the drop-down list:



Note: The available field options depend on the selected operating system. If you switch between operating system options, all currently defined conditions will be deleted.

- When **Windows and Unix** is selected, *all* the group and field options are available.
 - When **Windows** is selected, the following groups of options are available:
 - Logged in
 - Ran Application
 - Visited URL
 - Executed SQL Command
 - When **Unix** is selected, the following groups of options are available:
 - Logged in
 - Executed Command
- 5) Select the required operator for the condition from the drop-down list (for example, is, is not, does not start with, contains, and so on).
- 6) Specify the value(s) against which to test the condition. Note that you can enter multiple values, separated by commas. Multiple commas use the "OR" logic.
- 7) Repeat the above steps for each condition that you want to define.
- 8) When you have finished, click **Save** to save your settings.

The following topics provide some scenarios which are designed to help you understand how to configure **Did What?** conditions using the group and field options in the **Create Alert Rule** page:

- [How to Configure the "Ran Application" Group Options](#)
- [How to Configure the "Visited URL" Group Options](#)
- [How to Define an "Executed SQL Command" Statement](#)
- [How to Configure the "Executed Command" Group Options](#)

How to Configure the "Ran Application" Group Options

This topic provides details and a typical scenario to help you understand how to configure the **Did What?** field options in the **Ran Application** group.

Note: These options apply to Windows operating systems only.

For general information about defining **Did What?** conditions, see [Defining the "Did What?" Conditions](#).

The **Ran Application** group includes the following options for configuring conditions:

Option	Description	When should I use this option?	Condition Examples
Application name	Name of the application that the user ran. Note: Application names are listed in the Windows Task Manager.	Use this option if you want to configure an alert when the user runs a specific application.	"Ran Application: Application name is SSMS - SQL Server Management Studio" Other value examples: "regedit, install, setup"
Application full path	Full path of the application that the user ran.	Use this option if you want to configure an alert based on the explicit path to the application.	"Ran Application: Application full path is C:\Program Files\OpenVPN\bin\openvpn.exe"
Process name	Name of the process that the user ran.	Use this option if you want to configure an alert when the user runs a specific process.	"Ran Application: Process name is regedit, WINWORD, iexplore, services Note: You must specify the process name without the file extension (for example, "regedit" instead of "regedit.exe").
Window title	Title of a window that was opened by the user.	Use this option if you want to configure an alert when a specific window title is opened or when the title contains specific words that you are looking for.	• "Ran Application: Window title is hosts.txt - Notepad, Viewing Alerts.docx - Microsoft Word • "Ran Application: Window title contains host, permission, security

Permission level	Logged-in user's permissions level.	Use the "is Admin" permission level to check that an application is run with elevated permissions (Admin permissions).	"Ran Application: Permission level is Admin"
		Use the "is not Admin" permission level to check if a user is trying to run an application without "root/admin" permissions on the logged-in server.	"Ran Application: Permission level is not Admin"

Example Scenario

The following scenario provide some examples of how to use some of the **Ran Application** options to configure the conditions for an alert rule.

Alert rule example: Trigger an alert when an unauthorized (non-administrator) user tries to view a sensitive system or configuration file (such as regedit).

Note: For purposes of this example, the scope of the alert rule is "per session", which means that an alert will be generated only on the first occurrence of every unique match of the rule in each session. Full details about defining the scope of rules are provided in [Defining the "Did What?" Conditions](#).

Condition Example	Description	User Activity	Alert Generated?
"Ran application: Application name is Regedit, SSMS - SQL Server Management Studio, Setup, Notepad"	This condition specifies that every first time in a session that the user runs the Regedit, SQL Manager, Setup or Notepad applications, an alert should be generated.	1. User logs in to a session and runs the Regedit application.	YES Alert will be generated because the application name matches the condition.
		2. Within the same session, the user runs Setup.	YES An alert is generated because even though this is the same session, this application name also matches the condition.
		3. Within the same session, the user runs the Regedit application.	NO An alert is not generated because this is not the first time in the session that the user runs this application.
"Ran application: Window title contains hosts, permissions, security"			YES

	This condition specifies that every first time in a session a window title contains the word "hosts", "permissions" or "security", an alert should be generated.	1. User logs in to a session and opens the sensitive "hosts.txt" file in Notepad. The window title shows "hosts.txt" - Notepad".	
		2. Within the same session, the user opens a document entitled "Viewing permissions.docx - Microsoft Word".	YES An alert is generated because even though this is the same session, the window title contains a word that matches the condition.
"Ran application: Permission level is not Admin"	This condition specifies that an alert should be generated if the logged-in user does not have Administrator permissions.	User tries to access the "hosts.txt" file without root/admin permissions.	YES

When you have finished defining the conditions for this scenario, the **Did What?** details in the **Activity Alert Rules** tab should look like this:

Did What?

Application name is Regedit, SSMS - SQL Management Studio, Setup, Notepad
AND Window title contains hosts, permission, security
AND Permission level is not Admin

 Windows

How to Configure the "Visited URL" Group Options

This topic provides details and a typical scenario to help you understand how to configure **Did What?** conditions using the **Visited URL** group of options.

Note: These options apply to Windows operating systems only.

For general information about defining **Did What?** conditions, see [Defining the "Did What?" Conditions](#).

The **Visited UR** group includes the following options for configuring **Did what?** conditions:

Option	Description	When should I use this option?	Example Condition
Site	URL domain or host name of the Website that was visited.	Use this option if you want to be alerted when the user visits a specific Website, regardless of which pages were opened or how many pages were viewed.	"Visited URL: Site contains facebook, twitter" would generate an alert on the URL: "www.facebook.com/login?..."
URL prefix	The first part of the visited Website from the beginning of the URL until the end of the matched text.	Use this option if you want to know which specific pages(s) the user visited in a Website.	"Visited URL: URL prefix contains AdminUsersView" would generate an alert on the URL: "http://111.222.333.444:4884/ObserveIT/AdminUsersView.aspx?GroupIndex=3&TabIndex=1&lang=en"
Any part of URL	Any part of the visited Website URL that matches the text.	Use this option if you want to be alerted whenever the user accesses a new page or searches for a specific page or application in a Website.	"Visited URL: Any part of URL contains linkedIn" would generate an alert on the URL: "https://www.linkedin.com/profile/view?id=88888&trk=nav_responsive_tab_profile"

Example Scenarios

The following scenarios provide some examples of how and when alerts are triggered using the **Visited URL** group of conditions.

Note: For purposes of these scenarios, the scope of the alert rule is defined "per session", which means that an alert will be generated only on the first occurrence of every unique match of the rule in each session. You can also you can define alerts to be generated once per application/process, or once per a specified number of minutes. Full details about defining the scope of rules are provided in [Defining the "Did What?" Conditions](#).

Alert Rule	Condition Example	Description	User Activity	Alert Generated?
Trigger an alert the first time in a session that a user "browses social media sites during working hours".	"Visited URL: Site contains facebook, twitter"	Generate an alert every time the URL domain contains "facebook" or "twitter".	1. User logs in to Facebook: enters the URL: "www.facebook.com/login?..."	YES
			2. User goes to a friend's page: enters the URL: "www.facebook.com/friend?...."	NO alert is generated, because the "Site" rule refers only to the domain part of the URL: "www.facebook.com".
			3. User logs in to Twitter: "www.twitter.com/login..."	YES
Trigger an alert every first time in a session a user enters the User Administration area of the ObserveIT Web Console.	"Visited URL: URL prefix contains AdminUsersView"	Generate an alert every first time the URL prefix contains "AdminUsersView".	1. User opens the browser: "http://111.222.33.444:4884/ObserveIT/AdminUsersView.aspx?GroupIndex=3&TabIndex=1&lang=en"	YES
			2. User opens a new browser: "http://111.222.33.444:4884/ObserveIT/AdminUsersView.aspx?GroupIndex=2&TabIndex=1&lang=en"	NO alert is generated, because this is not a new occurrence of the "URL prefix" rule.

			3. User goes to: "http://111.222.33.555:5994/ObserveIT/AdminUsersView/users.aspx?GroupIndex=2&TabIndex=1&lang=en"	YES Matches the text URL prefix "/ObserveIT/AdminUsersView" but the site is different than the first site opened in the session.
Trigger an alert every time in a session that a user accesses, opens a new page, or searches for "LinkedIn".	"Visited URL: Any part of URL contains linkedIn"	Generate an alert every time "any part of URL" contains "linkedIn".	1. User logs in to LinkedIn: enters the URL "https://www.linkedin.com/nhome/"	YES
			2. User goes to their profile: "https://www.linkedin.com/profile/view?id=88888&trk=nav_responsive_tab_profile"	YES
			3. User searches Google for "linkedin" "https://www.google.co.il/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#ie=UTF-8&q=linkedin&sourceid=chrome-psyapi2"	YES

How to Define an "Executed SQL Command" Statement

The **Executed SQL Command** group option enables you to define a rule by running SQL statements containing specific keywords that you want to find. This feature applies on Windows operating systems only.

Note: SQL Server 2012 is not supported.

For example, if you want to generate an alert on a user trying to access a list of credit cards in a customer's database, you might specify the following SQL statement conditions:

"Executed SQL Command: Statement contains update, drop"
AND "Executed SQL Command: Statement contains CREDIT_CARD"

How to Configure the "Executed Command" Group Options

This topic provides details of usage and scenarios to help you understand how to configure the **Did What?** field options in the **Executed Command** group.

Note: These options are available on Unix operating systems only.

For general information about defining **Did What?** conditions, see [Defining the "Did What?" Conditions](#).

The **Executed Command** group includes the following options for configuring conditions:

Option	Description	When should I use this option?	Examples
Command name	The name of the Unix command that the user ran.	Use this option if you want to be alerted when the user runs a specific Unix command.	If a Unix user is trying to remove a sensitive directory, you might define the following condition: "Executed Command: Command name is rm" Other examples of command names include: su, emacs, tail, ls, sudo, setuid
Full path	The full path of the command (including any command line arguments).	Use this option if you want to configure an alert based on the explicit path of a command.	usr/sbin/otcheck/rm
Argument	The object of the Unix command.	Use this option if you want to configure an alert based on a command's object or user action.	If the user is trying to remove a sensitive directory (such as "observeit"), you might define the following condition: "Executed Command: Argument is observeit" Other examples of arguments include: sys, admin, oracle, r, -f

Switch	The switch (flag) that defines the action on the command.	The "Switch" option provides more search combinations than the "Argument" option, enabling you to find exactly what you need. For example, if you are looking in an alert rule for the argument "-r", the switch option allows you to use: "-rf" or "-fr" which extends the range of your search options.	In the case of a user trying to remove a sensitive directory, the following condition might be used: "Executed Command: Switch is -rf" Usage examples: • Switch is -rf (that is, both switches are on) • Switch is -r, -f, (that is, either switch is on) • Switch is not -r, -f (that is, neither switch is on)
Permissions	The logged-in user's permissions: • are own • other than own • are root • are root (other than own)	Use these options if you want to generate an alert if a user tries to change or switch credentials.	• "Executed Command: Permissions are own" (checks if the user logged in with their own credentials.) • "Executed Command: Permissions other than own" (checks if the user logged in with their own credentials, and then switched to someone else's credentials via the 'oitcheck/su' command.) • "Executed Command: Permissions are root" (checks if the user logged in with 'root' credentials.) • "Executed Command: Permissions are root (other than own)" (checks if the user logged in with their own 'root' credentials, and then switched to someone else's credentials via the 'root/su' command.)

Note: On Unix/Linux operating systems, user names, file/directory names, commands, and computer names are all case-sensitive. Unix/Linux alert rules are also case-sensitive.

Example Scenarios

The following scenarios provide some examples of how you can use the **Executed Command** options to configure alert rules.

Note: For purposes of these examples, the scope of the alert rule is "per session", which means that an alert will be generated only on the first occurrence of every unique match of the rule in each session. Full details about defining the scope of rules are provided in [Defining the "Did What?" Conditions](#).

Alert Rule	Description	Conditions
------------	-------------	------------

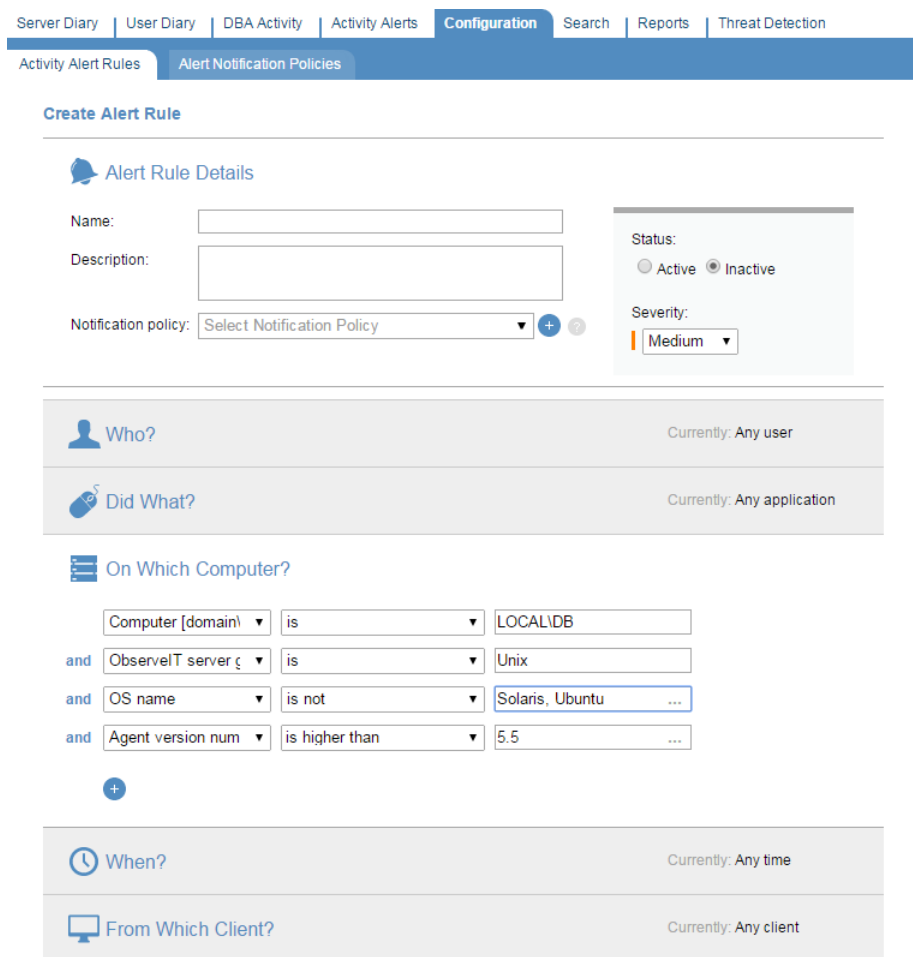
Trigger an alert when (Unix) user tries to change credentials to a privileged user.	User is trying to grant more permissions by using su or sudo commands or by running a command that grants root permissions.	"Executed Command: Permissions are root (other than own)" or "Executed Command: Command name is su, sudo"
Trigger an alert when Unix user tries to remove a sensitive directory.	Unix user is trying to remove a directory containing "observeit" in its name while running "rm" command using "-r" or "-f" flags.	"Executed Command: Command name is rm" and "Executed Command: Argument is observeit" and "Executed Command: Switch is -r, -f"
Trigger an alert when a new user is added with root permissions.	Remote contractor with root permissions creates a new user account with 'root' permissions.	Executed Command: Command name is useradd (that is, create a new user) and "Executed Command: Switch is -o" (that is, create duplicate user ID) and "Executed Command: Switch is -u (that is, user ID) and "Executed Command: Argument is 0" (that is, assign root permissions)

Defining the "On Which Computer" Conditions

In the **On Which Computer** section of the **Create Alert Rule** page, you can define (or edit) the specific or groups of computers/servers on which the suspicious activity occurred.

To define the "On Which Computer" conditions

- 1) Open the **On Which Computer** section by clicking  **On Which Computer?** or the **Edit**  icon.



The screenshot shows the 'Create Alert Rule' page with the following sections:

- Alert Rule Details:**
 - Name:
 - Description:
 - Notification policy:  
 - Status: ☐ Active ☒ Inactive
 - Severity:
- Who?:** Currently: Any user
- Did What?:** Currently: Any application
- On Which Computer?:**
 - Computer [domain]
 - and ObservelT server ζ
 - and OS name
 - and Agent version num
- When?:** Currently: Any time
- From Which Client?:** Currently: Any client

Important: Before you begin, make sure that you have read the "Rules for Configuring Alert Conditions" described in [Understanding the Logic for Triggering Alerts](#).

- 2) To define the specific or groups of computers/servers on which the action occurred, select the required field, relevant operator, and specify value(s) for each condition that you want to define, as described in the following table.

Options for Defining the "On Which Computer?" Conditions

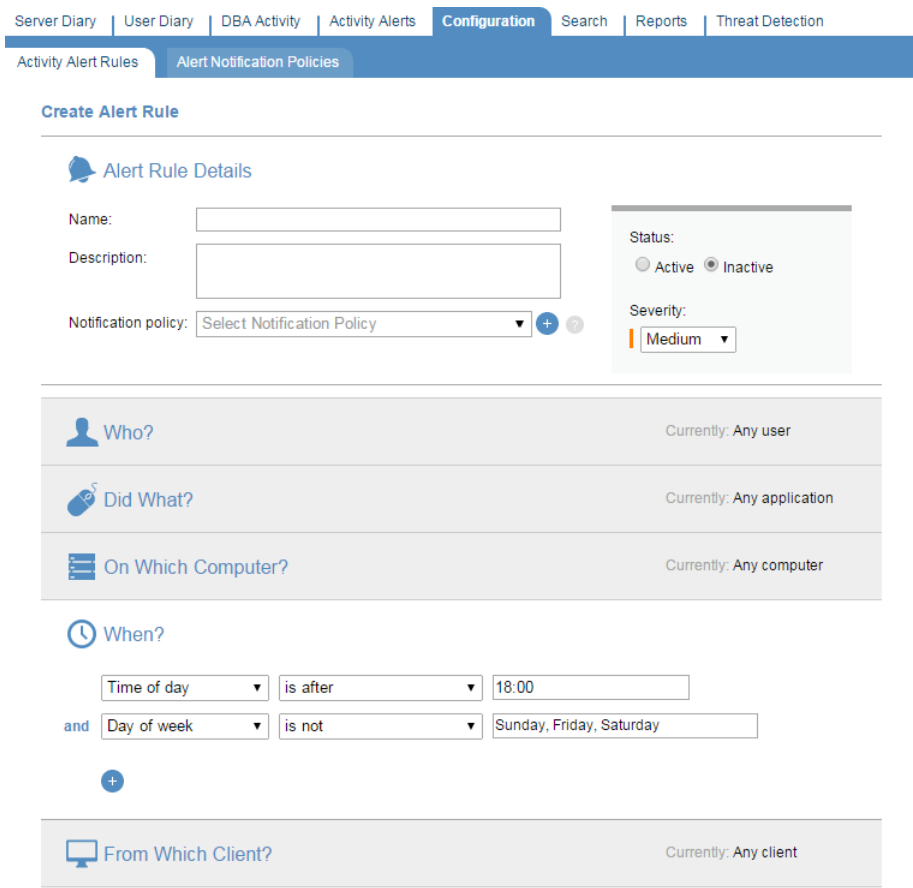
Field	Operator	Example Values
Computer domain\name	• is • is not • contains • does not contain • starts with • does not start with • ends with • does not end with • is empty • is not empty	LOCAL\DB, DomainA\FIN
ObserveIT server group name	Same as above	Windows, GroupA, Unix
Computer IP address	Same as above	10.1.100.100, 10.1.200.61
OS name	Same as above	Windows 2012 R2, Ubuntu, Solaris 11
Agent version number	• is • is not • is higher than • is lower than	5.5, 5.6.9

Defining the "When?" Conditions

In the **When?** section of the **Create Alert Rule** page, you can define (or edit) what day and/or at what time the suspicious activity occurred.

To define the "When?" conditions

- 1) Open the **When?** section by clicking  or the **Edit**  icon.



The screenshot shows the 'Create Alert Rule' page. The top navigation bar includes 'Server Diary', 'User Diary', 'DBA Activity', 'Activity Alerts', 'Configuration' (selected), 'Search', 'Reports', and 'Threat Detection'. Below the navigation bar are tabs for 'Activity Alert Rules' and 'Alert Notification Policies'. The 'Create Alert Rule' section is active. It contains an 'Alert Rule Details' section with fields for 'Name', 'Description', and 'Notification policy' (a dropdown menu). To the right of these fields are 'Status' (radio buttons for 'Active' and 'Inactive', with 'Inactive' selected) and 'Severity' (a dropdown menu set to 'Medium'). Below the details section are three expandable sections: 'Who?' (Currently: Any user), 'Did What?' (Currently: Any application), and 'On Which Computer?' (Currently: Any computer). The 'When?' section is expanded, showing two conditions: 'Time of day' is after 18:00, and 'Day of week' is not Sunday, Friday, Saturday. At the bottom is the 'From Which Client?' section (Currently: Any client).

Important: Before you begin, make sure that you have read the "Rules for Configuring Alert Conditions" described in [Understanding the Logic for Triggering Alerts](#).

- 2) To define (or edit) the time (specific date, range of dates, time of day, or days of the week) that the action occurred, select the relevant options, as described in the following table.

Note: If the Agent and the server are in different time zones, date and time alerts are based on Agent local time. This means that non-working hours in the Agent location might be regular working hours in the server's local time zone.

Options for Defining the "When?" Conditions

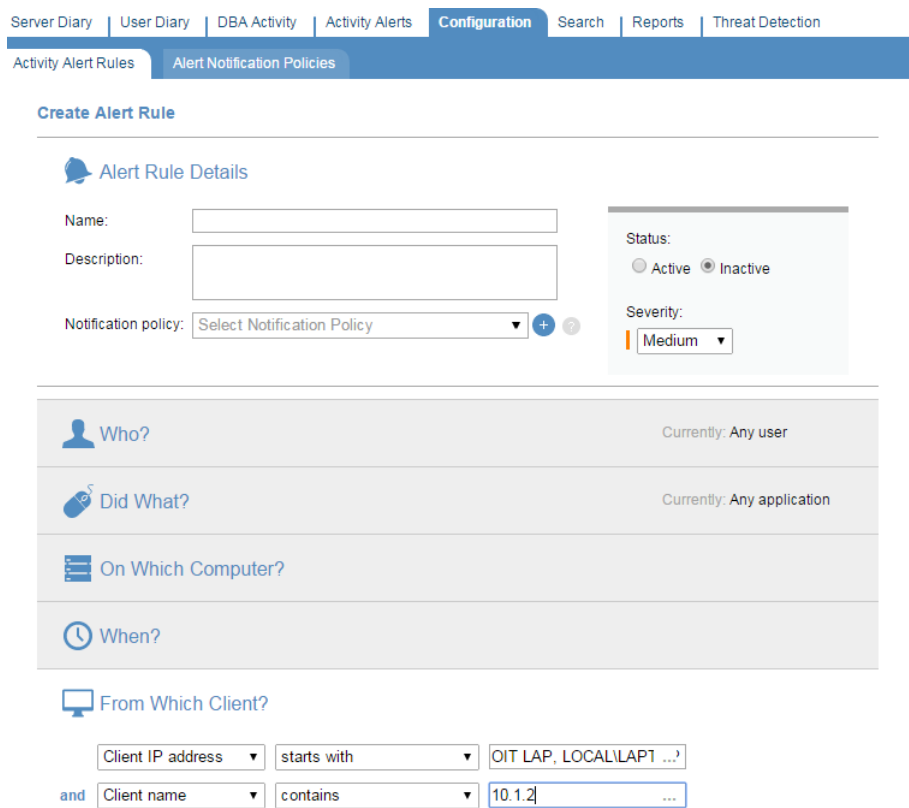
Field	Operator	Example Values
Day of week	• is • is not	Saturday, Sunday
Time of day	• is before • is after • is between • is not between	10:59am, between 08:00am and 06:00pm
Specific date	• is • is not • is before • is after • is between • is not between	20/4/2014, 22/4/2014, between 25/4/2014 and 27/4/2014
Specific date and time	• is • is not • is before • is after • is between • is not between	between 25/4/2014 09:00pm and 27/4/2014 06:00pm

Defining the "From Which Client" Conditions

In the **From Which Client** section of the **Create Alert Rule** page, you can define (or edit) the name or IP address of the client computer from which the suspicious activity occurred.

To define the "From Which Client" conditions

- 1) Open the **From Which Client** section by clicking  **From Which Client?** or the **Edit**  icon.



The screenshot shows the 'Create Alert Rule' page in ObserveIT. The page has a navigation bar with links: Server Diary, User Diary, DBA Activity, Activity Alerts, Configuration (selected), Search, Reports, and Threat Detection. Below the navigation bar, there are tabs for 'Activity Alert Rules' and 'Alert Notification Policies'. The 'Create Alert Rule' section is active, showing 'Alert Rule Details' with fields for Name, Description, and Notification policy. To the right of these fields are 'Status' (Active/Inactive) and 'Severity' (Medium) options. Below this is a section for 'Who?', 'Did What?', 'On Which Computer?', and 'When?'. The 'From Which Client?' section is expanded, showing two conditions: 'Client IP address starts with OIT LAP, LOCAL\LAP1 ...' and 'Client name contains 10.1.2 ...'.

Important: Before you begin, make sure that you have read the "Rules for Configuring Alert Conditions" described in [Understanding the Logic for Triggering Alerts](#).

- 2) To specify the client computer name or IP address that was used to connect to the monitored computers, select the required option, the relevant operator, and specify the required value(s) for each condition that you want to define, as described in the following table.

Options for Defining the "From Which Client?" Conditions

Field	Operator	Example
Client name	- is - is not - is empty - is not empty - contains - does not contain - starts with - does not start with - ends with - does not end with	OITLAP, OITPC , LOCAL\LAPTOP
Client IP address	Same as above	10.1.0.16, 10.1.2.100

Defining Alert Notification Policies

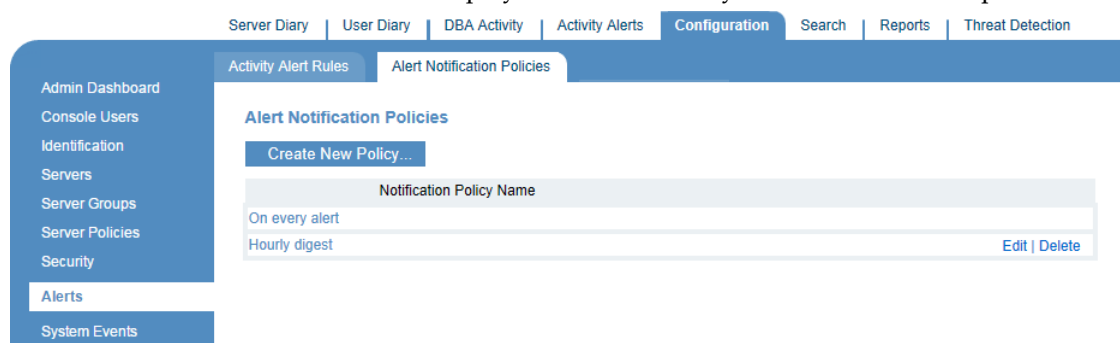
Alert notification policies enable ObserveIT administrators to define the email notifications that will be created when an alert is generated. These policies define to whom and how often emails will be sent in the event of an alert. By using configurable policies for alert notifications, they can be easily edited (for example, by changing the email address) and applied to multiple alert rules. Every Alert rule is associated with a single notification policy.

Alert notification policies are configured in the **Alert Notification Policies** tab in the ObserveIT Web Console. From this page, the administrator can create new notification policies, edit existing policies, and delete policies.

To create a new notification policy

- 1) Navigate to **Configuration > Alerts > Alert Notification Policies**.

The **Alert Notification Policies** tab displays a list of currently defined notification policies.



- 2) Click the **Create New Policy** button.

Edit Alert Notification Policy

Policy name:

Email Recipients

Email address: **Add**

Remove

Email Frequency

☒ On every alert

☐ Digest email, no more than once every minutes

☐ Daily digest email at 08:00:00

Save **Cancel**

- 3) In the **Edit Alert Notification Policy** dialog box, configure recipients for the email notification, as follows:

1. Enter the user's email address in the text box, and click **Add Address**. The email address will be added to the list.
2. Repeat the above step for each email address you want to add.

Note: To remove an email address from the list, select it and click **Remove**.

- 4) Configure how often recipients will receive the email notification, by selecting one of the following options:
- Email on every alert (default frequency).
 - Send digest email no more than once every X minutes.
 - Send a daily digest email at a fixed time every day (for example, 08:00 AM).
- 5) Click **Save** to save your settings.

The new notification policy will be available for selection in the **Activity Alert Rules** page. See [Creating Alert Rules](#).

To edit an existing notification policy

- 1) In the **Alert Notification Policies** page, select the policy that want to edit, or click the **Edit** link next to it.

- 2) In the **Edit Alert Notification Policy** dialog box, edit any of the settings, as described in steps 2 and 3 of the previous procedure.
- 3) Click **Save** to save your settings.

The edited notification policy will be available for selection in the **Activity Alert Rules** page.

To delete a notification policy

- 1) In the **Alert Notification Policies** page, click the **Delete** link next to the policy you want to delete. A dialog box opens, warning you about any alert rules that are currently using this policy.

- 2) If you are sure that you want to continue, click **Delete**.

The deleted notification policy will no longer be available for selection in the **Activity Alert Rules** page.

Editing and Duplicating Alert Rules

This topic describes how to edit and/or duplicate the content of an existing alert rule.

Note: The procedures for editing and duplicating alert rules are identical.

To edit an existing alert rule

- 1) In the **Alert Rules** list (in the **Activity Alert Rules** tab), click the relevant alert rule name, or click the **Edit** link next to it.

The **Edit Alert Rule** page opens, showing the details and conditions currently defined for the selected alert rule (for example, as shown in the following example).

The screenshot displays the 'Edit Alert Rule' configuration page. The left sidebar contains navigation links for various system components. The main panel is divided into sections for defining the alert rule's details and conditions. The 'Alert Rule Details' section includes fields for the rule's name, description, and notification policy. The 'Who?' section defines the user or process triggering the alert. The 'Did What?' section specifies the action being monitored. The 'On Which Computer?' section defines the scope of the alert. The 'When?' section sets the time and day conditions. The 'From Which Client?' section defines the client scope. The page concludes with 'Cancel' and 'Save' buttons.

- 2) In the **Alert Rule Details** section, in the **Name** field, edit the name of the alert rule.
- 3) Provide a **Description** for the rule that explains its meaning or motivation.
- 4) Select a **Notification policy** that defines who should receive email notifications when an alert from this rule is triggered, and how often. For example: "Daily digest for Division Managers".

Note: To define a new policy, click the  icon (see [Defining Alert Notification Policies](#)). There is no default notification policy; new alert rules are created with no policy, which means that newly generated alerts will not trigger any email.

- 5) Select the status of the alert rule: **Active** or **Inactive**.
- 6) Select the severity of the alert rule: **High**, **Medium**, or **Low**.
- 7) Edit the **Who?**, **Did What?**, **On Which Computer?**, **From Which Client?**, **When?** conditions for the rule that will trigger the alert, as described in the following topics:
 - [Defining the "Who?" Conditions](#)

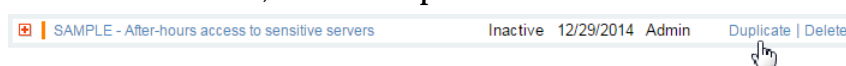
- [Defining the "Did What?" Conditions](#)
- [Defining the "On Which Computer" Conditions](#)
- [Defining the "When?" Conditions](#)
- [Defining the "From Which Client" Conditions](#)

Note: For descriptions of the logic for defining alert conditions, see [Understanding the Logic for Triggering Alerts](#).

- When you have finished editing your alert rule, click **Save** to save your settings.
The updated alert rule is displayed in the **Activity Alert Rules** page.

To duplicate an alert rule

- In the **Alert Rules** list, click the **Duplicate** link next to the relevant alert rule.



The **Edit Alert Rule** page opens with a new alert rule initialized to the exact content of the selected item, named "Copy of <selected alert rule name>".

- Proceed with steps 2-8 above to edit the duplicated rule, as required.

Deleting Alert Rules

ObserveIT administrators can delete alert rules that are no longer relevant (they may have been created for demo or training purposes and are no longer required).

Note: Only an ObserveIT administrator can delete alert rules (that is, not any user with administrative permissions).

To delete an alert rule

- In the **Alert Rules** list, select the rule(s) you want to delete, and click the adjacent **Delete** link.



A confirmation dialog box opens.

- Click **OK** to confirm the deletion(s).
The rule(s) are deleted, and the **Alert Rules** list is refreshed.

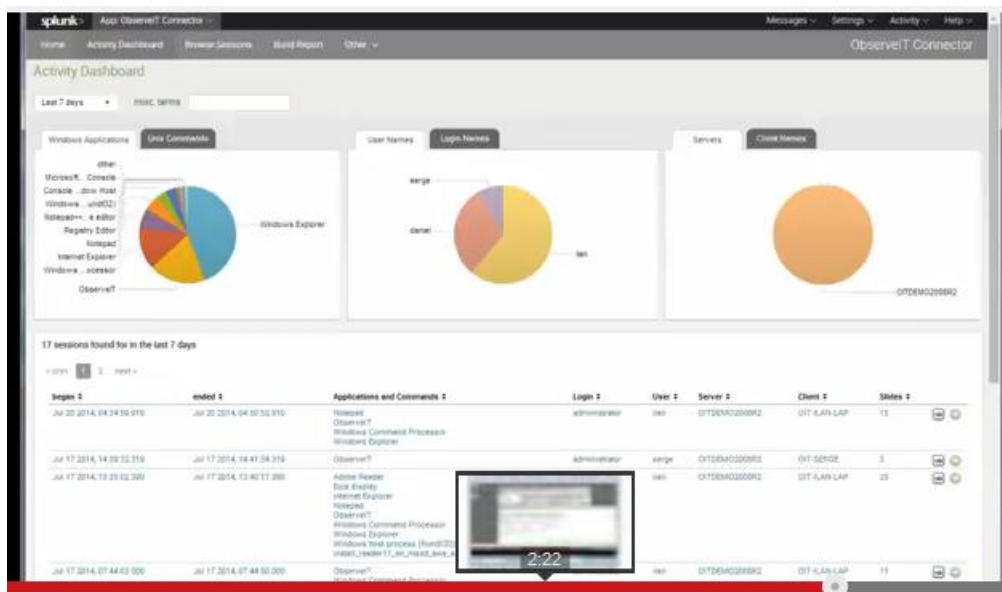
Integrating Alerts in SIEM Products

ObserveIT alerts can be easily integrated into an organization's existing SIEM system, providing real-time alerting and reporting capabilities.

Note: In this version of ObserveIT, integration is provided with the HP ArcSight SIEM monitoring software. For further details, see [Integrating Logs into SIEM Systems](#).

The log file from ObserveIT activity alerts can be exported for integration into SIEM monitoring software. Third-party monitoring and management tools (such as, Microsoft System Center Operation Manager, IBM QRadar, HP ArcSight, Splunk, McAfee SIEM/ELM) can parse the ObserveIT log file, and create events, triggers, and alerts, based on text strings of information that appear inside the log file.

Following is an example of an activity dashboard showing alerts that can be viewed and analyzed in the "Splunk" SIEM monitoring software. Note that from this dashboard view, by clicking the **Video** icon, you can link directly to the session's video recordings at the exact location where the alert was generated.



Important: For instructions on how to integrate ObserveIT log data into the HP ArcSight SIEM product by using the CEF open log management standard, see [Integrating ObserveIT with HP ArcSight CEF](#).

System Events

System events are triggered by the ObserveIT system. Events might be triggered when users reach their database storage limits, when a user logs in or when a pairing request is made, or during the health check monitoring of the Agent, Notification Service, Application Server, or Web Console.

For example, when ObserveIT Identity Theft Detection is configured (see [Identity Theft Detection](#)), administrators can verify that users are authorized to log in from the specified (client) computers and to the specified servers. After a user logs in to a server from the desktop, the ObserveIT administrator sends an email to the user confirming the login and event type. If identity theft is suspected, the user reports the suspicious login event to the administrator and a high severity alert is triggered.

ObserveIT administrators can view and manage system events from the **Configuration > System Events** page in the Web Console.

The **System Events** page displays a list of the currently defined system events, according to the specified severity and filter criteria.

The screenshot displays the 'System Events' page in the ObserveIT web console. The page has a navigation sidebar on the left with options like 'Admin Dashboard', 'Console Users', 'Identification', 'Servers', 'Server Groups', 'Server Policies', 'Security', 'Alerts', 'System Events', 'Identity Theft Detection', 'Messages', 'Ticket Integration', 'License', 'SMTP Settings', 'Monitor Log', 'LDAP Settings', 'Storage', 'Archive', 'Saved Sessions', 'Audit', and 'System Log'. The main content area is titled 'System Events' and includes a 'System Events Notification Policy' tab. Below the title, there are filters for 'Severity' (set to 'All') and 'Server' (set to 'All'), along with a 'More Filters' link and 'Reset' and 'Show' buttons. The event list shows 1-20 of 55 events, with a date filter for '1/7/2015'. The events are listed in a table with columns: Received, Code, Category, Name, and Server. The events include various status updates, tampering alerts, and service terminations.

Received	Code	Category	Name	Server
3:01 PM	1304	Functionality	Application Server is running	W2K8-S8-QA11
3:01 PM	1218	Tampering	Agent offline data files were tampered with	W2K8-S8-QA11
3:01 PM	1301	Functionality	Application Server is not working properly	W2K8-S8-QA11
3:00 PM	1201	Functionality	Agent service has started	W2K8-S8-QA11
3:00 PM	1221	Communication	Agent machine and service are accessible	c59-32-3
2:59 PM	1203	Functionality	Agent service was terminated	W2K8-S8-QA11
2:59 PM	1219	Functionality	Agent service not responding	c59-32-3
2:59 PM	1218	Tampering	Agent offline data files were tampered with	W2K8-S8-QA11
2:58 PM	1304	Functionality	Application Server is running	W2K8-S8-QA11
2:58 PM	1301	Functionality	Application Server is not working properly	W2K8-S8-QA11
2:57 PM	1220	Tampering	Process was killed and automatically restarted	W2K8-S8-QA11
2:56 PM	1201	Functionality	Agent service has started	W2K8-S8-QA11
2:56 PM	1221	Communication	Agent machine and service are accessible	c59-32-3
2:54 PM	1203	Functionality	Agent service was terminated	W2K8-S8-QA11
2:54 PM	1219	Functionality	Agent service not responding	c59-32-3
2:54 PM	1304	Functionality	Application Server is running	W2K8-S8-QA11
2:52 PM	1231	Data Loss	Offline data loss, threshold exceeded	W2K8-S8-QA11
2:52 PM	1301	Functionality	Application Server is not working properly	W2K8-S8-QA11
2:52 PM	1220	Tampering	Process was killed and automatically restarted	W2K8-S8-QA11

In the **System Events** page, administrators can:

- [View system events](#) generated by the ObserveIT system and view related details including name, severity, and type
- [Filter the events displayed per specified criteria](#)
- [Add comments to events](#)
- [Define the remediation status of events](#)
- [Configure email notification policies for events](#) to determine who gets notified by email, for which event types, and at what frequency

For descriptions of the event types, and some possible causes and solutions, see [Event Types](#).

Event Types

When an event is generated by the ObserveIT system, the event name and details appear in the **System Events** list. The following tables describe some of the event types, organized per event source, with some possible causes and solutions (as relevant).

Agent Events

Code	Event Name	Category	Severity	Description
1201	Agent Service has started	Functionality	Low	The ObserveIT Agent Service has reported that it has started.
1202	Agent Service has stopped	Functionality	High	The ObserveIT Agent Service has reported that it has stopped. To receive Agent health check reports, it must be restarted.
1203	Agent Service was terminated	Functionality	High	The ObserveIT Agent Service was terminated (due to system causes), however, the machine is responsive. To receive Agent health check reports, it must be restarted.
1204	Unrecorded Agent sessions	Recording	High	There are unrecorded Agent sessions. This occurs when a user ends the Agent process (or disables interception in Unix). To resolve this in Windows, go to the Task Manager and restart the RCDCL process. In Unix, enable interception using the <code>oitcons</code> utility.

Code	Event Name	Category	Severity	Description
1205	Agent installation files were tampered with (missing file)	Tampering	High	The ObserveIT Agent Service has reported that installation files were tampered with. Files may have been deleted or changed. Check the problem and reinstall the Agent, or replace the tampered file with the file version that was installed previously.
1206	Agent installation files were tampered with (changed file)	Tampering	High	The ObserveIT Agent Service has reported that installation files were tampered with. Files may have been renamed and/or contents changed. Check the problem and reinstall the Agent, or replace the tampered file with the file version that was installed previously.
1207	Agent Registry keys were tampered with	Tampering	High	An ObserveIT Registry key was changed. Registry keys may have been deleted and/or values changed. This might affect Agent functionality. To resolve this, look at the AgentRegistryKeys database table, and restore the Registry accordingly.
1208	Agent Registry keys are now OK	Tampering	Low	The ObserveIT Agent Service has reported that the Agent Registry keys/configuration files have been restored.
1209	Agent installation files were restored	Tampering	Low	The ObserveIT Agent Service has reported that installation files were restored after tampering.
1210	Agent installation files were tampered with	Tampering	High	The ObserveIT Agent Service has reported that installation files were tampered with. Files may have been renamed and/or contents changed. Check the problem and reinstall the Agent, or replace the tampered file with the file version that was installed previously.

Code	Event Name	Category	Severity	Description
1213	Unix Agent interception was tampered with	Tampering	High	The Unix Agent interception setting was tampered with, so that new sessions will not be recorded. Perhaps a user did this to prevent his activities from being recorded. To resolve this, enable interception using the <code>oitcons</code> utility.
1218	Agent offline data files were tampered with	Tampering	High	Session data was tampered with while the Agent was in offline mode. Files may have been renamed, or contents changed by a user who worked offline to hide his activities. (Offline files are not sent to the Application Server.) When the Agent is online again, the Agent Service reports the list of files that were tampered with.
1219	Agent Service is not responding	Functionality	High	The ObserveIT Agent Service is down, perhaps due to a network malfunction or disconnection between the Agent and the Application Server, or other unknown reasons. To understand the reason, open the ICMP port, and restart the Agent Service.
1220	Process was killed and automatically restarted	Tampering	High	The Agent process was killed and automatically restarted by Watchdog.
1221	Agent machine and service are accessible	Communication	Low	The ObserveIT Agent and service are activated.
1223	Agent computer is inaccessible	Communication	High	The Agent machine is disconnected from the network. Check the ICMP port, if it is closed, reopen it.
1224	Agent Service was killed	Functionality	High	The ObserveIT Agent Service has reported that it was killed by a Unix command executed by the user (<code>kill</code>). To receive Agent health check reports, it must be restarted.

Code	Event Name	Category	Severity	Description
1230	Agent data loss	Data Loss	High	Data loss occurred while the Agent was running. This may have occurred due to resource overload or some issue with the SQL server or the Application Server. Check that the SQL server and Application Server are working properly.
1231	Offline data loss, threshold exceeded	Data Loss	High	The volume of data exceeded its configured limit while the Agent was in offline mode, resulting in data loss. You must increase the offline data limit in the configuration file.
1232	Offline data loss, lack of disk space	Data Loss	High	Data was lost while the Agent was in offline mode due to insufficient disk space. Increase the disk space to prevent this from recurring.
1240	Agent is now recording active sessions	Recording	Low	Agent sessions are now being recorded.
1242	Agent process was reactivated by Watchdog	Functionality	High	The Agent process was reactivated by Watchdog.
1250	Agent recording is enabled via Server Policy	Recording	Low	The recording of user actions was enabled in the Web Console Server Policies configuration.
1251	Agent recording is disabled via Server Policy	Recording	High	The recording of user actions was disabled in the Web Console Server Policies configuration.
1501	Agent interception is off	Recording	High	The Unix Agent internal Watchdog "obitd" service failed to start the ObserveIT logger after a problem was detected, and recording was disabled. Another reason can be that someone did this on purpose using the <code>oitcons</code> utility, for example, as part of an upgrade process. To enable interception, use the <code>oitcons</code> utility.
1502	Agent interception is on	Recording	High	The Unix Agent interception is on, and recording is enabled.

Code	Event Name	Category	Severity	Description
1602	Agent registration was successful	Installation	Medium	The Agent was successfully registered.
1603	Agent installation failed due to incorrect security password	Installation	Low	The Agent installation failed due to incorrect security password. Check your password and try to install again.
1604	Agent installation failed	Installation	Low	The Agent installation failed without a security password, or for unknown reasons. Go to the setup log, and look for possible errors.
1605	Agent installation with password was successful	Installation	Low	The Agent was successfully installed with a security password.
1606	Agent installation without a password was successful	Installation	Medium	The Agent was successfully installed without a security password.
1607	Uninstallation of Agent failed due to incorrect security password	Installation	Low	Uninstallation of Agent failed due to an incorrect security password. Check your password and try to uninstall again, and if that fails, contact technical support.
1608	Uninstallation of Agent failed	Installation	Low	Uninstallation of Agent failed without a security password, or for unknown reasons. Try to uninstall again and/or contact technical support.
1609	Uninstallation of Agent with password was successful	Installation	Low	The Agent was successfully uninstalled with a security password.
1610	Uninstallation of Agent without a password was successful	Installation	Medium	The Agent was successfully uninstalled without a security password.
1611	Agent was unregistered	Installation	High	The Agent was unregistered, and was removed from the license.

Application Server Events

Code	Event Name	Category	Severity	Description
1301	Application Server is not working properly	Functionality	High	The ObserveIT Application Server is not working properly. No reply is received when a keepalive request is sent, and the Application Server pool is down. Restart the IIS to restart the Application Server.
1304	Application Server is running	Functionality	Low	The ObserveIT Application Server has resumed operations.
1310	Application Server successfully saved recorded data	Communication	Low	The ObserveIT Application Server successfully saved recorded data.
1311	Application Server unable to save recorded data	Communication	High	The ObserveIT Application Server failed to save recorded data to the database. Check the SQL server.
1403	Writing data to file system failed	Communication	High	The ObserveIT Application Server failed to save recorded data on the file system. Check read-write permissions on the file system path.
1404	Writing data to file system succeeded	Communication	Low	The ObserveIT Application Server successfully saved recorded data on the file system.

Database Server Events

Code	Event Name	Category	Severity	Description
1425	Some data was not recorded in the database	Data Loss	High	Screenshot data and/or Unix commands failed to be saved to the ObserveIT_Data database. Check the accessibility to this database.

Health Monitoring Service Events

Code	Event Name	Category	Severity	Description
1324	Health Monitoring Service is not working properly	Functionality	High	The Health Monitoring Service is not working properly. Perhaps the service was terminated or was configured incorrectly. When this occurs, the Admin Dashboard will not display updated data. To resolve this, restart the Health Monitoring Service (go to Start > Services).
1325	Health Monitoring Service is OK	Functionality	Low	The Health Monitoring Service is OK.
1327	Health Monitoring Service has started	Functionality	Low	The Health Monitoring Service has started.
1328	Health Monitoring Service has stopped	Functionality	Low	The Health Monitoring Service has stopped.

Identity Theft Events

Code	Event Name	Category	Severity	Description
1100	Login from paired client	Identity Theft	--	A user logged in from a paired client machine. This user-client pair is approved.
1101	Secondary login from paired client	Identity Theft	--	A user logged in via ObserveIT Secondary Identification from a paired client machine. This user-client pair is valid.
1102	Login from unpaired client	Identity Theft	Low	A user logged in from an unpaired client machine. This user-client pair is NOT valid.
1103	Secondary login from unpaired client	Identity Theft	Low	A user logged in via ObserveIT Secondary Identification from an unpaired client machine. This user-client pair is NOT valid.
1104	Login with no valid pair	Identity Theft	Medium	A user logged in from an unpaired client machine. This user-client pair is NOT valid and this user is already paired with another client.

Code	Event Name	Category	Severity	Description
1105	Secondary login with no valid pairs	Identity Theft	Medium	A user logged in via ObserveIT Secondary Identification from an unpaired client machine. This user-client pair is NOT valid and this user is already paired with another client.
1106	Suspected login reported	Identity Theft	High	A user reported a suspicious use of his credentials.
1107	Suspected secondary login reported	Identity Theft	High	A user reported a suspicious use of his credentials via ObserveIT Secondary Identification.
1108	User-client pairing request	Identity Theft	Low	A user sent a user-client pairing request.
1109	Failed to send an email to user	Identity Theft	Medium	Failed to send a "suspicious use of credentials" email to the user.

Notification Service Events

Code	Event Name	Category	Severity	Description
1302	Notification Service is OK	Functionality	Low	The Notification Service is working properly.
1303	Notification Service is not working properly	Functionality	High	The Notification Service is not working properly. Perhaps the service was terminated or was configured incorrectly. When this occurs, there will be no archives, no event emails, and no scheduled reports. To resolve this, restart the service (go to Start > Services).
1305	Notification Service has started	Functionality	Low	The Notification Service has started.
1306	Notification Service has stopped	Functionality	Low	The Notification Service has stopped. Restart the service (go to Start > Services).
1405	ArcSight file size reached 0.5	Communication	Low	File size reached 0.5 of the maximum size defined.
1406	ArcSight file size reached 0.75	Communication	Medium	File size reached 0.75 of the maximum size defined.
1407	ArcSight file size reached 0.99	Communication	High	File size reached 0.99 of the maximum size defined.

Code	Event Name	Category	Severity	Description
1408	ArcSight file size past maximum	Communication	High	File past the maximum size defined.
1409	Monitor Log could not create directory	Communication	High	You may not have sufficient permissions to create the directory.
1410	Monitor Log could not write to file	Communication	High	You may not have sufficient permissions to write a log file.

Rule Engine

Code	Event Name	Category	Severity	Description
1322	Rule Engine Service is not working properly	Functionality	High	The Rule Engine Service was unable to create alert rules. Perhaps the service was terminated or was configured incorrectly. Restart the service (go to Start > Services).
1323	Rule Engine Service is OK	Functionality	Low	The Rule Engine Service is working properly.
1329	Rule Engine Service has started	Functionality	Low	The Rule Engine Service has started.
1330	Rule Engine Service has stopped	Functionality	High	The Rule Engine Service has stopped. Restart the service (go to Start > Services).

Storage Threshold

Code	Event Name	Category	Severity	Description
1401	Storage threshold has reached its limit	Data Loss	Medium	The storage threshold (%) has reached its configured limit. Additional storage should be configured.
1402	Allocated storage space has reached its limit	Data Loss	High	The maximum allocated storage space has reached its configured limit. To prevent screen capture data loss, additional storage space must be configured immediately.

Viewing System Events

In the **System Events** list, you can view the names and severities of all generated system events, with the newest events at the top (organized by date/time and color coded per severity level).

To view system events

- 1) Navigate to **Configuration > System Events**. (Alternatively, in the **Configuration > Servers** page, click the **System Events** link or the **Status** link to open the **System Events** page filtered to display all the events related to the Agent group.)

The **System Events** list displays the events that occurred in the system, according to the specified severity and filter criteria.

The screenshot shows the 'System Events' page in the configuration interface. The page has a sidebar on the left with navigation links: Admin Dashboard, Console Users, Identification, Servers, Server Groups, Server Policies, Security, Alerts, System Events, Identity Theft Detection, Messages, Ticket Integration, License, SMTP Settings, Monitor Log, LDAP Settings, Storage, Archive, Saved Sessions, Audit, and System Log. The main content area is titled 'System Events' and includes a filter section with 'Severity' and 'Server' dropdowns, both set to 'All'. Below the filter is a 'More Filters' link and 'Reset' and 'Show' buttons. The event list shows 1-20 of 55 events, with a 'Next > Last >>' link. The table has columns: Received, Code, Category, Name, and Server. The events are color-coded by severity: Red (High), Orange (Medium), Green (Normal/Active), and Blue (Low/Administrative). The events are listed in descending order of time.

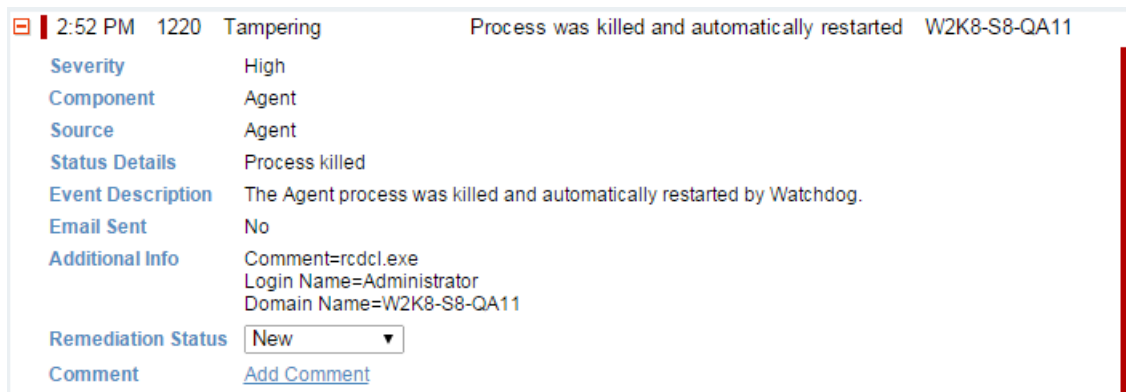
Received	Code	Category	Name	Server
1/7/2015				
3:01 PM	1304	Functionality	Application Server is running	W2K8-S8-QA11
3:01 PM	1218	Tampering	Agent offline data files were tampered with	W2K8-S8-QA11
3:01 PM	1301	Functionality	Application Server is not working properly	W2K8-S8-QA11
3:00 PM	1201	Functionality	Agent service has started	W2K8-S8-QA11
3:00 PM	1221	Communication	Agent machine and service are accessible	c59-32-3
2:59 PM	1203	Functionality	Agent service was terminated	W2K8-S8-QA11
2:59 PM	1219	Functionality	Agent service not responding	c59-32-3
2:59 PM	1218	Tampering	Agent offline data files were tampered with	W2K8-S8-QA11
2:58 PM	1304	Functionality	Application Server is running	W2K8-S8-QA11
2:58 PM	1301	Functionality	Application Server is not working properly	W2K8-S8-QA11
2:57 PM	1220	Tampering	Process was killed and automatically restarted	W2K8-S8-QA11
2:56 PM	1201	Functionality	Agent service has started	W2K8-S8-QA11
2:56 PM	1221	Communication	Agent machine and service are accessible	c59-32-3
2:54 PM	1203	Functionality	Agent service was terminated	W2K8-S8-QA11
2:54 PM	1219	Functionality	Agent service not responding	c59-32-3
2:54 PM	1304	Functionality	Application Server is running	W2K8-S8-QA11
2:52 PM	1231	Data Loss	Offline data loss, threshold exceeded	W2K8-S8-QA11
2:52 PM	1301	Functionality	Application Server is not working properly	W2K8-S8-QA11
2:52 PM	1220	Tampering	Process was killed and automatically restarted	W2K8-S8-QA11

For each event, the **System Events** list displays the following:

- **Colored severity bar** indicates the event/operational status severity level (Red (High)=Error, Orange (Medium)=Unreachable/Disabled, Green (Normal/Active)=OK, Blue (Low/Administrative)=Unregistered/Uninstalled). (See also [Colored Severity Levels and Icons](#) in the **Admin Dashboard** section.)
- **Date and time** that the event was triggered.
- **Code** that identifies the event.
- **Category** to which the event belongs: Identity Theft, Installation, Functionality, Data Loss, Tampering, Communication, Recording.
- **Name** of the event that occurred.
- **Server** on which the event occurred.

Note: "Offline" event rows are colored "gray" in the **System Events** list (as shown in the above figure). When an event occurs offline, when the system is online again, you can easily view and identify the "offline" events in the **System Events** list.

- 2) You can expand an event to view more details.



 2:52 PM 1220	Tampering	Process was killed and automatically restarted	W2K8-S8-QA11
Severity	High		
Component	Agent		
Source	Agent		
Status Details	Process killed		
Event Description	The Agent process was killed and automatically restarted by Watchdog.		
Email Sent	No		
Additional Info	Comment=rcdcl.exe Login Name=Administrator Domain Name=W2K8-S8-QA11		
Remediation Status	New		
Comment	Add Comment		

Depending on the event type, the information may include:

- **Severity:** the event severity (High, Medium, Low)
 - **Component:** the component type on which the event was reported (for example, Agent)
 - **Source:** the component that reported the event (Identity Theft, Agent, Notification Service, Application Server, Web Console, Services, Database, Health Monitoring, Rule Engine)
 - **Status Details:** the status details (for example, Service stopped, Tampered with)
 - **Event Description:** a brief description of the event
 - **Email sent:** whether an email was sent (Yes, No)
 - **Additional Info:** additional event information (for example, list of the files or registries that were tampered with)
 - **Remediation Status:** the remediation status of the event (New, In Process, or Closed)
 - **Comment:** a link for adding/displaying comments for the event
- 3) You can filter the **System Events** list according to specified criteria (including the event severities, sources by which events are triggered, and categories by which events are defined). For details, see [Filtering Events](#).

Filtering Events

You can filter the events displayed in the **System Events** list per specified criteria.

To filter the events displayed in the System Events list

- 1) From the **Severity** drop-down list (at the top of the **System Events** page), select the severity of events that you want to view (the options include: **High & Medium**, **High**, **Medium**, **Low**). By default, **All** event severities are displayed.

[System Events](#)

- 2) From the **Server** drop-down list, select the particular server for which you want to view events (or select **All** to view all servers).
- 3) Expand the **More Filters** section by clicking to filter the events displayed according to additional criteria, as described in the table below.
- 4) When you have finished defining your search criteria, click **Show** to update the event list according to the specified details.

To clear the filter fields, click **Reset**.

More Filters

Filter	Description
Category	To search for events by category (by the mechanism that generated the event), select an option from the list or select All to view events from all event categories. (The available category depends on the event Source.) Options include: • Identity Theft (Identity Theft source) • Installation (Agent source) • Functionality (Agent, Application Server, Health Monitoring, Notification Service, Rule Engine source) • Data Loss (Agent, Database, Web Console source) • Tampering (Agent source) • Communication (Agent, Application Server, Notification Service source) • Recording (Agent source)
Component	To search for events by the component type on which the events were reported, select an option from the list (Agent, Application Server, Database, File System, Web Console, Rule Engine, Notification Service, Health Monitoring Service), or select All to view all events.

Login	To search for events by the login name of the user who ran the session in which the event(s) occurred, select an option from the list (or select All).
Client	To search for events by the client computer from which the user logged in, specify the details (or search for it), or select All to view all events.
Event ID	To search for a specific event by ID, type the event ID in the text box.
Status Details	To search for events by status details, select an option from the list (Service Stopped , Service Terminated , and so on), or select All to view events per all status details. For further details, see Assessing Agent Statuses and Details .
Event Code	To search by event code, select an option from the list, or select All to view all events. You can click  to view a list displaying the code numbers and details of all events.
Source	To search by source (the component that reported the event), select an option from the list (or select All). During the live monitoring of ObserveIT, events can be triggered from the following sources: • Identity Theft events are triggered by user login or pairing requests. • Agent events are triggered by the Agent (for example, during health check monitoring). • Notification Service events are triggered by the Notification Service (for example, "Monitor log could not write to file"). • Application Server events are triggered from the Application Server (for example, "The ObserveIT Application Server has stopped working"). • Web Console events are triggered from the Web Console (for example, "Allocated storage space has reached its limit"). • Services events are triggered by system services. • Database events are triggered by the database. • Health Monitoring events are triggered by the Health Monitoring Service. • Rule Engine events are triggered by the Rule Engine Service.
Remediation Status	To search for events by remediation status, select an option from the list: • New • In Process (currently being handled) • Closed • All (this includes only events that are New and In Process)
Email Sent	To search for events for which an email notification was sent or not sent, select Yes or No , or select All to view all events.
Comment	To search for events by comment, type the relevant text in the text box.
Period	To search for events by time period, specify a time period ("Last") or a date range for your search ("Start Date" and "End Date").

Adding Comments to Events

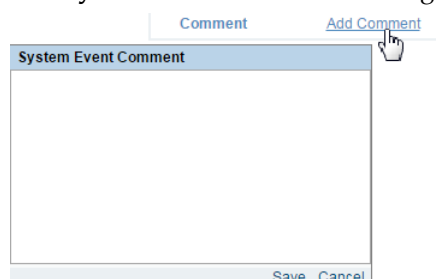
In the **System Events** page, you can add or edit a comment for an event, if and when required.

You can search for events according to comments that were entered.

To add/edit a comment for an event

- 1) In the **System Events** list, click the **Add Comment** link in the expanded details of the event to which you want to add a comment.

The **System Event Comment** dialog box opens, where you can enter your comment.



- 2) Click **Save** to save your comment.

The comment is displayed as a link in the **Comment** field in the expanded event details area. You can click this link to edit the comment in the text box.

To search for events according to comments that were entered

- 1) In the **Comment** text box in the **Filters** area, enter text related to the comment of the event(s) that you want to view.
- 2) Click **Show** to show the events based on the specified comment text.

Defining the Remediation Status of Events

In the **System Events** page, you can define or edit the current remediation status of the events.

You can search for events according to their defined remediation status.

To define the status of an event

- In the **System Events** list, from the drop-down list in the expanded details of the event whose remediation status you want to configure, select one of the following options:
 - **New:** The event is new.
 - **In Process:** The event is currently being handled.
 - **Closed:** The event is no longer relevant.

To search for events according to the defined remediation status

- 1) From the **Remediation Status** drop-down list in the **Filters** area, select the remediation status of the events you want to view. Options include:
 - **All:** to view events of any status
 - **New & In Process:** to view all **New** and **In Process** events
 - **New**
 - **In Process**
 - **Closed**

- 2) Click **Show** to show the events based on the specified remediation status.

Configuring Email Notification Settings for Events

Administrators can assign a notification policy to each system event to designate who gets notified by email, for which event types, and at what frequency. The system events notification policy determines whether the recipients receive immediate notification with separate emails upon each event, digest emails of event activity per specified number of minutes, or digest emails on a daily basis at a fixed time. For example, IT security officers in charge of handling high-severity system events can be notified immediately upon every event with a separate email for each system event notification. Events of lower severity or priority can be sent to relevant personnel in digest emails at predetermined intervals. Other individuals, such as compliance officers or managers, may require only a daily summary of the day's system events.

To configure the System Events Notification Policy

- 1) Navigate to **Configuration > System Events**.
- 2) Click the **System Events Notification Policy** tab.

The screenshot displays the 'System Events Notification Policy' configuration interface. The sidebar on the left includes links to 'Admin Dashboard', 'Console Users', 'Identification', 'Servers', 'Server Groups', 'Server Policies', 'Security', 'Alerts', 'System Events', 'Identity Theft Detection', 'Messages', 'Ticket Integration', 'License', 'SMTP Settings', 'Monitor Log', 'LDAP Settings', 'Storage', 'Archive', 'Saved Sessions', 'Audit', 'System Log', 'Latest Sessions', 'W12-S12-D02', 'Admin...', 'Quick Help', 'Installation Guide', 'User Guide', 'Configuration Guide', and 'Configuration Guide'. The main content area is titled 'System Events Notification Policy' and contains three sections:

- Email:** This section includes an 'Email address' input field with an 'Add' button. Below it is a list of email addresses, with 'ines@observeit.com' selected. A 'Remove' button is located below the list.
- Event Type Selection:** This section features a search bar labeled 'Search by event type'. Below the search bar are two lists of event types. The left list includes event types such as '1106 -High - Suspected login reported', '1107 -High - Suspected secondary login reported', '1202 -High - Agent service has stopped', '1203 -High - Agent service was terminated', '1204 -High - Unrecorded Agent Sessions', '1205 -High - Agent installation files were tampered with (missing file)', '1206 -High - Agent installation files were tampered with (file changed)', '1219 -High - Agent service not responding', and '1220 -High - Process was killed and automatically restarted'. The right list includes event types such as '1207 -High - Agent Registry keys were tampered with', '1210 -High - Agent installation files were tampered with', '1213 -High - Unix Agent interception was tampered with', and '1218 -High - Agent offline data files were tampered with'. A double-headed arrow is positioned between the two lists.
- Email Frequency:** This section contains three radio buttons: 'On every event', 'Digest email, no more than once every [minutes]', and 'Daily digest email at [18:00:00]'. The 'Daily digest email at [18:00:00]' option is selected.

A 'Save' button is located at the bottom right of the configuration area.

- 3) In the **Email address** field, type an email address, and click **Add**.
- 4) Repeat the above step for each email address to which you want send an email notification when an event is triggered.

To remove an email address, select the check box of the email address you want to remove and click **Remove**.

- 5) In the **Event Type Selection** section, click the relevant event types to add them to the "selected" list (on the right). (This designates which events will be included in email notifications.)

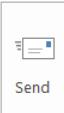
Note: Since there are numerous event types, it is recommended to filter the event types list (on the left) by typing the relevant "search" text in the **Event Type Selection** text box. For example, you may want to search by a specific severity level ("high"), event code ("1219"), or any keyword ("installation").

To remove event types from the "selected" list, click the relevant event type. They reappear in the "unselected" list on the left, and will not be included in email notifications.

- 6) In the **Email Frequency** section, select an option to specify how often the emails should be sent:
- **On every event** (the default frequency)
 - **Digest email**, no more than once every x minutes. An email is sent every x minutes if new system events were recently generated. The Event Digest email is sent only when at least one event was generated since the last digest was sent *and* the specified number of minutes passed since the last digest email.
 - **Daily digest email** at a fixed time every day (for example, 8:00 a.m.). An email is sent at the designated time every 24 hours even if no system events occurred within the prior 24 hours. If no events occurred, the subject remains the same (showing "0 events") and the body will contain only, "No system events generated in the past 24 hours."
- 7) Click **Save** to save the settings.

When the "selected" events occur, email notifications will be sent to the specified email addresses (according to the configured email frequency).

The following is a sample email notification that users might receive when a system event is triggered.

Send

To...

Cc...

Bcc...

Subject

System Event Summary

High-severity Events

- 1296 [Unrecorded Agent sessions](#)
- 767 [Agent service stopped](#)
- 70 [Agent service was terminated](#)
- 9 [Agent installation failed](#)

Medium-severity Events

- 530 [Agent registration was successful](#)

System Event Details

10 of 3793 shown here | [view all](#)

[High-severity Events](#) (10 of 2192 shown here)

Agent service stopped (Event ID: 1)

Received Time: Monday, 10/6/2014 3:22 PM

Severity: High

Event Code: 1202

Event Name: Agent Service has stopped

Event Description: The ObserveIT Agent Service has reported that it has stopped.

Server: OIT-LILI

Component: Agent

Source: Agent

Remediation: New

Status:

[View Details](#)

Identity Theft Detection

Due to the multiple security challenges we face today, there is a need for a higher level of security to protect users from identity theft. When identity theft occurs, fraudsters impersonate the identity of someone else in order to access their computer. The ObserveIT Identity Theft Detection solution is designed to detect access to ObserveIT monitored servers from unauthorized client computers.

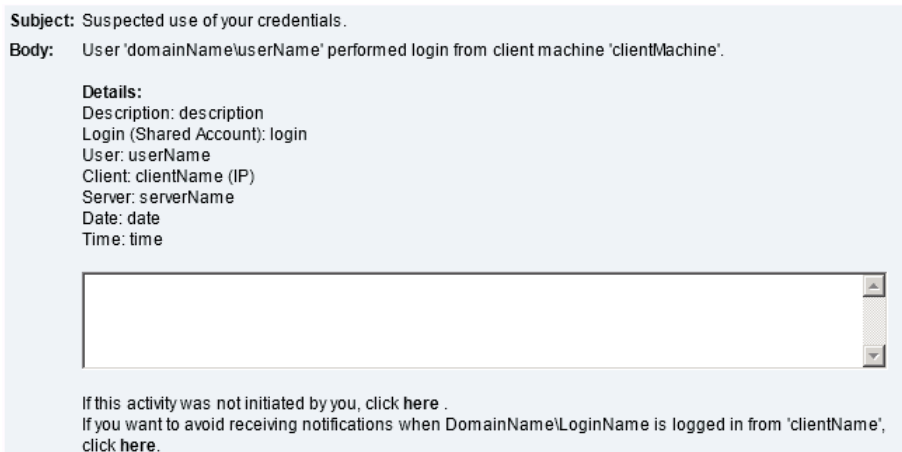
When Identity Theft Detection is enabled, and users are logged on to ObserveIT-monitored servers, ObserveIT administrators or security officers will be notified about any suspicious login. A suspicious login is defined when a user tries to log in from an unauthorized client machine.

ObserveIT keeps track of authorized user login IDs and their client machines by "pairing" the domain name/login name of the user with the client computer from which the user is logged in. If a user logs in to a server from a client that is not paired to the user, an email is sent to the user, stating that there is a suspicious login with this user's credentials. For further details, see [Configuring Pairing Requests](#).

Events are generated for each and every login whether or not they originate from paired user-clients. If a user requests a user-client pairing, a "pairing request" event is issued. The administrator can track and monitor all authorized and unauthorized login and pairing request events. For further details, see [System Events](#).

For example, if a hacker steals the credentials of a user and logs in from a remote machine, or if an internal user uses the administrator's password to log in to a server from the user's desktop, a suspicious login event is generated, and the user will receive notification about this via email. The email confirms which server the user logged on to, and from which client (user) machine they logged in. After receiving the email notification, if the user (or administrator) is indeed the person who logged in, he can ignore the email or submit another pairing request. If the user (or administrator) denies that he was the person who logged in, he should report this to the administrator.

Following is an example of a suspected identity theft email notification:



Note: To enable the Identity Theft Detection feature, the **Enable Identity Theft Detection** check box must be selected in the server's policy settings. For further details, see [Enabling Identity Theft Detection](#).

Overview of the Identity Theft Detection Process

- 1) The user logs in to a server from the desktop.
- 2) If Identity Theft Detection is enabled, the user receives an email notification about the login activity. At the same time, an event is triggered. For further details, see [System Events](#).

Note: In order for a user to receive email notifications, the user's email must be configured in the user's profile on the LDAP server. For further details on defining the LDAP mail field name, see LDAP Settings Configuration.

- 3) If the email notification indicates a suspicious login activity which was not initiated by the user:
 - a) The user can click the first link in the email text (that is, "If this activity was not initiated by you, click **here**.") to create a high severity event which will appear in the **Events** list. See [System Events](#).
 - b) An email is sent to the ObserveIT administrator reporting the suspicious login event.
- 4) If the email notification indicates login activity which *was* initiated by the user, the user can either ignore the email, or click the second link in the email text (that is, "If you want to avoid receiving notifications when DomainName/LoginName is logged in from 'clientName', click **here**."). By clicking this link, the user submits a pairing request to the administrator which in effect says "I do not want to receive emails when I connect from this client. Please approve this user-client pairing."

If the pairing request is approved by the administrator, the user will no longer receive emails about activity for this specific user-client pairing. If the administrator rejects the pairing request, the user will continue to receive email notifications about this user-client activity. In addition, a new "pairing request" event is added to the Events table with a "Not Approved" status, and a message is sent to the user confirming this.

Note: If Identity Theft Detection is enabled, and the ObserveIT system fails to send an email notification to the user, the email will be redirected to the administrator.

The following topics describe:

- [Configuring Pairing Requests](#)
- [Configuring Identity Theft Settings](#)

Configuring Pairing Requests

ObserveIT keeps track of authorized user login IDs and their client machines by "pairing" the domain name/login name of the user with the client computer from which the user logged in.

If a user logs in to a server from a client that is not paired to the user, the user is notified by email that a suspicious login occurred using the user's credentials. If the email notification indicates that the login *was* initiated by the user, the user can ignore the email, or submit a "pairing request" to the administrator, which in effect says "I do not want to receive emails when I connect from this client. Please approve this user-client pairing." If the pairing request is approved by the administrator, after receiving a confirmation email that the request was approved, the user will no longer receive emails about activity for this specific user-client pairing. If the administrator rejects the pairing request, the user receives a confirmation email that the request was rejected, and will continue to receive email notifications about this user-client activity. In addition, a new "pairing request" event is added to the Events table with a "Not Approved" status (see [System Events](#)).

For further details, see [Identity Theft Detection](#).

Creating Pairing Requests

Users can create as many pairing requests as required.

Note: An administrator can manually define and approve user-client pairs without waiting for pairing requests. For example, if the IT administrator knows that the user OBSERVEIT\danny's desktop is "OITDANNY", he can pair this user-client before Danny receives any email notifications.

To create a new pairing request

- 1) Navigate to **Configuration > Identity Theft Detection**.
- 2) Click the **Pairing Requests** tab.

The screenshot shows the ObserveIT Configuration interface. The left sidebar contains navigation links: Admin Dashboard, Console Users, Identification, Servers, Server Groups, Server Policies, Security, Alerts, System Events, Identity Theft Detection (selected), Messages, Ticket Integration, License, SMTP Settings, Monitor Log, LDAP Settings, Storage, Archive, Saved Sessions, Audit, System Log, and Latest Sessions. The top navigation bar has 'Configuration' and 'Pairing Requests' tabs. The 'Pairing Requests' tab is active, showing the 'Pairing Requests' section. It includes an 'Add User-Client Pair' button, a 'Pending Requests' section with a search bar and a table of pending requests, and an 'Approved User-Client Pairs' section with a search bar and a table of approved pairs.

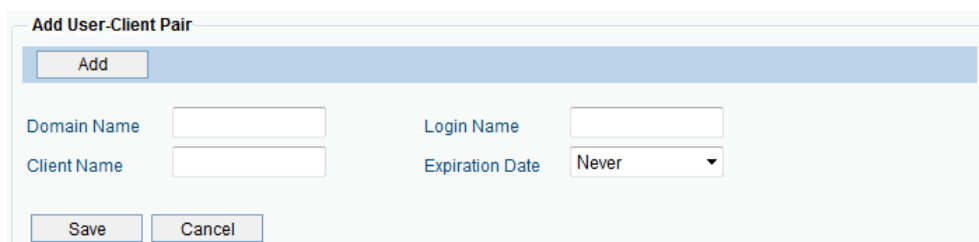
Pending Requests

Received	Client	Domain	Login	Expiration
☐	OITYA	Q1-W08-64SQ8-2	Administrator	Never

Approved User-Client Pairs

Domain	Login	Client	Expiration	Delete
OITWEB	michelle	OITWEB	5/6/2012	Delete
OIT-RINA	rina	OIT-WEB	Never	Delete
obsdev.local	Administrator	OITYI	Never	Delete
OITWEBA	tom	OIT2003DEV3	4/7/2012	Delete
OIT-RINA	tom	client	4/7/2012	Delete
OIT-RINA	rina	client	4/7/2012	Delete

- 3) In the **Add User-Client Pair** section, click **Add**.



- 4) (Mandatory) Specify the following information about the new pairing request:
- **Domain Name:** The domain name of the user.
 - **Login Name:** The login name of the user.
 - **Client Name:** The client computer to which the user is allowed to log in.
 - **Expiration Date:** The date after which the approved pairing request will no longer be valid. Options are: **3 months**, **1 year**, **3 years**, or **Never**.
- 5) Click **Save**.

The new user-client pairing request is added to the **Approved User-Client Pairs** list.

Note: You can filter the **Approved User-Client Pairs** list in order to retrieve requests from specific domains, logins, and/or clients. To search for specific approved pairs, specify your search criteria in the fields provided above the list, and click **Search**.

Approving and Rejecting Pending Requests

If a user logs in to a server from a client that is not paired to the user (that is, it does not appear in the **Approved User-Client Pairs** list), a pairing request is created. The pairing request will appear in the **Pending Requests** list. The ObserveIT administrator can approve or reject the pending request.

If there is no indication of suspicious login activity, the administrator will approve the request (and it will appear in the **Approved User-Client Pairs** list). If the login event is suspicious (that is, identity theft is suspected), the administrator receives an email reporting the suspicious login event, and will reject the pairing request.

To approve a pending request

- In the **Pending Requests** list, select the pairing request, and click **Approve**.
After receiving a confirmation email that the request was approved, the user will no longer receive emails about activity for this specific user-client pairing.

To reject a pending request

- In the **Pending Requests** list, select the pairing request, and click **Reject**.
After receiving a confirmation email that the request was rejected, the user will continue to receive email notifications about this user-client activity.

Note: You can filter the **Pending Requests** list in order to retrieve requests from specific domains, logins, and/or clients. To search for specific pending requests, specify your search criteria in the fields provided above the list, and click **Search**.

Configuring Identity Theft Settings

Important: When Identity Theft Detection is enabled in ObserveIT, in order for users to receive email notifications, SMTP must be configured, and the LDAP field name must be defined on the LDAP server. For further details, see [SMTP Configuration](#) and [LDAP Settings Configuration](#).

To send email notifications to users about logins and pairing requests, you can:

- Specify the email addresses to which emails will be sent upon new pairing requests.
- Define the default period of time for which the approved pairing requests will be valid.
- Select the server policies on which these Identity Theft Detection settings will be enabled.
- Preview, and edit if required, the email notification text that will be sent to the specified email addresses.

Defining Email Addresses

To define the email addresses to which the specified email will be sent upon each new pairing request

- 1) Navigate to **Configuration > Identity Theft Detection**.

- Click the **Settings** tab.

The screenshot shows the ObserveIT Configuration Guide interface. The top navigation bar includes links for Server Diary, User Diary, DBA Activity, Activity Alerts, Configuration, Search, Reports, and Threat Detection. The left sidebar lists various system components like Admin Dashboard, Console Users, Identification, Servers, Server Groups, Server Policies, Security, Alerts, System Events, Identity Theft Detection, Messages, Ticket Integration, License, SMTP Settings, Monitor Log, LDAP Settings, Storage, Archive, Saved Sessions, Audit, and System Log. The main content area is titled 'Settings' and contains several sections:

- Email:** A section for managing email addresses for pairing requests. It includes a text input field, a list of email addresses (danny@gmail.com, sue@observeit.com), and buttons for 'Add' and 'Remove'.
- Expiration:** A section for setting the pairing expiration period, with a dropdown menu currently set to 'Never'.
- Policies:** A section for selecting server configuration policies. It includes a list of policies (Default Metadata Only Policy, Default Recording Disabled Policy, Default Unix-based Policy, Default Windows-based Policy) and a section for applying policies to specific servers.
- Email Template:** A section for defining the email template for pairing requests. It includes a text area for the email body and a section for defining the email subject and body content.

- In the **Email** field, enter the user's email address, and click **Add**.

The email address is added to the list.

- Repeat the above step for each email address you want to add.

To remove an email address from the list, select it and click **Remove**.

Defining the Pairing Expiration Period

When approving a pairing request, the administrator must specify the length of time that the approved request will be valid.

To define the expiration period after which approved pairing requests will no longer be valid

- In the **Configuration > Identity Theft Detection > Settings** tab, select the email address(es) for which you want to define a pairing expiration period.

- 2) From the **Pairing Expiration Period** drop-down list, select the length of time that you want to allow approved pairing requests for these email addresses (users) to be valid. Options are: **3 months, 1 year, 3 years, or Never.**

After the specified expiration period, pairing requests will no longer be approved for the selected users' email addresses.

Applying Identity Theft Settings to Server Policies

To apply identity theft settings to one or more Server Configuration Policies

- 1) In the **Policies** section of the **Settings** tab, select the check boxes of the server policy templates, and/or server policies on which you want to apply the identity theft settings.

Note: It is recommended that you select all the server policy templates.

- 2) Click **Save** to save your settings.

Previewing the Email Text

- 1) In the **Email Template** section of the **Settings** tab, you can see a preview of the email text that will be sent to the user.

This email text is not editable since it is automatically generated when an event occurs, but, if required, you can add more information about the event using the text box that is provided.

- 2) Click **Save** to save the changes.

A message dialog box opens, prompting you to confirm that you want to make these changes to the Identity Theft settings.

- 3) Click **OK** to confirm.

Managing Messages

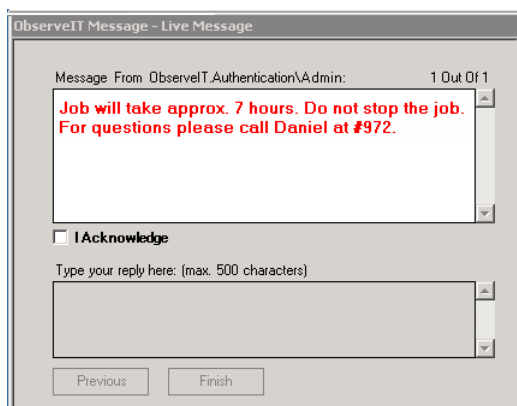
Note: The creation and configuration of messages is supported only on Windows Agents.

ObserveIT enables you to create and configure messages that will be displayed when a user logs on to one or more servers. These messages include information for the user(s), instructions, requests to perform specific tasks, contact information in case of software or hardware issues, and more.

By default, messages will be displayed to any user that logs on to the monitored servers. You can exclude specific users/groups from receiving a message and/or display a message to a limited number of users/groups.

Note: ObserveIT easily integrates with your Active Directory forest, enabling you to include (or exclude) user and groups from any domain in the forest in which the ObserveIT server-side components are installed, and in which the ObserveIT Agents are deployed (if different). Cross forest trusts can also be used. Although using groups from Active directory domains is possible with any group scope (domain local, global, or universal), it is recommended that you follow Microsoft's best practices on group object usage. For further details, refer to [Active Directory Best Practices](#).

Following is an example of a message that a user might receive from the administrator:



About Messages

- Messages can be configured to be displayed on all servers, on some servers, for all users logging on to these servers, or for specific users. In addition, you can configure messages to be displayed constantly, for a few hours, or until a specified date or time.
- Messages can be used to receive input from the user(s) logging on to these servers. After users see a message, they can provide textual feedback, such as, information about the reason for their logging on the server(s), the purpose of their connection, the actions they intend to perform, contact information, ticket or support request numbers, and more. This feedback is recorded in the ObserveIT console and can be viewed by an ObserveIT Admin or View-Only Admin, depending on their role and permissions scope.
- Unless specifically configured to lock the user's desktop, messages do not prevent users from continuing their actions and performing tasks on the server(s) for which the messages apply. To prevent users from performing harmful actions, use the built-in Windows permissions and user-rights mechanism.
- Users must acknowledge the message(s) they receive. This acknowledgment is recorded in the ObserveIT console, and can be used as proof that the user(s) have indeed been warned about a specific task, and that they understood and accepted the message.
- If a reply is configured as mandatory, the user must enter a text reply in addition to acknowledging the message.

Note: The **Mandatory Reply** feature is supported only on Windows Agents that are running ObserveIT version 5.6.0 and above. It is not supported on Unix or Linux Agents, or on Windows Agents that are running ObserveIT versions prior to 5.6.0.

- During the replay of a live session, if the Administrator wants to prevent the user from continuing to record the current session, he /she can send a message to the user and lock the user's desktop after a specified timeout period.

Note: The **Lock User's Desktop** feature is supported only on Windows Agents that are running ObserveIT version 5.6.0 and above. It is not supported on Unix or Linux Agents, or on Windows Agents that are running ObserveIT versions prior to 5.6.0.

- When messages are no longer needed, they can be disabled (and potentially re-enabled later), or deleted.

Message tasks include:

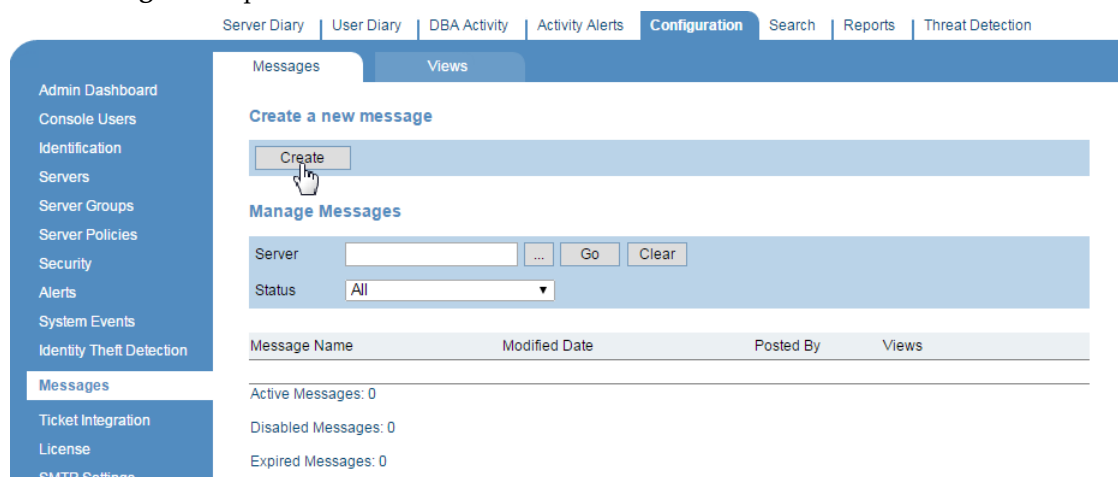
- [Creating Messages](#)
- [Editing Messages](#)
- [Viewing Messages](#)
- [Deleting Messages](#)
- [Disabling Messages](#)
- [Acknowledging and Replying to Messages](#)

Creating Messages

To create a message

- 1) Navigate to **Configuration > Messages**.

The **Messages** tab opens.



- 2) Click **Create**.

The message details page opens.

Message

[Back to Messages](#) Cancel Save

Message Details

Subject
Warning message

Message body (Please enter the text that will be displayed on the server(s)).
Security regulations require that you acknowledge that you are aware that all your actions on this server are being recorded.

☒ Mandatory Reply
☒ Lock User's Desktop

Advanced Cancel Save

- 3) In the **Message Details** section, enter a message subject and the message text that you want the user to read.
- 4) To enforce the user to send a text reply to the message, select the **Mandatory Reply** check box.
- 5) To configure the message to lock the user's desktop (if required), select the **Lock User's Desktop** check box.
- 6) Click **Save** to save the message configuration.

After a message is saved, it appears on the user's desktop immediately after they log in to the monitored server(s). Users are required to acknowledge the message(s) they receive. This acknowledgment is recorded in the ObserveIT Console, and can be used as proof that the user(s) have indeed been warned about a specific task, and that they understood and accepted the message. When **Mandatory Reply** is configured for messages, users must provide textual feedback, such as information about the reason for their logging on the server(s), the purpose of their connection, the actions they intend to perform, contact information, ticket or support request numbers, and more. When **Lock User's Desktop** is configured for a message, users will be unable to access their desktop until they acknowledge the message.

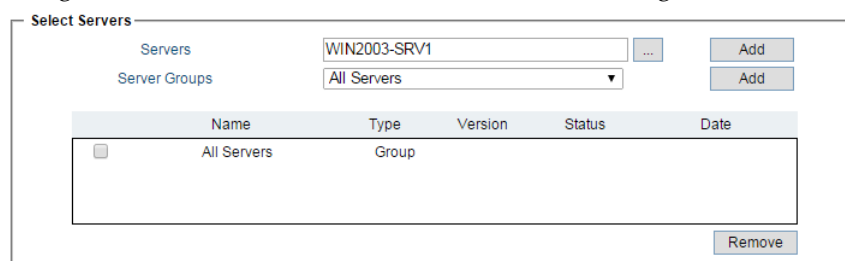
Configuring Advanced Message Settings - Servers, Users, Message Display Duration

You can specify the servers on which to display the message, the users who will receive the message, and the message display duration.

To select the servers on which to display the message

- 1) In the **Message Details** section (in the **Message > Create** page), click  to expand the **Advanced** section.

By default, the message will be displayed on all the monitored servers. You can change that by using the **Select Servers** section of the **Advanced** settings.



Name	Type	Version	Status	Date
All Servers	Group			

- 2) In the **Select Servers** section, in the **Servers** field, click  to browse for specific servers on which you want to display the message.
- 3) From the **Server Groups** drop-down list, select a group of servers to add to the list.

Note: Unless you want the message to be displayed on all the monitored servers, make sure you also remove the **All Servers** group from the list of servers.

To select the users who will receive the message

- 1) In the **Select Users** section of the **Advanced** settings, you can configure which users will receive the message, as follows.

By default, the message will be displayed to any user that logs on to the monitored servers.

By default, the message will be displayed forever, until disabled or deleted by an ObserveIT administrator.

Display Message Duration

☒ Forever
☐ For the next hours.
☐ Up to
☐ Display message only once (Do not select this check box if you always want this message to be displayed).

- Change the display interval of the message by selecting one of the options (**Forever**, **For the next x hours**, or **Up To** date).
- If you want to display the message only once, select the **Display message only once** check box.

When you have finished configuring the **Advanced** settings, click the **Save** button at the bottom of the page.

Editing Messages

You can edit messages in order to make changes to the title, text, or other settings.

To edit messages

- In the **Configuration > Messages** page, click the **Edit** link next to the message you want to edit.

The message's details page opens, where you can edit the message.

Viewing Messages

You can view all instances where a message was displayed on servers. This information can be used to track user sessions and their interaction with the desktop. Furthermore, having proof that a user was indeed presented with the message, and acknowledged it, can be useful for auditing and security purposes. You can view messages in several places.

To view messages

- In the **Messages** list in the **Configuration > Messages** page, navigate to the **Views** column and note the number of times that the message was displayed.

- 2) Click the message you want to view.

Messages Views

Create a new message

Create

Manage Messages

Create

Server ... Go Clear

Status All

Results: 1 - 2 of 2 1

Message Name	Modified Date	Posted By	Views
Who has approved access t...	8/1/2010 5:37:13 PM	Admin	2
Do not stop the backup jo...	8/1/2010 5:22:46 PM	Admin	6

Active Messages

Job will take approx. 7 hours. Do not stop the job. For questions please call Daniel at #972.

Disabled Messages: 0

The **Views** tab opens, displaying all the instances of the selected message, including the server name, user name, date and time, where the message was displayed, and when the user acknowledged it. It also displays the user input or feedback, if any was provided.

Configuration

Messages Views

Messages Diary

Server ... Go Clear

Message To Display Do not stop the backup job!

Message To Display

Name: Do not stop the backup job!

Body: Job will take approx. 7 hours. Do not stop the job. For questions please call Daniel at #972.

Results: 1 - 6 of 6 1

Name	Body	Reply	Login	Host	Displayed At	Acknowledge
Do not sto...	Job will t...	Ok, just checking the security log...	Administrator	WIN2003-SRV1	8/1/2010 5:43:23 PM	05:49:46 PM
Do not sto...	Job will t...	no reply was given	Administrator	WIN2003-SRV1	8/1/2010 5:38:08 PM	05:42:32 PM
Do not sto...	Job will t...	no reply was given	Administrator	WIN2003-SRV1	8/1/2010 5:37:31 PM	05:37:39 PM
Do not sto...	Job will t...	I am just checking the Event Viewer.	Administrator	WIN2003-SRV1	8/1/2010 5:25:14 PM	05:26:48 PM
Do not sto...	Job will t...	no problem...	Administrator	WIN2003-SRV1	8/1/2010 5:24:06 PM	05:24:48 PM
Do not sto...	Job will t...	ok	Administrator	WIN2003-SRV1	8/1/2010 5:23:18 PM	05:23:39 PM

- 3) You can filter this display by using a specific server name. Click the button to browse for specific servers.

To view messages in the Server Diary

- 1) In the **Server Diary > Activities View**, you can view messages in the sessions list. Search for the required server and user session, then expand it to view the messages.

Session Duration	Login	User	Server	Client	Slides	Video
8/1/2010						
5:43 PM - 5:50 PM	Administrator	n/a	WIN2003-SRV1 (local)		29	
Print this information Print detailed information						
Message: Job will take approx. 7 hours. D... Reply: Ok, just checking the security l... Acknowledge: Yes Message: Enter the name of the person tha... Reply: No Reply Acknowledge: Yes						
ObserveIT Message - Do not stop the backup job!						
ObserveIT Message - Who has approved access to this server?						
Program Manager						
Remote Desktops (2)						
Add New Connection						

- 2) In the **Server Diary > Messages View**, you can view all instances of messages on the selected server. To display all the messages, from the **Message to Display** drop-down list, click **All Messages**.

Activities

Applications

Inventory

Software

Search

Messages

Latest Sessions

WIN2003-OIT... Admini...

WIN2003-SRV... Admini...

WINXP-CL... Admini...

WIN2003-DC Admini...

Quick Help

Installation

Getting Started

Server Diary

Messages

Messages Diary

Server

WIN2003-SRV1

Go

Message To Display

All Messages

All Messages

Do not stop the backup job!

Who has approved access to this ser...

Results: 1 - 9 of 9

Name	Body	Reply	User	Login	Displayed At	Acknowledge
Who has ap...	Enter the ...	no reply was given	n/a	Administrator	8/1/2010 5:49:46 PM	05:49:48 PM
Do not sto...	Job will t...	Ok, just checking the security log...	n/a	Administrator	8/1/2010 5:43:23 PM	05:49:46 PM
Who has ap...	Enter the ...	no reply was given	n/a	Administrator	8/1/2010 5:39:20 PM	05:42:35 PM
Do not sto...	Job will t...	no reply was given	n/a	Administrator	8/1/2010 5:38:08 PM	05:42:32 PM
Who has ap...	Enter the ...	Danielp	n/a	Administrator	8/1/2010 5:37:39 PM	05:37:43 PM
Do not sto...	Job will t...	no reply was given	n/a	Administrator	8/1/2010 5:37:31 PM	05:37:39 PM
Do not sto...	Job will t...	I am just checking the Event Viewer.	n/a	Administrator	8/1/2010 5:25:14 PM	05:26:48 PM
Do not sto...	Job will t...	no problem...	n/a	Administrator	8/1/2010 5:24:06 PM	05:24:48 PM
Do not sto...	Job will t...	ok	n/a	Administrator	8/1/2010 5:23:18 PM	05:23:39 PM

To view messages in the Session Player

- In the **Configuration > Messages > Views** tab, click the **Video** icon next to the relevant message to replay a user session which will display the message, as the user experienced it.

Deleting Messages

After a message is created, it can be easily deleted.

Note: A deleted message cannot be re-enabled.

To delete a message

- In the **Configuration > Messages** page, click the **Delete** link next to the message you want to delete.

The screenshot shows the ObserveIT Configuration > Messages page. The left sidebar contains a navigation menu with options like Admin Dashboard, Console Users, Identification, Servers, Server Groups, Server Policies, Security, Alerts, System Events, Identity Theft Detection, Messages, Ticket Integration, License, SMTP Settings, Monitor Log, and LDAP Settings. The main content area has tabs for Messages and Views. Under Messages, there is a 'Create a new message' section with a 'Create' button, and a 'Manage Messages' section with filters for Server and Status. A table lists messages, with one message 'Warning message' shown. The table has columns for Message Name, Modified Date, Posted By, and Views. For the 'Warning message', the Modified Date is 1/12/2015 6:57:16 PM, Posted By is Admin, and Views is 0. To the right of the message are links for Edit, Disable, and Delete. A tooltip points to the Delete link with the text 'Click to delete this message'.

Disabling Messages

After a message is created, it can be easily disabled. Disabling a message allows you to temporarily prevent it from being displayed. Disabled messages can be re-enabled.

To disable a message

- In the **Configuration > Messages** page, click the **Disable** link next to the message you want to disable.

This screenshot is identical to the one above, showing the ObserveIT Configuration > Messages page. However, the tooltip points to the 'Disable' link instead of the 'Delete' link, with the text 'Click to disable this message'.

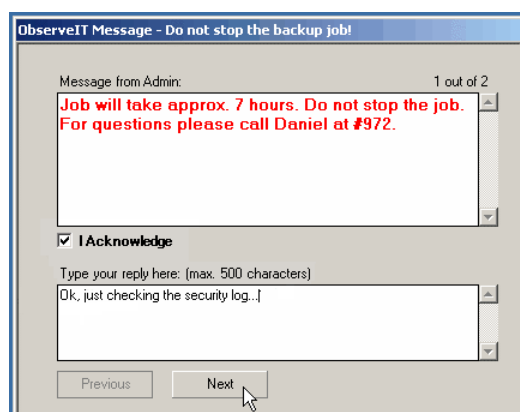
To re-enable the message, click the **Enable** link next to the message.

Acknowledging and Replying to Messages

Acknowledging Messages

Users must acknowledge each message they receive. This information can be used to track user sessions and their interaction with the desktop. Furthermore, having proof that a user was indeed presented with the message, and that they acknowledged it, can be useful for auditing and security purposes. Without acknowledging the message(s), the messages window cannot be moved, minimized, or closed.

When a message is displayed, the user must select the **I Acknowledge** check box in order to proceed to the next message (in the case of multiple messages queued for display), and for the **Finish** button to be available.



Note: ObserveIT does NOT prevent the user from working with applications around the window. However, if the user does not acknowledge a message, this will be seen in the ObserveIT **Server Diary**.

After acknowledging the last (or only) message, the **Finish** button becomes available. The time of user acknowledgment can also be viewed with the message and feedback information.

Replying to Messages - Providing User Input on Messages

Users that receive messages can provide textual feedback or input for each message. The feedback box remains grayed-out until the user selects the **I Acknowledge** check box, after which the user can enter feedback. There is a 500 character limit on the feedback. If multiple messages are queued for display, the user can provide separate feedback for each of the messages.

Note: If a reply is configured as mandatory, the user *must* enter a text reply in addition to acknowledging the message.

When the user has finished providing input, the user can click **Next** to proceed to the next message. For the final message, the user must click the **Finish** to close the messages window.

Ticketing System Integration

When ObserveIT's session recording system is integrated with an IT ticketing system, selected IT administrators or remote vendors can be requested to enter a valid ticket number in order to complete the login process to a corporate server. A ticket is an element in an issue tracking system that references specific information about the issue. Each ticket has a unique reference number, also known as a case, issue or call log number, which allows the user to quickly locate, add information, or update the status of the issue or request.

The benefits of integrating an IT ticketing system with ObserveIT's session recording system include:

- Enforced segregation of duties.
- Improved security by limiting server access to administrators and remote vendors who are in possession of a specific ticket number for which access to the server is required.
- Improved tracking of sessions. You can search for all sessions that are related to a specific ticket instead of using search key words or looking through lists of sessions.
- Faster and easier user activity auditing. By linking tickets directly to the video recording of the server session that addressed the ticket, you can easily review the exact actions performed by administrators in the context of the ticket.

The following types of ticketing systems can be integrated with ObserveIT:

- **Built-in ticketing systems** are provided by ObserveIT as out-of-the-box integrations (ServiceNow is currently supported).
- **Customized ticketing systems** are implemented by customers according to their own requirements.

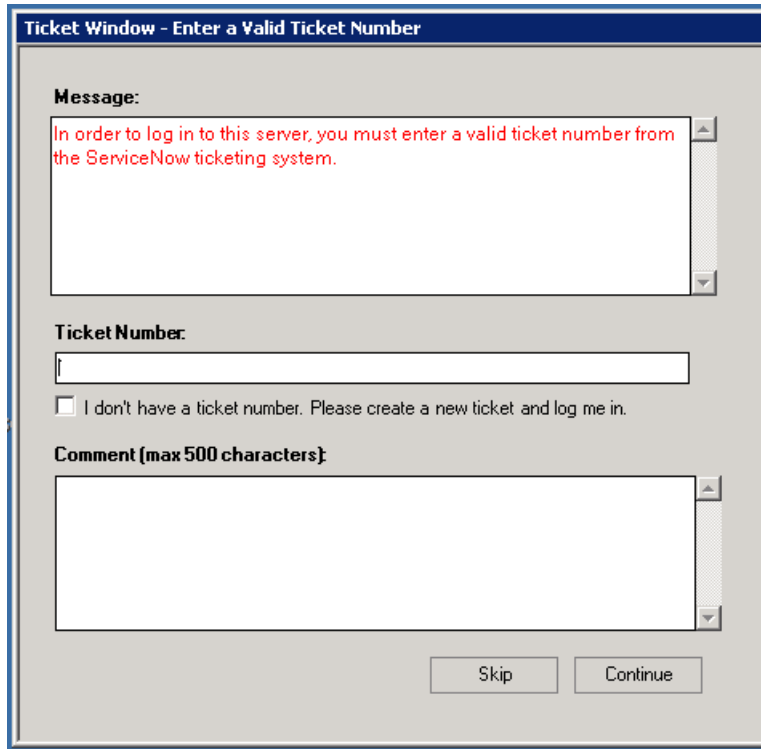
Note: ObserveIT provides API instructions to help customers build a Web Service that will enable them to implement the integration of ObserveIT with their own ticketing system. The ObserveIT installation package includes a template project as an example of a Web Service that was created by ObserveIT to demonstrate how the customer Web Service should be built. For further details, see the [ObserveIT Ticketing Integration Guide](#).

Overview of the IT Ticketing System Integration Process with ObserveIT

- 1) An IT administrator/remote vendor logs on to an ObserveIT-monitored server or workstation by entering their credentials in the regular Windows Authentication log on screen.

Note: If ObserveIT's Identification Services are enabled and configured, users will be required to identify themselves with a secondary ObserveIT log on prompt. For further details, see [Identification Services](#).

- 2) Before the user can access the requested server, a message is displayed prompting the user to enter a valid ticket number from a ticketing system in order to log on to the server, as shown in the following example.



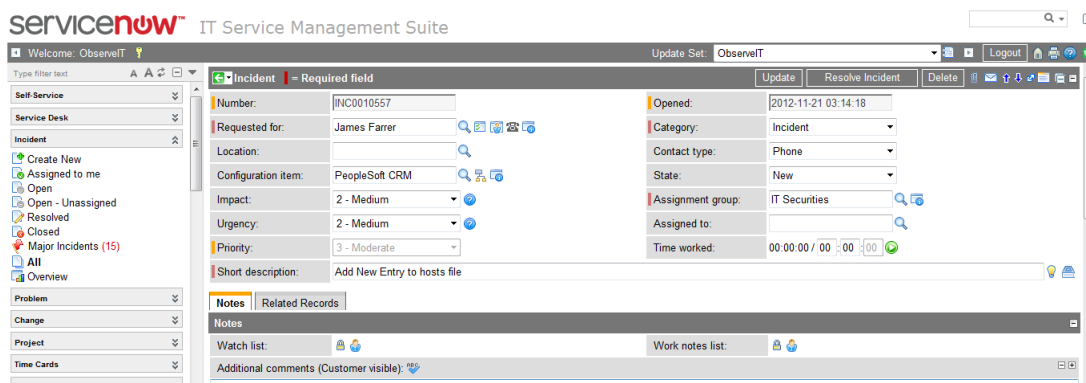
The screenshot shows a dialog box titled "Ticket Window - Enter a Valid Ticket Number". It contains a "Message:" section with a text area displaying the message: "In order to log in to this server, you must enter a valid ticket number from the ServiceNow ticketing system." Below this is a "Ticket Number:" label followed by a text input field. Under the input field is a checkbox with the text "I don't have a ticket number. Please create a new ticket and log me in." Below the checkbox is a "Comment (max 500 characters):" label followed by a larger text area. At the bottom right of the dialog are two buttons: "Skip" and "Continue".

Note: A "ticket policy" may be configured to allow a user that does not have a valid ticket number to request the creation of a new ticket on-the-fly and be logged in, or to allow access to the system even without a valid ticket number (in this case, the **Skip** button will be enabled) . For further details, see [Configuring Ticketing Policies](#).

- 3) ObserveIT verifies, via the ticketing system, that the ticket number is valid before allowing the user to proceed. If the user enters an incorrect ticket number, an error is displayed.
- 4) After logging on to the server, the user can make required session changes, including any requests specified in the ticket itself.
- 5) The ticket associated with the session is linked to a video recording of the session. In addition, specific information about the login session is automatically saved by ObserveIT and included in the ticketing system.

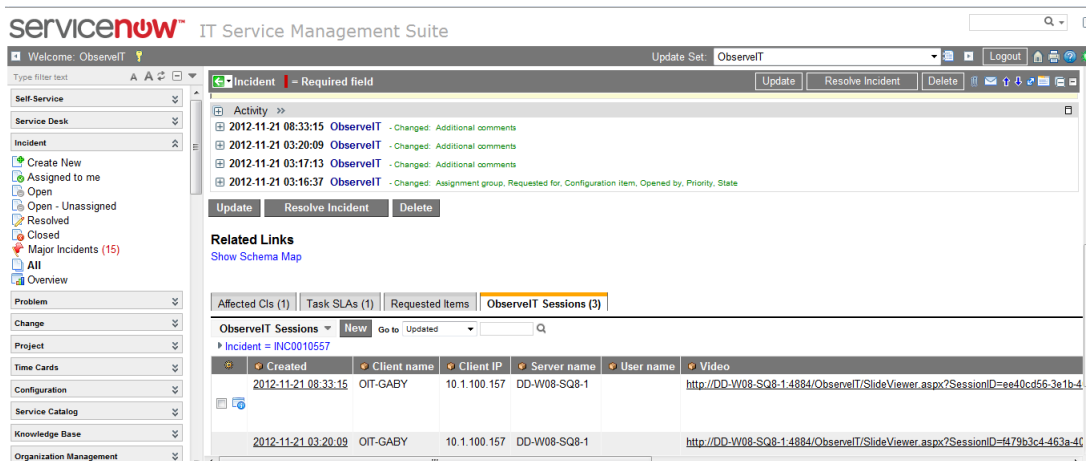
Viewing Ticket Details

In the ticketing system itself, you can open the ticket number and view the ticket details, as shown in the following example.



The lower part of the ticketing system window displays all the activity that occurred on the ticket, including user comments. You can see all the sessions that are associated with the ticket with links to the video of each session, and other information that was included by ObserveIT (such as, the server that was used, date of session, and so on).

Note: You can click directly on the link to call up that session, and play back the session in the **Session Player**, as required. For further details, see *Replaying User Sessions* (in the User Guide).



The following topics in this section describe how to configure ticketing policies and ticketing systems settings:

- [Configuring Ticketing Policies](#)
- [Configuring Ticketing Systems](#)

Configuring Ticketing Policies

When an IT ticketing system is integrated with ObserveIT's session recording system, IT administrators or remote vendors may be required to enter a valid ticket number in order to complete the login process to corporate servers. To enable this feature, you must configure ticketing policies in the ObserveIT system. For further details, see [Ticketing System Integration](#).

When configuring a ticketing policy, you can specify the servers and server groups on which the ticketing policy will be applied. You can also specify which users will receive a ticketing policy message upon logging in to the monitored servers; you can exclude specific users/groups from receiving the message or display the message to a limited number of users/groups.

Note: ObserveIT easily integrates with your Active Directory forest, enabling you to include (or exclude) user and groups from any domain in the forest in which the ObserveIT server-side components are installed, and in which the ObserveIT Agents are deployed (if different). Cross forest trusts can also be used. Although using groups from Active directory domains is possible with any group scope (domain local, global, or universal), it is recommended that you follow Microsoft's best practices on group object usage. For further details, refer to [Active Directory Best Practices](#).

The following procedures describe how to:

- Create a new ticketing policy
- Edit the parameters of existing ticketing policies
- Disable ticketing policies
- Delete ticketing systems

To create a new ticketing policy

- 1) Navigate to **Configuration > Ticketing Integration**.

The **Ticketing Policies** tab opens, displaying all the currently active and disabled ticket policies in the system. From this tab, you can create new ticketing policies, update the parameters of existing ticketing policies, disable, and delete ticketing policies.

Title	System Name	Modified Date	Posted By
Active Tickets			
ServiceNow Ticket Detail...	New System	11/22/2012 1:30:49 PM	Admin Disable Delete
Ticket Validation	Custom Web Service	11/22/2012 1:28:10 PM	Admin Disable Delete
Disabled Tickets			
Check Ticket Details	Custom Web Service	11/22/2012 1:32:34 PM	Admin Enable Delete

- 2) Click **Create**.

The **New Ticket** page opens.

- 3) From the **Ticketing system** drop-down list, select the name of the ticketing system to which you want to assign this ticketing policy.

Note: Ticketing systems can be built-in or customized. For further details, see [Configuring Ticketing Systems](#).

- 4) In the **Ticket Details** section, specify the following information:
 - a) **Window Title:** Define a title for the ticket which will appear in the Ticket Window upon user login (for example, "Enter a valid ticket number").
 - b) **Message To User:** Enter the message text that will be displayed to the user in the Ticket Window.
 - c) Optionally, if you want to enforce the user to send a text reply to the ticket message, select the **Comments Mandatory** check box.
 - d) **Policy Type:** Select one of the following options to define the required policy regarding the ticket number:
 - **Always require a valid** existing ticket number: The user will not be able to log in to the system without providing a valid ticket number.

- **Require a valid ticket number, but also allow on-the-fly creation of a new ticket:** If the user does not have a valid ticket number, the user can select the check box, I don't have a ticket number. Please create a new ticket and log me in, and a new ticket will be created in the ticketing system.
 - **Ticket number is optional:** A ticket number is not mandatory for the user to be able to log in to the system.
- a) **System Logo File (optional):** Browse to select the logo image file to include the logo of the selected ticketing system. The selected image is displayed in the preview box. (You can click **Remove** next to the image to change it). Note that supported image formats are .jpg, .png, or .gif; maximum supported image dimensions are 160 pixels (width) x 40 pixels (height).
- 5) In the **Select Servers** section, configure the servers and server groups on which the ticketing policy will be applied, as follows:
- To browse for specific servers on which to apply the ticketing policy, click the  button and select the servers from the Server List, then click **Add**.
 - To apply the ticket policy to a group of servers, select the server group from the **Server Groups** drop-down list, then click **Add**. Options include: **All Servers**, **Active Servers**, **Windows Servers**, or **Unix Servers**.

Note: You must add at least one server. Default servers are not provided.

To remove servers from the list of servers on which the ticket policy will be applied, select them and click **Remove**.

- 6) In the **Select Users**, specify which users will receive the ticketing policy message upon logging in to the monitored servers. By default, the message will be displayed to any user that logs on to the selected servers.

Select Users

☒ Send message to any users logging on to above servers:
To exclude specific users from logging on, please enter **Domain Name Login** (e.g. *administrator or OBSERVEIT\danielp).

Exclude: Domain (* for all) Login

User \

Domain\User	Created Date	Type

☐ Send message only to the following users:
To include specific users from logging on, please enter **Domain Name Login** (e.g. *administrator or OBSERVEIT\danielp).

Include: Domain (* for all) Login

User \

Domain\User	Created Date	Type

- 7) To exclude specific users from receiving the ticketing policy message, you can add them to the **Exclude** list.
 - a) From the **Exclude** drop-down list, select **User** or **Group**.
 - b) If you selected **User**, enter the **Domain** or select it from the list, specify the user's **Login** name, and click **Add**.
 - c) If you selected **Group**, enter the **Domain Name** or select it from the list, specify the group name in the **Group Name** field, and click **Add**.

Note: The **Domain/Domain Name** drop-down list displays all the domains in the Active Directory forest in which the ObserveIT Application Server is a member. You can select "*" to exclude any user with the specified login name from receiving the message, regardless of the user's domain.

To remove users or groups from the **Exclude** list, select them and click **Remove**.

- 8) To display the ticketing policy message to a limited number of users, select **Send message only to the following users**, and specify the required users or user groups that you want to include, as follows:
 - a) From the **Include** drop-down list, select **User** or **Group**.
 - b) If you selected **User**, enter the **Domain** or select it from the list, specify the user's **Login** name, and click **Add**.
 - c) If you selected **Group**, enter the **Domain Name** or select it from the list, specify the group name in the **Group Name** field, and click **Add**.

Note: The **Domain** drop-down list displays all the domains in all the forests in the network. You can select "*" to enable any user with the specified login name to receive the ticketing message, regardless of the user's domain.

To remove users or groups from the **Include** list, select them and click **Remove**.

- 9) When you have finished configuring your new ticketing policy, click **Save**.

The newly-created ticketing policy is displayed in the list of **Active Tickets** in the **Ticketing Policies** tab.

To update an existing ticket policy

- 1) In the list of **Active Tickets** in the **Ticketing Policies** tab, select the ticket policy that you want to update.
- 2) Edit the required parameters (as described above), and click **Save**.

The updated ticketing policy is displayed in the list of **Active Tickets** in the **Ticketing Policies** tab.

To disable a ticket policy

- In the list of **Active Tickets** in the **Ticketing Policies** tab, select the ticket policy that you want to disable, and click the adjacent **Disable** link.

The ticket policy is moved to the list of **Disabled Tickets** in the **Ticketing Policies** tab.

To delete a ticket policy

- In the list of **Active Tickets** in the **Ticketing Policies** tab, select the ticket policy that you want to delete, and click the adjacent **Delete** link.

After a confirmation message, the ticket policy is removed from the list of **Active Tickets**.

Configuring Ticketing Systems

When IT administrators or remote vendors are required to enter a ticket number from a ticketing system in order to complete the login process to a corporate server, the ticket number that is entered by the user must be validated against the ticketing system.

ObserveIT ticketing systems can be built-in or customized.

- 1) Built-in ticketing systems are provided by ObserveIT as out-of-the-box integrations ("ServiceNow" is currently supported).
- 2) Customized ticketing systems are implemented by customers according to their own requirements.

Note: ObserveIT provides a template project as an example of a Web Service to help customers implement the integration with their own IT ticketing system. For further details, refer to the [ObserveIT Ticketing Integration Guide](#).

The following procedures describe how to:

- Create new ticketing systems
- Edit the parameters of existing ticketing systems
- Delete ticketing systems

To create a new ticketing system

- 1) Navigate to **Configuration > Ticket Integration**.
- 2) Click the **Ticketing Systems** tab.

The **Ticketing Systems** tab opens, displaying a list of all the currently existing ticketing systems. Each ticketing system has a name and a URL to the server on which it is located.

The screenshot shows the ObserveIT Configuration page. The 'Configuration' tab is selected, and the 'Ticketing Systems' sub-tab is active. On the left, a sidebar menu lists various system components. The main content area, titled 'Ticketing Systems Settings', contains a 'Create' button and a table of existing ticketing systems.

System Name	Ticketing System	Server URL	
Custom Web Service	Custom Integration	http://localhost:4884/ObserveITApplicationServer/Tick...	Delete
New System	ServiceNow	https://crossfuzdev.service-now.com/	Delete

- 3) Click the **Create** button.

The **Ticketing System Settings** page opens, enabling you to define the ticketing system and test the connection settings.

- 4) In the **Connection Settings** section, specify the following information:
 - a) From the **Ticketing System** drop-down list, select either **ServiceNow** (built-in) or **Custom Integration**, depending on the type of ticketing system you want to create.
 - b) In **System Name**, specify a name for the new ticketing system.
 - c) In **Service URL**, enter the URL to the server on which the ticketing system (built-in) is located, or to the Web Service that was used to create the ticketing system (for a custom integration).
 - d) If you are configuring a built-in ticketing system, enter your **User Name** and **Password**. Note that these fields are not mandatory for a custom integration.
 - e) In the **Validation Message** text box, enter a message which the user will see in the case of an invalid ticket number, or accept the default message by clicking the **Default** button.
 - f) If you are configuring a built-in ticketing system, you can choose the relevant check box to **Validate the User ID in ticket** and/or **Validate Server ID in ticket** when validating the ticket number.
- 5) After configuring your ticketing system, click **Test Connection** to test the connection settings. A message is displayed, informing whether the connection is successful.
- 6) If the connection is successful, click **Save** to save your settings.
The newly-created ticketing system will be included in the list of ticketing systems on which you can apply ticketing policies. For details, see [Configuring Ticketing Policies](#).

To update an existing ticketing system

- 1) In the list of currently existing ticketing systems, select the ticket system whose parameters you want to update.
- 2) Edit the required parameters (as described above), test the connection, and then save your settings.
The updated ticketing system will be included in the list of ticketing systems.

To delete a ticket system

- In the list of currently existing ticketing systems, select the ticket system you want to delete, and click the adjacent **Delete** link.

A confirmation message is displayed. The ticketing system is removed from the list.

SMTP Configuration

To send messages to the configured Console Users, ObserveIT must be configured to use SMTP.

To configure SMTP settings

- In the **Configuration > SMTP Settings** tab, enter the following information:

- Name or IP address of the **SMTP Server**
- Mail From** email address
- User Name** and **Password**, to authenticate with the SMTP server

This can be an internal SMTP server such as Exchange 2000/2003/2007/2010, an internal server running IIS and the SMTP service, or your ISP's outgoing email server.

You can also configure a different port, if required by the SMTP service provider.

- Click **Update** to save the settings.

When using your ISP's outgoing SMTP server, make sure that you are using the correct user name and password. When in doubt, contact your ISP.

The screenshot displays the 'SMTP Settings' configuration page within the ObserveIT interface. The page has a blue header with navigation tabs: Server Diary, User Diary, DBA Activity, Activity Alerts, Configuration (selected), Search, Reports, and Threat Detection. A left sidebar contains a menu with options: Admin Dashboard, Console Users, Identification, Servers, Server Groups, Server Policies, Security, Alerts, System Events, Identity Theft Detection, Messages, Ticket Integration, License, SMTP Settings (highlighted), and Monitor Log. The main content area is titled 'SMTP Settings' and contains the following fields and controls:

- SMTP Server:** Text box containing '192.168.100.1'.
- Port:** Text box containing '25'.
- Mail From:** Text box containing 'support@observeit.com'.
- User Name:** Text box containing 'administrator'.
- Password:** Text box with masked characters (dots).
- Buttons:** 'Update' and 'Delete' buttons are located below the Password field.
- Message:** A prompt below the buttons reads 'Please enter a valid email address for the settings verification message.'
- Email Address:** An empty text box for verification.
- Send Button:** A button located below the Email Address field.

A message will be displayed confirming that the settings were successfully applied.

- To verify the settings, enter a valid email address in the **Email Address** text box, and click **Send**.

Monitoring Log Files

ObserveIT creates textual log files for recording all activity as it happens on the monitored servers. These log files, which are stored on the server's hard disk, contain important metadata information, such as the date and time of user sessions, server name, user name, application window titles, Unix commands, and executable names. In addition, the log files include image URLs for each recorded user session.

You can use third-party monitoring and management tools (such as, Microsoft System Center Operation Manager, or similar products from leading vendors, such as, IBM QRadar, HP ArcSight, Splunk, McAfee SIEM/ELM) to parse the log files, and create events, triggers, and alerts, based on text strings of information that appear inside the log files. ObserveIT can thus be integrated into your existing monitoring software and provide very important real-time alerting and reporting capabilities.

Note: In this version of ObserveIT, integration is provided with the HP ArcSight SIEM monitoring software, by enabling the export of ObserveIT log data in ArcSight CEF format.

For information about how to configure alert or event logging with Microsoft System Center Operation Manager 2007, refer to the Knowledge Base article: [Creating security alerts of abnormal user actions on Windows servers using Microsoft System Center Operation Manager and ObserveIT](#).

The following topics describe:

- [Monitoring ObserveIT Logs](#)
- [Integrating Logs into SIEM Systems](#)

Monitoring ObserveIT Logs

The monitor log files record all activity as it happens on the servers. These log files contain important metadata information such as the date and time of a user session, server name, user session, user name, application window titles, Unix commands, executable names, and more. Monitored log files include an image URL for each recorded user session.

ObserveIT creates two types of log files that monitor all user activity (Windows and Unix-based server activities, and activity alerts) and user logins on the servers: **User Activities** log file and **User Logins** log file.

The **User Activities** log file comprises the following files:

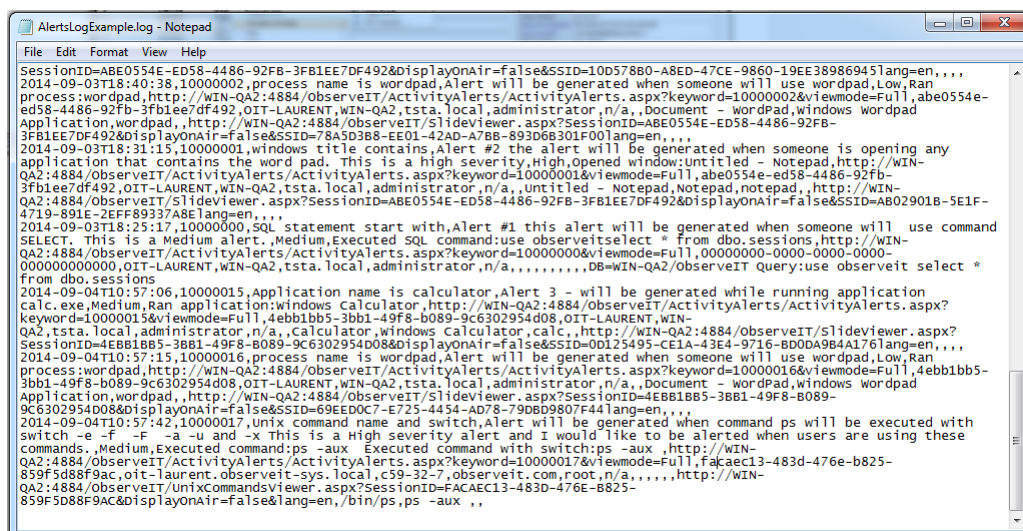
- 1) `cmYYYYmmdd.log`: Monitors both Windows-based and Unix-based server activities. This file is located under Directory 3.
- 2) `AlYYYYmmdd.log`: Monitors the activity alerts in the system. This file is located under the "Alerts" Directory.
- 3) `exYYYYmmdd.log`: Monitors all Windows-based server activities. This file is located under Directory 1.
- 4) `unYYYYmmdd.log`: Monitors all Unix-based server activities. This file is located under Directory 1.

The **User Logins** log file monitors user logins to all the servers. This file, named `exyyyymmdd.log`, is located under Directory 2.

By default, the monitor log files are saved to: `C:\Program Files (x86)\ObserveIT\NotificationService\LogFiles`. The user account used by the ObserveIT Notification Service must have read and write permissions for the specified location.

Note: When changing the default log folder location, new session data will be stored in the new path; existing data will remain in the old location.

Following is an example of an ObserveIT monitor log showing alerts activity data:



```

AlertsLogExample.log - Notepad
File Edit Format View Help
SessionID=ABE0554E-ED58-4486-92FB-3FB1EE7DF492&DisplayOnAir=false&SSID=10D578B0-A8ED-47CE-9860-19E389869451lang=en,...
2014-09-03T18:40:38,10000002,process name is wordpad,Alert will be generated when someone will use wordpad,Low,Ran
process:wordpad,http://WIN-QA2:4884/ObserveIT/ActivityAlerts/ActivityAlerts.aspx?keyword=10000002&viewmode=Full,abe0554e-
ed58-4486-92fb-3fb1ee7df492,OIT-LAURENT,WIN-QA2,tsta.local,administrator,n/a,,Document - wordPad,Windows wordpad
Application,wordpad,http://WIN-QA2:4884/ObserveIT/Slideviewer.aspx?SessionID=ABE0554E-ED58-4486-92FB-
3FB1EE7DF492&DisplayOnAir=false&SSID=78A5D3B8-EE01-42AD-A7B8-893D68301F00lang=en,...
2014-09-03T18:31:15,10000001,windows title contains,Alert #2 the alert will be generated when someone is opening any
application that contains the word pad. This is a high severity,High,opened window:Untitled - Notepad,http://WIN-
QA2:4884/ObserveIT/ActivityAlerts/ActivityAlerts.aspx?keyword=10000001&viewmode=Full,abe0554e-ed58-4486-92fb-
3fb1ee7df492,OIT-LAURENT,WIN-QA2,tsta.local,administrator,n/a,,Untitled - Notepad,Notepad,http://WIN-
QA2:4884/ObserveIT/Slideviewer.aspx?SessionID=ABE0554E-ED58-4486-92FB-3FB1EE7DF492&DisplayOnAir=false&SSID=AB02901B-5E1F-
4719-891E-2EFF89337A8E1lang=en,...
2014-09-03T18:25:17,10000000,SQL statement start with,Alert #1 this alert will be generated when someone will use command
SELECT. This is a Medium alert,Medium,Executed SQL command:use observeitselect * from dbo.sessions,http://WIN-
QA2:4884/ObserveIT/ActivityAlerts/ActivityAlerts.aspx?keyword=10000000&viewmode=Full,00000000-0000-0000-0000-
000000000000,OIT-LAURENT,WIN-QA2,tsta.local,administrator,n/a,,,,,,,,,DB-WIN-QA2/ObserveIT Query:use observeit select *
from dbo.sessions
2014-09-04T10:57:06,10000015,Application name is calculator,Alert 3 - will be generated while running application
calc.exe,Medium,Ran application:windows calculator,http://WIN-QA2:4884/ObserveIT/ActivityAlerts/ActivityAlerts.aspx?
keyword=10000015&viewmode=Full,4eb1bb5-3bb1-49f8-b089-9c6302954d08,OIT-LAURENT,WIN-
QA2,tsta.local,administrator,n/a,,calculator,Windows calculator,calc.,http://WIN-QA2:4884/ObserveIT/Slideviewer.aspx?
SessionID=4EB1BB5-3BB1-49F8-B089-9C6302954D08&DisplayOnAir=false&SSID=0D125495-CE1A-43E4-9716-BD0DA9B4A176lang=en,...
2014-09-04T10:57:15,10000016,process name is wordpad,Alert will be generated when someone will use wordpad,Low,Ran
process:wordpad,http://WIN-QA2:4884/ObserveIT/ActivityAlerts/ActivityAlerts.aspx?keyword=10000016&viewmode=Full,4eb1bb5-
3bb1-49f8-b089-9c6302954d08,OIT-LAURENT,WIN-QA2,tsta.local,administrator,n/a,,Document - wordPad,Windows wordpad
Application,wordpad,http://WIN-QA2:4884/ObserveIT/Slideviewer.aspx?SessionID=4EB1BB5-3BB1-49F8-B089-
9C6302954D08&DisplayOnAir=false&SSID=69EE00C7-E725-4434-AD78-790B09807F44lang=en,...
2014-09-04T10:57:42,10000017,unix command name and switch,Alert will be generated when command ps will be executed with
switch -e -f -F -a -u and -x This is a High severity alert and I would like to be alerted when users are using these
commands,Medium,Executed command:ps -aux Executed command with switch:ps -aux,http://WIN-
QA2:4884/ObserveIT/ActivityAlerts/ActivityAlerts.aspx?keyword=10000017&viewmode=Full,facaec13-483d-476e-b825-
859f5d88f9ac,oit-laurent.observeit-sys.local,c39-32-7,observeit.com,root,n/a,,,,,,,,,http://WIN-
QA2:4884/ObserveIT/Unixcommandsviewer.aspx?SessionID=facaec13-483d-476e-b825-
859f5d88f9ac&DisplayOnAir=false&lang=en,/bin/ps,ps -aux ,

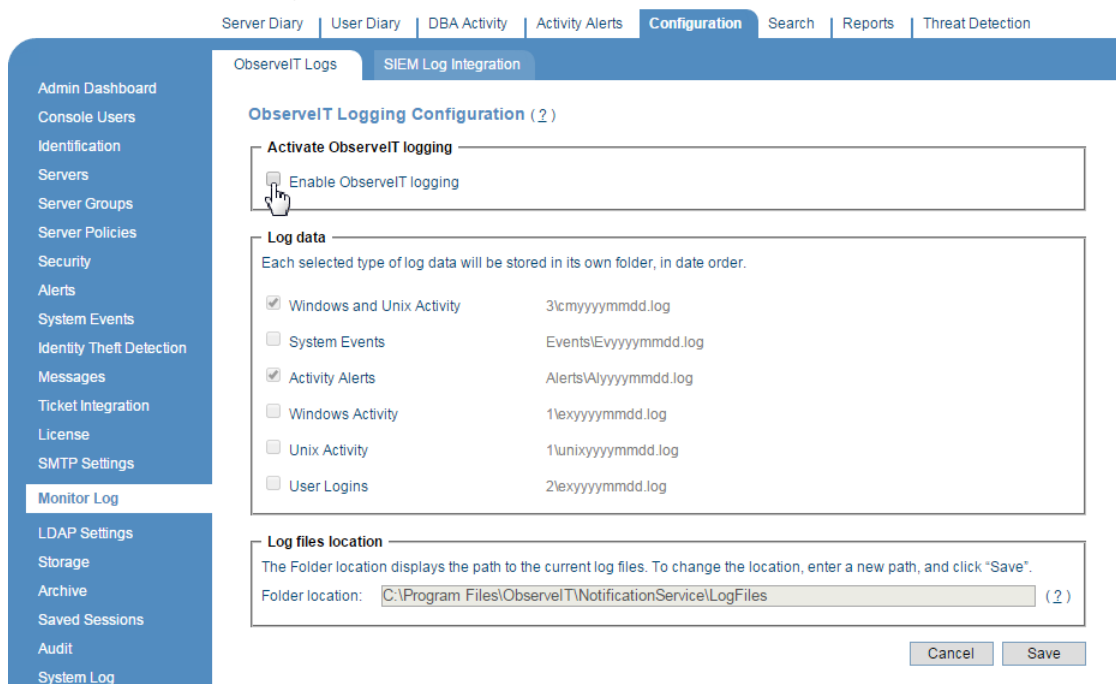
```

Enabling Monitoring of ObserveIT Log Files

To enable the monitoring of ObserveIT log files

- 1) Navigate to **Configuration > Monitor Logs**.

2) Click the **ObserveIT Logs** tab.



3) Select the **Enable ObserveIT logging** check box.

Note: By default, the monitoring of logs is disabled. You cannot enable both ObserveIT logging and SIEM logging simultaneously, since this might cause serious performance issues.

4) In the **Log data** section, select the types of data you want to monitor:

- Windows and Unix Activity
- Activity Alerts
- Windows Activity
- Unix Activity
- User Logins

5) In the **Folder location** field, accept the default location or specify a new path to the monitor log files.

6) Click **Save** to save the settings.

After a few minutes, the log files will be generated. Each day new log files are created.

Note the following:

- Currently, there is no automatic mechanism to delete older log files; you must manually and periodically delete them when they are no longer current. However, you can schedule an automated script that will delete them for you automatically.
- Log files have no operational dependency on the functionality of ObserveIT; therefore, you can delete older log files without losing any information.

To disable the monitoring of the log files

- Clear the **Enable ObserveIT logging** check box, and click **Save**.

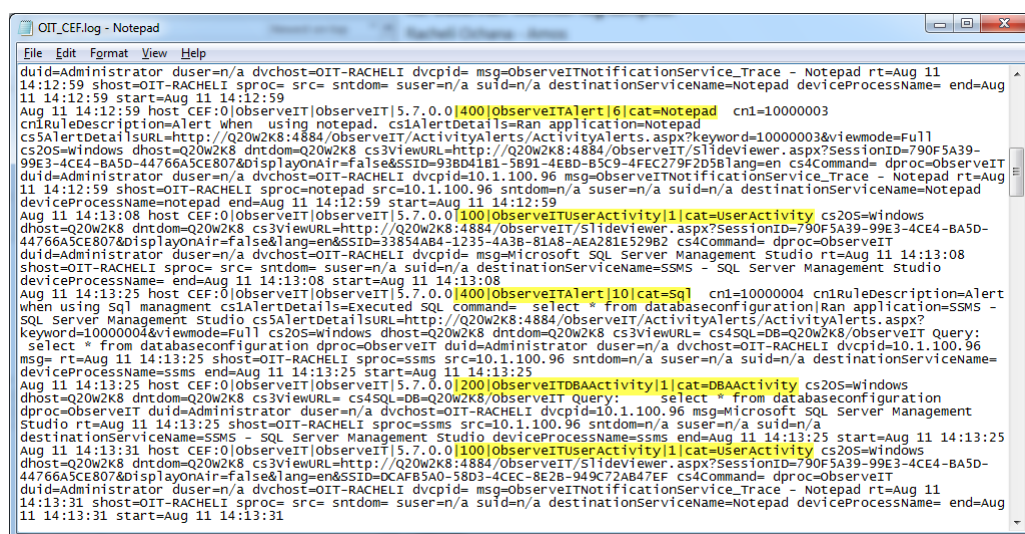
Integrating Logs into SIEM Systems

ObserveIT can be integrated into your existing SIEM monitoring software to enhance real-time alerting and reporting capabilities. Integration support is provided with the HP ArcSight SIEM product by enabling the export of ObserveIT log data to ArcSight CEF format. All log files from ObserveIT user activities, DBA activity, activity alerts, and system events, can be exported and integrated in the SIEM monitoring software. SIEM integration will parse these files based upon text strings that appear inside the log.

Important: For instructions on how to integrate ObserveIT log data into the HP ArcSight SIEM product by using the CEF open log management standard, see [Integrating ObserveIT with HP Arcsight CEF](#).

Log files must be located in a library to which the ObserveIT Notification Service user has write permissions. By default, the log file location is C:\Program Files (x86)\ObserveIT\NotificationService\LogFiles\ArcSight.

The default log file name is OIT_CEF.log. Following is an example of an OIT_CEF.log file showing user activity, DBA activity, and alerts activity data.



```

OIT_CEF.log - Notepad
File Edit Format View Help
duid=Administrator duser=n/a dvchost=OIT-RACHELI dvcpid= msg=ObserveITNotificationService_Trace - Notepad rt=Aug 11
14:12:59 shost=OIT-RACHELI sproc= src= sntdom= suser=n/a suid=n/a destinationServiceName=Notepad deviceProcessName= end=Aug
11 14:12:59 start=Aug 11 14:12:59
Aug 11 14:12:59 host CEF:0|ObserveIT|ObserveIT|5.7.0.0|400|ObserveITAlert|6|cat=Notepad cn1=10000003
cn1RuleDescription=Alert when using notepad. cs1AlertDetails=Run application=Notepad
cs5AlertDetailsURL=http://Q20w2k8:4884/ObserveIT/ActivityAlerts/ActivityAlerts.aspx?keyword=10000003&viewmode=Full
cs205=Windows dhost=Q20w2k8 dntdom=Q20w2k8 cs3viewURL=http://Q20w2k8:4884/ObserveIT/SlideViewer.aspx?sessionId=790F5A39-99E3-4CE4-BA5D-44766A5CE807&displayOnAir=false&SSID=93BD4181-5891-AE8D-B5C9-4FEC279F2D58lang=en cs4Command= dproc=ObserveIT
duid=Administrator duser=n/a dvchost=OIT-RACHELI dvcpid=10.1.100.96 msg=ObserveITNotificationService_Trace - Notepad rt=Aug
11 14:12:59 shost=OIT-RACHELI sproc=notepad src=10.1.100.96 sntdom=n/a suser=n/a suid=n/a destinationServiceName=Notepad
deviceProcessName=notepad end=Aug 11 14:12:59 start=Aug 11 14:12:59
Aug 11 14:13:08 host CEF:0|ObserveIT|ObserveIT|5.7.0.0|100|ObserveITUserActivity|1|cat=UserActivity cs205=Windows
dhost=Q20w2k8 dntdom=Q20w2k8 cs3viewURL=http://Q20w2k8:4884/ObserveIT/SlideViewer.aspx?sessionId=790F5A39-99E3-4CE4-BA5D-
44766A5CE807&displayOnAir=false&SSID=33854A84-1235-4A3B-81A8-AEA281E529B2 cs4Command= dproc=ObserveIT
duid=Administrator duser=n/a dvchost=OIT-RACHELI dvcpid= msg=Microsoft SQL Server Management Studio rt=Aug 11 14:13:08
shost=OIT-RACHELI sproc= src= sntdom= suser=n/a suid=n/a destinationServiceName=SSMS - SQL Server Management Studio
deviceProcessName= end=Aug 11 14:13:08 start=Aug 11 14:13:08
Aug 11 14:13:25 host CEF:0|ObserveIT|ObserveIT|5.7.0.0|400|ObserveITAlert|10|cat=Sql cn1=10000004 cn1RuleDescription=Alert
when using sql management cs5AlertDetails=Executed SQL command= select * from databaseconfiguration[Ran application=SSMS -
SQL Server Management Studio cs4AlertDetailsURL=http://Q20w2k8:4884/ObserveIT/ActivityAlerts/ActivityAlerts.aspx?
keyword=10000004&viewmode=Full cs205=Windows dhost=Q20w2k8 dntdom=Q20w2k8 cs3viewURL= cs4SQL=QB=Q20w2k8/ObserveIT Query:
select * from databaseconfiguration dproc=ObserveIT duid=Administrator duser=n/a dvchost=OIT-RACHELI dvcpid=10.1.100.96
msg= rt=Aug 11 14:13:25 shost=OIT-RACHELI sproc=ssms src=10.1.100.96 sntdom=n/a suser=n/a suid=n/a destinationServiceName=
deviceProcessName=ssms end=Aug 11 14:13:25 start=Aug 11 14:13:25
Aug 11 14:13:25 host CEF:0|ObserveIT|ObserveIT|5.7.0.0|200|ObserveITDBAActivity|1|cat=DBAActivity cs205=Windows
dhost=Q20w2k8 dntdom=Q20w2k8 cs3viewURL= cs4SQL=QB=Q20w2k8/ObserveIT Query: select * from databaseconfiguration
dproc=ObserveIT duid=Administrator duser=n/a dvchost=OIT-RACHELI dvcpid=10.1.100.96 msg=Microsoft SQL Server Management
Studio rt=Aug 11 14:13:25 shost=OIT-RACHELI sproc=ssms src=10.1.100.96 sntdom=n/a suser=n/a suid=n/a
destinationServiceName=SSMS - SQL Server Management Studio deviceProcessName=ssms end=Aug 11 14:13:25 start=Aug 11 14:13:25
Aug 11 14:13:31 host CEF:0|ObserveIT|ObserveIT|5.7.0.0|100|ObserveITUserActivity|1|cat=UserActivity cs205=Windows
dhost=Q20w2k8 dntdom=Q20w2k8 cs3viewURL=http://Q20w2k8:4884/ObserveIT/SlideViewer.aspx?sessionId=790F5A39-99E3-4CE4-BA5D-
44766A5CE807&displayOnAir=false&SSID=DCAF5A0-58D3-4CEC-8E2B-949C72AB47EF cs4Command= dproc=ObserveIT
duid=Administrator duser=n/a dvchost=OIT-RACHELI dvcpid= msg=ObserveITNotificationService_Trace - Notepad rt=Aug 11
14:13:31 shost=OIT-RACHELI sproc= src= sntdom= suser=n/a suid=n/a destinationServiceName=Notepad deviceProcessName= end=Aug
11 14:13:31 start=Aug 11 14:13:31
  
```

In the CEF header, each data type is identified by a unique ID:

- User activity = 100
- DBA activity = 200
- System events = 300
- Alerts activity = 400

Alerts are identified by their severity level:

- High = 10
- Medium = 8
- Low = 6

Configuring SIEM Log Integration

The following procedure describes how to configure SIEM log integration, including:

- Activating SIEM log integration and selecting the log data types.
- Specifying the log file location and log file name.
- Scheduling a log file cleanup.

Note: By default, SIEM log integration is disabled. You cannot enable both ObserveIT logging and SIEM logging simultaneously, since this might cause serious performance issues.

To configure SIEM log integration

- 1) Navigate to **Configuration > Monitor Logs**.
- 2) Click the **SIEM Log Integration** tab.

The screenshot displays the ObserveIT Configuration interface. The top navigation bar includes tabs for Server Diary, User Diary, DBA Activity, Activity Alerts, Configuration, Search, Reports, and Threat Detection. The left sidebar lists various system components, with 'Monitor Log' selected. The main content area is titled 'SIEM Log Integration (2)' and contains three sections: 'Activate SIEM log integration' with a checked 'Enable export to ArcSight format' checkbox; 'Log data' with checkboxes for 'Windows and Unix Activity' (checked), 'Activity Alerts' (checked), 'DBA Activity' (unchecked), and 'System Events' (unchecked); and 'Log file properties' with a text box for 'Folder location' (C:\Program Files (x86)\ObserveIT\NotificationService\LogFiles\ArcSight) and a text box for 'File name' (OIT_CEF.log). Below these is a 'Log file cleanup' section with radio buttons for 'Run daily at' (08:00:00) and 'Run every' (1 Hours). 'Cancel' and 'Save' buttons are at the bottom right.

- 3) Select the **Enable export to ArcSight format** check box.

Note: Integration is currently provided by default with the HP ArcSight SIEM product.

4) In the **Log data** section, select at least one of the following data types for monitoring:

- Windows and Unix Activity - selected by default.
- Activity Alerts - selected by default.
- DBA Activity
- System Events

All selected log type data will be stored in one file; by default, `OIT_CEF.log`.

5) In the **Log file properties** section:

1. In the **Folder location** field, accept the default log file location `C:\Program Files (x86)\ObserveIT\NotificationService\LogFiles\ArcSight` or specify a new path to the monitor log files. When changing the default log folder location, new session data will be stored in the new path; existing data will remain in the old location.

Note: The user account used by the ObserveIT Notification Service must have read and write permissions for the path. If the user account does not have sufficient permissions to create the directory or write to the log file, a system event is generated. In addition, the log file size is limited to a predefined size; if the file size exceeds the maximum defined size, a system event will be generated. For further details, see [System Events](#).

2. In the **File name** field, use the default log file name `OIT_CEF.log` or specify a new one.

6) In the **Log file cleanup** section, schedule the frequency for clearing the log file:

- Select **Run daily at**, and specify the required time of day for the daily cleanup.

Or

Select **Run every**, and specify the required number of days, hours, or minutes for the cleanup.

7) Click **Save** to save the settings.

After a few minutes, the log file will be generated. A new log file will be created according to the scheduled cleanup frequency.

LDAP Settings Configuration

When deployed in a workgroup installation scenario, ObserveIT Console Users are created locally in the ObserveIT Web Console. This means that you need to manually create a Console User for each user that requires access to the ObserveIT Web Console. In addition, when using ObserveIT's Identification Services, users logging on to the monitored servers or workstations with generic-type user accounts, such as the built-in Administrator, will be forced to provide secondary credentials that will be used to identify them. In this scenario, the ObserveIT auditor will know who really used the Administrator account. Similar to Console Users, when deployed in a workgroup installation scenario, local ObserveIT users must be created in the Web Console, and these credentials must be provided to the users logging on to the monitored computers, in order for them to successfully identify themselves with the ObserveIT Identification Services.

ObserveIT allows you to create a connection between the ObserveIT Application and Web Console server components and an external LDAP server, such as a Microsoft-based Active Directory Domain Controller. This connection is an LDAP, read-only connection, in which the ObserveIT server components query the LDAP server for log on information. This enables you to utilize the user accounts and (in some cases) group accounts from within the Active Directory domain, to obtain access to the ObserveIT Web Console and provide users with the necessary credentials for the ObserveIT Identification Services.

- If the server on which the ObserveIT Application server is installed is a member of an Active Directory domain, that Active Directory domain will be automatically added to the list of LDAP Targets, and will be configured as an "Automatic"-type LDAP Target. This will enable the usage of Active Directory users and groups from all domains in the Active Directory forests that are connected to the current forest. For further details, see [Automatic LDAP Targets](#).

Note: ObserveIT easily integrates with your Active Directory forest, enabling you to use user and group objects from any domain in the forest in which the ObserveIT server-side components are installed, and in which the ObserveIT Agents are deployed (if different). Cross forest trusts can also be used. Although using groups from Active directory domains is possible with any group scope (domain local, global, or universal), it is recommended that you follow Microsoft's best practices on group object usage. For further details, refer to [Active Directory Best Practices](#).

- If the server on which the ObserveIT Application server is installed is not a member of any Active Directory domain, you can manually add LDAP Targets, and these will be configured as "Manual"-type LDAP Targets. This will enable the usage of Active Directory users; however, you cannot use groups from that domain. To allow ObserveIT to use Windows Authentication against an Active Directory target, you must identify the Domain, User Name, and Password to be used to access that domain.

For further details, see [Console Users](#) and [Configuring Active Directory Groups](#).

Note: The ObserveIT Web Console Server must be able to communicate through LDAP traffic with at least one of the domain controllers in the target Active Directory domain. LDAP traffic uses TCP port 389 in most cases. If a Firewall exists between the ObserveIT Web Console Server and that domain controller, you will need to configure the Firewall to properly allow LDAP traffic to and from that domain controller. Consult with your Firewall vendor or manual to learn how to properly configure your Firewall.

Server Diary | User Diary | DBA Activity | Activity Alerts | **Configuration** | Search | Reports | Threat Detection

Admin Dashboard
Console Users
Identification
Servers
Server Groups
Server Policies
Security
Alerts
System Events
Identity Theft Detection
Messages
Ticket Integration
License
SMTP Settings
Monitor Log
LDAP Settings
Storage
Archive
Saved Sessions
Audit
System Log

Latest Sessions

OIT-LILI	Admini...
OIT-GUYG	UserNa...
WIN-DBG	UserNa...
OIT-NAT	UserNa...
D11W3SS-1	UserNa...
c58-32-14	UserNa...
D17W6S8-2	Admini...
aiX7-dv1	UserNa...

LDAP Settings

Authentication Configuration

Automatic LDAP Target

Note: Clicking the "Detect Domain Controller" button will first detect whether the ObserveIT Application Server belongs to an Active Directory domain. If true, an automatic-type LDAP path will be added to the LDAP list below. Only automatic-type ("Auto") domains can be used for Active Directory Groups.

Detect Domain Membership
Synchronize LDAP Groups

Manual LDAP Target

Manual LDAP targets can be used to authenticate users for 2 purposes: Console Users and Identification Services.

Type the correct LDAP path by using the following example:

LDAP://Domain_Controller_Name_or_IP/DC=Domain_Name.DC=Suffix
(for example, if your Domain Controller name is OBS-DC1, and your domain name is OBSERVEIT-SYS.LOCAL, then use the following LDAP path: LDAP://OBS-DC1/DC=OBSERVEIT-SYS.DC=LOCAL)

Note: If no name resolution is possible, you might need to enter the Domain Controller IP address instead.

LDAP Path
(Secure LDAP)

Enter user credentials to verify the LDAP path

User Name
Password

Add & Verify

LDAP Properties

LDAP mail field name
Update

LDAP Targets List

**You are using secure LDAP.*

LDAP Path	Domain Name	User Name	Alias	Type	Created Date	
LDAP://DC=OBSERV...	OBSERVEIT-SYS.LOCAL	guy	OBSERVEIT-SYS	Auto	9/9/2012	Delete

Note: ObserveIT also supports secured SSL communication to Active Directory via LDAP. When LDAPS is configured, all communication via Active Directory will be encrypted. An indication will be displayed in the LDAP Settings page (as shown in the above screenshot).

After an LDAP connection is properly established, the domain appears in two locations:

- **Configuration > Console Users** page, where you can create and configure additional ObserveIT Console Users that can administer ObserveIT, or that can be used to view recorded sessions. For further details, see [Console Users](#).
- **Configuration > Identification** page, where you can configure users that are required to identify themselves with a secondary ObserveIT logon whenever they log on to any ObserveIT-monitored server. For further details, see [Configuring Active Directory Identification Targets](#).

From the **Configuration > LDAP Settings** page of the Web Console, you can configure automatic and manual LDAP targets, and change the default LDAP email field name, if required.

See the following topics:

- [Automatic LDAP Targets and Adding Domains](#)
- [Adding Manual LDAP Targets](#)
- [Deleting LDAP Targets](#)
- [Changing the Default LDAP Email Field Name](#)

Automatic LDAP Targets and Adding Domains

If the server on which the ObserveIT Application server is installed is a member of an Active Directory domain, that Active Directory domain will be automatically added to the list of LDAP Targets, and will be configured as an "Automatic"-type LDAP Target.

There are two scenarios:

- 1) The server was already a member of the domain when the ObserveIT setup program was executed.

When the ObserveIT setup program determines that the server on which the ObserveIT Application server is installed is a member of an Active Directory domain, the setup program automatically adds that domain to the list of LDAP Targets. No further user action is required. The domain will be listed in the LDAP Target List as an "auto"-type LDAP Target.

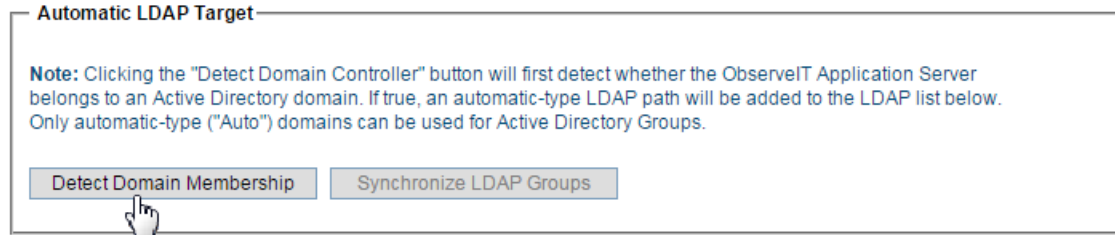
- 2) The server is made a member of the domain after the ObserveIT installation.

If, during the ObserveIT installation, the server on which the ObserveIT Application Server is installed is not a member of an Active Directory domain, the setup program will perform any changes to the LDAP Target List. However, it may be possible that a change was made after the ObserveIT installation, and one on which the ObserveIT Application server is installed as a member of a domain. In this case, you can add that domain to the list of LDAP Targets.

To add a domain to the list of LDAP Targets

- 1) Make sure that the server on which the ObserveIT Application server is installed is a member of a domain.
- 2) Navigate to **Configuration > LDAP Settings**.

- 3) In the **Automatic LDAP Target** section, click the **Detect Domain Membership** button.



If the Domain path and credentials are valid, the connection will be added to the LDAP Target List. The LDAP Target type will be set to "Auto".

LDAP Targets List

LDAP Path	Domain Name	User Name	Alias	Type	Created Date
LDAP://DC=OIT-DEMO,DC=LOCAL	OIT-DEMO.LOCAL			Auto	4/4/2014 Delete

Note: The **Detect Domain Membership** button is grayed out and cannot be used again, because the server can be a member of only one domain.

- 4) Click the **Synchronize LDAP Groups** to update new group names in Active Directory. This is only relevant if any Active Directory Groups names were changed in the ObserveIT configuration (for example, when including/excluding groups from being recorded).

After the LDAP connection is properly established, you can start working with Active Directory-based Console Users. Note that for auto-type LDAP Targets, Active Directory-based users and groups can be used.

Adding Manual LDAP Targets

If the server on which the ObserveIT Application server is installed is not a member of any Active Directory domain, you can manually add LDAP Targets.

To add a manual-type LDAP Target

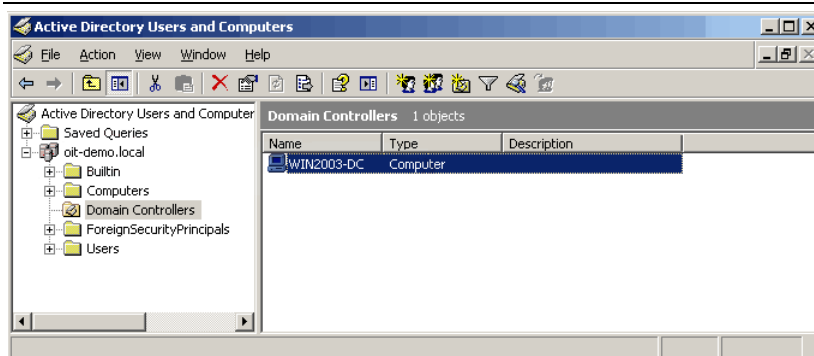
- 1) In the **Manual LDAP Target** section of the **Configuration > LDAP Settings** page, enter an LDAP Path.

Use one of the following options:

LDAP://Domain_Controller_Name/DC=Domain_Name,DC=Suffix

For example: LDAP://WIN2003-DC/DC=OIT-DEMO,DC=LOCAL

Note: The `Domain_Controller_Name` can be either the server's host name, or the server's IP address.



Note: In some cases, you will need to use UPPER CASE letters for the LDAP path.

2) Enter a **User Name** and **Password**.

Note: The required user name should have at least read access rights to the target domain. You do NOT need to use the Administrator account, or a user account that is a member of the Domain Admins group. However, if authentication fails, you could try to use such an account in order to test your connection.

3) Click **Add & Verify**.

Manual LDAP Target

Manual LDAP targets can be used to authenticate users for 2 purposes: Console Users and Identification Services.

Type the correct LDAP path by using the following example:

LDAP://Domain_Controller_Name_or_IP/DC=Domain_Name,DC=Suffix
 (for example, if your Domain Controller name is OBS-DC1, and your domain name is OBSERVEIT-SYS.LOCAL, then use the following LDAP path: LDAP://OBS-DC1/DC=OBSERVEIT-SYS,DC=LOCAL)

Note: If no name resolution is possible, you might need to enter the Domain Controller IP address instead.

LDAP Path

Enter user credentials to verify the LDAP path

User Name

Password

If the Domain path and credentials were valid, the connection will be added to the **LDAP Targets List**, and the LDAP Target type will be set to **Manual**.

Authentication Configuration

Domain named 'OIT-DEMO.LOCAL' successfully added.

Automatic LDAP Target

Note: Clicking on the "Detect Domain Controller" button will first detect if the ObserveIT Application server belongs to an Active Directory domain. If true, an automatic-type LDAP path will be added to the LDAP List below. Only automatic-type ("Auto") domains can be used for Active Directory Groups.

Manual LDAP Target

Manual LDAP targets can be used to authenticate users for 2 purposes: Console Users and Identification Services.

Type in the correct LDAP path by using the following example:

LDAP://Domain_Controller_Name_or_IP/DC=Domain_Name,DC=Suffix
 (for example, if your Domain Controller name is OBS-DC1, and your domain name is OBSERVEIT-SYS.LOCAL, then use the following LDAP path: LDAP://OBS-DC1/DC=OBSERVEIT-SYS,DC=LOCAL)

Note: If no name resolution is possible, you might need to enter the Domain Controller IP address instead.

LDAP Path

Enter user credentials to verify the LDAP path

User Name

Password

LDAP Targets List

LDAP Path	Domain Name	User Name	Alias	Type	Created Date	
LDAP://WIN2003-DC/DC=OIT-DEMO,DC=LOCAL	OIT-DEMO.LOCAL	administrator		Manual	4/4/2014	Delete

After the LDAP connection is properly established, you can start working with Active Directory-based Console Users.

Deleting LDAP Targets

LDAP targets can be deleted if they are no longer needed.

To delete an LDAP target

- 1) In the **LDAP Targets List** section of the **Configuration > LDAP Settings** page, click the **Delete** link next to the relevant LDAP target source.

LDAP Targets List						
LDAP Path	Domain Name	User Name	Alias	Type	Created Date	
LDAP://DC=OBSERVEIT-SYS,DC=LOCAL	OBSERVEIT-SYS.LOCAL	NETWORK SERVICE	OBSERVEIT-SYS	Auto	3/3/2014	Delete

A message is displayed, warning you that you are about to delete an LDAP Source.

Important: If you try to delete an LDAP Source when there are Forced-Identification Users and/or Console Users in the system, you will receive an error message. If there are no more LDAP sources, and Identification Services was configured, any user that tries to log on to the ObserveIT-monitored servers will be unable to do so. Deleting the LDAP Source might prevent Forced-Identification Users or Console Users from being able to pass the ObserveIT Identification or log on to the ObserveIT Web Console. To delete such an LDAP source, you must either remove the Forced-Identification Users or Console Users, create a different LDAP Source, or create Local ObserveIT Users instead.

- 2) Click **OK** to proceed.
The LDAP target is deleted.

Changing the Default LDAP Email Field Name

The user's email must be defined in the LDAP mail field name in order for the users to receive email notifications, and especially notifications about user login events (see [Configuring Identity Theft Settings](#)).

The default LDAP mail field name is "mail", but you can change this to a more specific user name, if required.

To change the default LDAP field name for email notifications

- 1) In the **LDAP Properties** section of the **Configuration > LDAP Settings** page, enter the LDAP email field name as specified in your LDAP server.

Note that the default is "mail".

LDAP Properties	
LDAP mail field name	mail Update

- 2) Click **Update** to save the new name.

Recording Metadata Information

In addition to visually recording user actions on monitored servers, ObserveIT records important information about what is seen on the screen, which applications are currently used, what actions the user has performed, the date and time of the action, and more. This information, which is called "metadata", is stored in ObserveIT's database, which is located on a central SQL Server. Because metadata is centrally stored and indexed, it can be used to easily search throughout recorded sessions, and provide a textual breakdown of each user session.

Although ObserveIT's main feature is its ability to visually record user sessions, in some cases, ObserveIT administrators will configure ObserveIT to record only metadata about specific applications that are accessed on specific servers. While this will reduce the visual auditing experience for the user session, this recorded metadata is a very important aspect of the auditing experience and capabilities. Because this metadata describes what is seen on the screen, you can perform very powerful searches across your entire enterprise. Although no visual trace will be available when selecting this option, it will still provide far more auditing capabilities than when compared to a server with no ObserveIT Agent installed.

There are two ways to record metadata information:

- Metadata only, without any graphical screenshots being recorded
- Record metadata for specific applications

Record Metadata Only

To record metadata only without any graphical screenshots, you must use the **Default Metadata Only Policy**, a preconfigured policy that records only metadata. By default, this policy is not linked to any Server. If you link that policy to one or more servers, these servers will only record metadata information.

Record Metadata for Specific Applications

You can create a new Server Policy that has specific applications excluded in the recording policy, or edit an existing policy to match your needs. You can also manually edit a specific server's configuration.

Note: By default, ObserveIT's Default Configuration Template is configured to record all applications AND the associated metadata. Therefore, in a default configuration scenario, there is no need to make any changes in order to record the metadata information.

For example, you might decide that, in a particular scenario, you only want to record these administrative-related applications:

- CMD.exe
- Notepad.exe
- MMC.exe
- Regedit.exe
- Mstsc.exe

To change either the particular Server's Configuration Policy or the Server Configuration Policy that affects that server

- 1) Navigate to **Configuration > Server Policies**.
- 2) Click the relevant policy to open its configuration page.

- 3) In the **Application Recording Policy** section, select the **Record only the following applications** option.
- 4) From the **Applications** drop-down list, select and add the specific applications.

After making the changes, the relevant screen section should look like:

- 5) When you have finished configuring the server, click **Save**.
- 6) Read the warning message, and if you are satisfied with your changes, click **OK** to proceed, or **Cancel** to discard your changes.

Note: As noted above in the first option, for other scenarios you can configure the **Record Metadata Only** setting to change the way the ObserveIT Server records applications. By using this setting, the ObserveIT Server will only record metadata for the applications accessed during a user's session. No graphic information will ever be recorded.

After making the necessary configuration changes, you will be able to replay and view the graphical recorded data for those applications, but will only have textual metadata information about any other application that was accessed on that server. These applications will be clearly identified by the  icon in the **Activities View** of the **Server Diary** or **User Diary**.

When viewing the recording, only the recorded applications will be visible.

Managing ObserveIT Storage

ObserveIT stores captured data and configuration settings inside Microsoft SQL Server databases. Storage includes configuration data, textual audit metadata and the actual screenshots for video replay, captured by the ObserveIT Agents.

During installation, the ObserveIT Database Server creates the following databases on the SQL Server:

- ObserveIT
- ObserveIT_Data
- ObserveIT_Archive_1
- ObserveIT_Archive_template

By default, the ObserveIT screenshots are stored in the SQL Server ObserveIT_Data database. However, if required, screen images data can be stored in the file system instead of the SQL database. The file system storage method is most commonly used for large deployments, or when the SQL Server database has performance issues. Recorded visual images can be stored either on the local hard drive of the ObserveIT Application Server, or on a file share in the network. For further details, see [Storing the ObserveIT Screenshots \(in the Installation Guide\)](#).

Note: When using file system storage, there is still a need to maintain the SQL Server database in order to store the recorded textual metadata, image pointers, and the ObserveIT configuration settings.

Configuring Database Storage

The SQL Server database is used to store configuration data, textual audit metadata and possibly (unless the file system is used) the screenshots captured by the ObserveIT Agents for video replay. The database continuously grows as more sessions are recorded. To prevent data loss as the database becomes full, ObserveIT enables you to configure additional storage space. You can configure a threshold (as a percentage of allocated disk space) specifying the maximum disk space that is allocated for the database. A system event is generated when the database storage threshold (%) reaches its configured limit, alerting you to configure additional storage space by updating the specified threshold or by running the archive process. For details about configuring ObserveIT archive storage, see [Archiving Information](#).

Configuring File System Storage

If you are using the file system for screen capture storage, you must have enough space on the disks that store the folder in which you want to store all the recorded visual images. When using a single file system, if the disk is full, the system stops recording, and you will need to remove data from the disk in order to continue recording. To extend and manage your file system storage without disrupting recording, ObserveIT enables you to configure multiple file systems. This means that when file system disks become full, you can define new file system locations to hold the ObserveIT screen capture data. You can define multiple file system locations for each database. Note that you will still be able to access the "old" file system locations in order to replay their recorded sessions.

By configuring a threshold for a system event to occur just before the file system reaches its maximum allocated storage, you can be alerted to configure additional storage before you experience screen capture data loss. The previous file system location will still be fully available for playback even while new screen capture data will be written to the new location.

Note: ObserveIT automatically manages the directory where you specify that screenshot data should be stored, including an auto-generated subdirectory tree per date and per session. The folder structure is automatically created so that the file system location (with the screen captures) appears as a subfolder to the database (which contains the related metadata). In this way, all relevant session data is kept together. Since you can define multiple file system locations for each database, you can also have a number of databases each with several file system locations.

The following topics in this section describe how to manage the ObserveIT database and file system storage, including:

- Viewing information about the current ObserveIT SQL database.
- Viewing session information on the SQL Servers that are recorded in the database.
- Identifying if the system is using the SQL database or the file system for screen capture storage.
- Setting thresholds for system alerts if the database or the file system reaches its maximum allocated storage.
- Creating new file system locations for screen capture data.
- Viewing previous file system locations in order to be able to replay recorded sessions.

See:

- [Viewing Database Information](#)
- [Configuring Screen Capture Data Storage](#)
- [Viewing Servers Database Information](#)

Viewing Database Information

By default, ObserveIT stores all the captured data (including screen images) and configuration settings inside Microsoft SQL Server databases. However, in many deployments, the file system is the preferred method for storing screen image data instead of the SQL database. Even when the file system is used for storing image data, a functional SQL Server database is still required for storing all the recorded metadata, image pointers, and configuration settings.

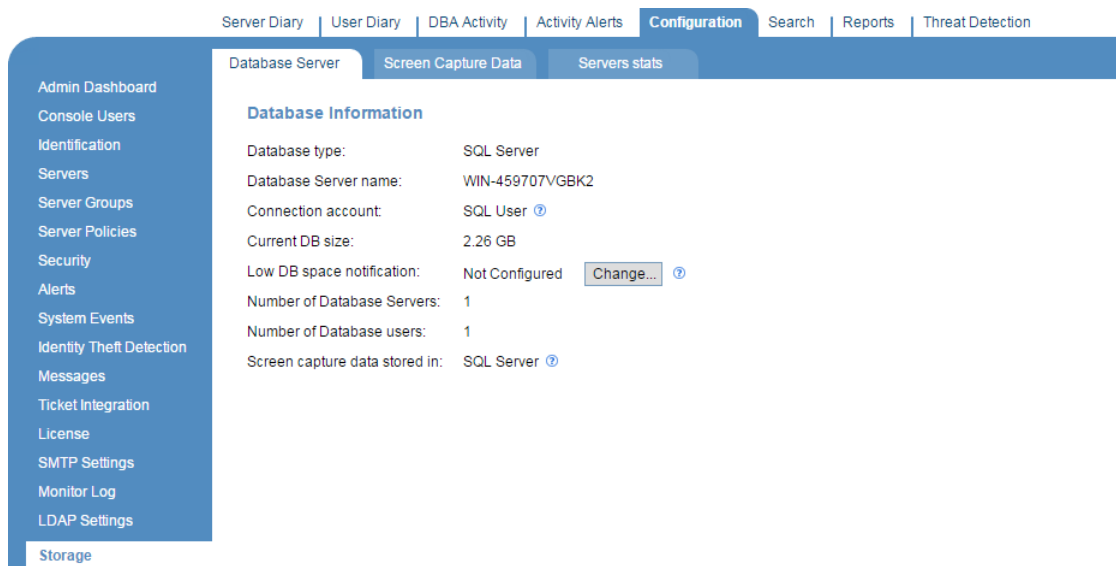
It is important to properly monitor the database site and its health. You can use any number of well-known procedures and monitoring tools to do this; however, it is beyond the scope of this document to deal with SQL management and monitoring best practices and tools.

The ObserveIT Web Console provides important information about the current status of the ObserveIT database server, including identifying whether the system is using the SQL database or the file system for screen capture storage.

To view information about the currently configured database storage

- 1) Navigate to **Configuration > Storage**.

2) Click the **Database Server** tab.



3) View the following information:

- Database type: SQL Server.
- Name of database server: The name of the server hosting the SQL Server.
- Connection account: SQL Server or Windows Authentication.
- Current DB size: The actual volume of data currently in the database (GB).

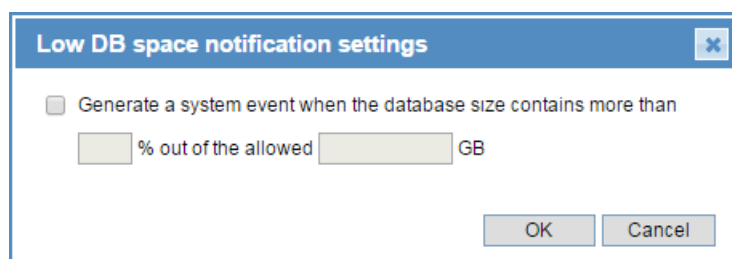
Note: If configured, **Maximum DB Size** shows the maximum space available for the database (GB) and the currently available percentage of free space.

- Low DB space notification: "Not configured"/threshold showing the maximum disk space allocated for the database.

Note that the threshold applies to *all* the databases. If required, you can release disk space by running the archive process (see [Archiving Information](#)).

To specify a different threshold, click the **Change** button. In the dialog box that opens, specify a new threshold for maximum allocated disk space, and click **OK**.

A system event will be generated when the database size contains more than ? % of the allowed ? GB.



To disable the system event, clear the check box **Generate a system event when the database size contains more than**, and click **OK**.

- Number of servers in DB: The total number of servers that are recorded in this database. This includes old and inactive servers that have been uninstalled, as ObserveIT never removes server data even after becoming inactive unless you archive or delete that information from the active database.

- Number of users in DB: The total number of users that are recorded in this database.
- Screen capture data stored in: SQL Server or File System.

Configuring Screen Capture Data Storage

By default, the ObserveIT screenshots are stored in the SQL Server database. However, in many deployments, the file system may be the preferred method for storing screen image data instead of the SQL Server database. When using the file system, the recorded visual images can be stored either on the local hard drive of the ObserveIT Application Server, or on a file share in the network.

In the **Screen Capture Data** tab of the **Configuration > Storage** page, you can:

- View active screen capture data storage information when using the SQL Server database.
- View and configure active screen capture data storage when using the file system or a network share.
- Create new file system locations for screen capture data.
- View local/network paths which were previously used by the system to store screen capture data.

Note that the contents of the **Screen Capture Data** tab differ, depending on whether the system is using the SQL Server database or the file system for storing screen captures (identified in the [Database Server](#) tab).

Viewing Screen Capture Data Storage when using the SQL Server Database

When the SQL Server database is used for storing screen image data, you can view the information about the currently active screen capture data storage.

To view screen capture data stored in the SQL Server database

- 1) Navigate to **Configuration > Storage**.
- 2) Click the **Screen Capture Data** tab.

The screenshot displays the ObserveIT web interface. The top navigation bar includes links for Server Diary, User Diary, DBA Activity, Activity Alerts, Configuration, Search, Reports, and Threat Detection. The left sidebar lists various system components like Admin Dashboard, Console Users, Identification, Servers, Server Groups, Server Policies, Security, Alerts, System Events, Identity Theft Detection, Messages, Ticket Integration, License, SMTP Settings, Monitor Log, and LDAP Settings. The 'Storage' option is highlighted in the sidebar. The main content area is titled 'Screen Capture Data Storage' and contains a box labeled 'Active Screen Capture Data Storage' with the following details:

Screen capture data stored in:	SQL Server ⓘ
Database Server:	WIN-459707VGBK2
Database name:	ObserveIT_Data
Database path:	c:\program files\microsoft sql server\mssql10_50.mssqlserver\mssql\data\ObserveIT_Data
Date range of included sessions:	1/6/2015 4:36 PM - 1/11/2015 12:29 PM
Current screen capture storage:	1.00 GB (278 Slides)

The following information is displayed:

- Screen capture data stored in: SQL Server
- Database server: Name of the server hosting the SQL Server.
- Database name: Name of the database storing the screen capture images.

- Database path: Path to the location of the database.
- Date range of included sessions: First date (and time) to last date (and time).
- Current screen capture storage: Size of storage for current screen capture session (GB) and number of slides.

Configuring Screen Capture Data Storage when using the File System/Network Share

As data quickly accumulates both in file numbers and overall data size, it is essential that you have enough storage space on the disks that store the folder in which you want to store all the recorded visual images. When only a single file system path location is defined, once the disk is full, the system stops recording, and you need to remove data from the disk in order to continue recording. From the **Screen Capture Data** tab, you can configure multiple file systems, which enables you to extend and manage your file system storage without disrupting recording.

Note: If required, you can release some disk space by running the archive process (see [Archiving Information](#)).

To configure screen capture data storage using the File System/Network Share

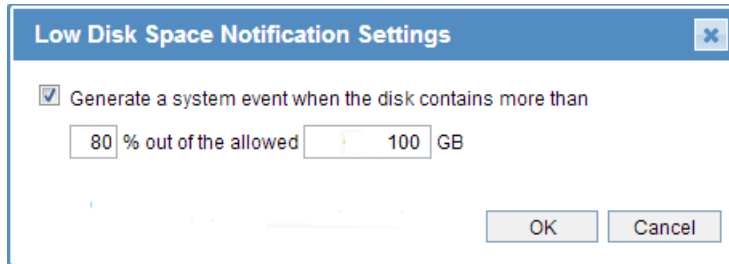
- 1) In the **Active Screen Capture Data Storage** section of the **Screen Capture Data** tab, in addition to viewing specific information about the active screen capture data storage, you can:
 1. Define a threshold that will trigger a system event if the file system reaches its maximum allocated storage.
 2. Create new file system locations for screen capture data.
 3. View previous file system locations in order to replay recorded sessions.

The following information is displayed about the currently active screen capture data storage:

- Screen capture data stored in: File System
- File system location: File system path (local on server, or network share)
- Date range of included sessions: First date (and time) to last date (and time)
- Current screen capture storage: Size of storage for current screen capture session (GB) and number of slides
- Low disk space notification: "Not Configured"/threshold showing the maximum actual disk space allocated for the screen capture data

To configure a threshold for a system event if the file system reaches its maximum allocated storage

- 1) In the **Screen Capture Data** tab, click the **Change** button (next to **Low disk space notification**) to open a dialog box that lets you configure/specify a different threshold.



- 2) Select the check box **Generate a system event when the disk contains more than**.

Note: To clear a system event, clear this check box, and click **OK**.

- 3) Specify the maximum disk space that you want to allocate for the screen capture data, by entering values in the % and **GB** fields.
- 4) Click **OK**.

A system event will be generated when the disk reaches the specified values. If the event is ignored, after the allocated disk space is reached, you may experience screen capture data loss.

Note: A message will be sent to the user after SMTP settings are configured and a recipient email address is configured (see [Configuring Email Notification Settings for Events](#)).

Creating a New File System Location for Screen Capture Data

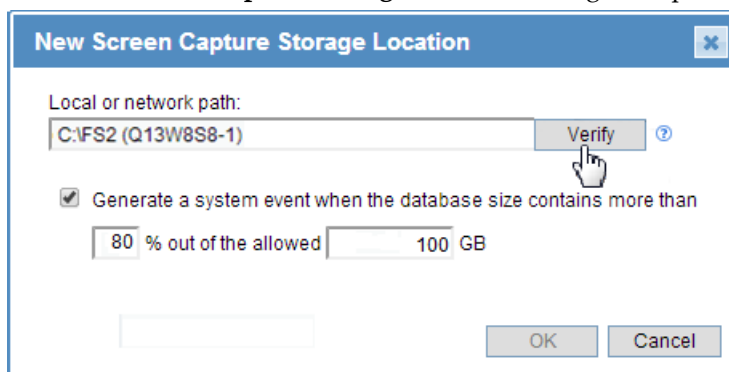
Before the current file system location reaches its maximum allocated storage, you can select a new file system location to hold the ObserveIT screen capture data.

Note: The previous location will still be fully available for playback even while new screen capture data will be written to the new location.

To create a new file system location for screen capture data

- 1) In the **Screen Capture Data** tab, click the **New Screen Capture Storage Location** button.

The **New Screen Capture Storage Location** dialog box opens.



- 2) Enter a new file system path, and click **Verify**.

The system checks that the new path exists, has not already been used, and is not a subfolder of an already used path. The system also checks that the user account used by the ObserveIT application pool on the Web console has read and write permissions for the specified path.

3) Click **OK**.

Note: If required, you can also configure a threshold setting for the new path that will generate a system event.

Before the changes and data are written to the new path, a confirmation dialog box opens:

"You are about to change the screen capture data storage location from <old path> to <new path>. This action cannot be reversed. However, as long as the path to the previous location is still accessible by the system, data in it can be replayed. After you click "Yes", all new session screen capture data will be stored in the new path. Are you sure that you want to proceed?"

4) Click **Yes** to proceed.

Once committed, the active path will change to the new path. The old path will be displayed in the **Additional Screen Capture Data Storage** section with the status "Available".

Important: The folder structure is automatically created so that the file system location (with the screen captures) appears as a subfolder to the database (which contains the related metadata). In this way, all relevant session data is kept together. Since you can define multiple file system locations for each active database, you can also see a number of databases each with several file system locations.

Viewing Additional Screen Capture Data Storage

To view additional screen capture data storage

- 1) In the **Additional Screen Capture Data Storage** section (in the **Screen Capture Data** tab), view the local/network paths which were previously used by the system to store screen capture data. To ensure playback availability, these paths must remain accessible. They appear in the list with the status "Available".
- 2) Select the check box **Show all paths (including empty or unavailable)** to view details of file paths which are currently unavailable for screen playback, or are empty (that is, they do not contain any screen capture data, possibly due to content archiving).

For each file system path, the following information is displayed:

- Path Location: File system path (local on server, or network share)
- Status: "Available", "Empty" or "Unavailable"
- Size (GB): Size of storage for screen capture session (in GB)
- Slides: Number of slides in screen capture session
- Date Added: Date that the file system path was created
- Added By: The user that created the file system path
- Last Session Date: Date of last screen capture

Additional Screen Capture Data Storage							
☒ Show all paths (including empty or unavailable) ?							
Path Location	Status	Size (GB)	Slides	Date added	Added by	Last Session Date	
C:\FS (Q13W8S8-1)	Available	0.01	62	03/20/2014	Installer	03/23/2014	
C:\FS2 (Q13W8S8-1)	Empty	0.00	0	03/23/2014	Admin	N/A	Remove

Note: If the status of a file path entry is "Empty", you can remove it by clicking the **Remove** link next to it.

Viewing Servers Database Information

In the **Servers Stats** tab of the **Configuration > Storage** page, you can view detailed information about sessions that were recorded on the SQL Servers in the database.

To view details about sessions that were recorded on the SQL Servers

- 1) Navigate to **Configuration > Storage**.
- 2) Click the **Servers Stats** tab to view a list of the servers that are recorded in the database.

The screenshot shows the ObserveIT interface. At the top, there are tabs: Server Diary, User Diary, DBA Activity, Activity Alerts, Configuration (selected), Search, Reports, and Threat Detection. Under the Configuration tab, there are sub-tabs: Database Server, Screen Capture Data, and Servers stats (selected). On the left, a sidebar menu lists various sections: Admin Dashboard, Console Users, Identification, Servers, Server Groups, Server Policies, Security, Alerts, System Events, Identity Theft Detection, Messages, Ticket Integration, License, SMTP Settings, Monitor Log, LDAP Settings, and Storage (highlighted). The main content area displays 'Servers Database Information' with a table showing one server entry.

Server Name	Slides	Sessions	First Session	Last Session
W2K8-S8-D02	278	12	1/6/2015	1/11/2015

The following information is displayed for each server in the list:

- Name of the recorded server.
- Size of the server's recorded data (number of slides).
- Total number of sessions in the server.
- Dates of the first and last session recorded for the server.

Note: The date of the first sessions in the database may be later than what you would expect from the database actual age. For example, if the ObserveIT database was installed on the 1st of January 2014, and an archiving job was run on the 1st of October, archiving all sessions older than the past month, the "First Session" parameter will show the 1st of September. To find these sessions, navigate to the **Configuration > Archive > Diary** tab.

Important Notes:

- The more sessions a server has, the more data it uses. Considerations must be taken when dealing with very large database sizes, and proper SQL tuning needs to be performed in order not to reduce the overall server performance.
- Some versions of SQL Express are limited in database size and will only hold a database no larger than 4 GB. When using SQL Express, take that limit into consideration.
- By default, ObserveIT never deletes data from the database, however, you can use the **Archive** tab to remove or archive old server data. See [Archiving Information](#).
- When archiving is used, the database size may not shrink in actual physical size. To reduce the overall size of the database, use proper SQL server maintenance procedures.

Archiving Information

Archiving of data and keeping the database to a manageable size is a concern for all organizations. Storing obsolete and irrelevant data online reduces the overall performance of a database server. To minimize performance problems that are caused by maintaining excess data, you can implement an archiving strategy. By archiving data, you can decrease disk space usage and reduce the maintenance required, for example in defragmentation, backup and restore procedures. From a performance point of view, if a production database or file system storage has obsolete data that is never or rarely used, query execution can be time-consuming because queries also scan obsolete data. To improve query performance, you should move obsolete data from the production database/file system to another archive database/file system.

ObserveIT's database archiving feature provides enhanced database performance by moving obsolete data from the main production database to a secondary archive database. Archiving of data can also be performed on file systems that are used for storing screen capture data. Archiving jobs can be launched manually or can be scheduled for automatic periodic archive rotation.

Note: The archive data can be split into daily transactions, thus enabling an even larger volume of data to be archived.

Before you begin to configure archiving, you should be aware of the following considerations:

- An archive job always uses the most recently created archive database. As soon as the new archive database is created by the SQL Server administrator, ObserveIT will begin using it. The previously used archived database and its session contents will still be accessible for restore and replay.
- If you are using the file system to store your recorded sessions' visual images (see Storing the ObserveIT Screenshots in the Installation Guide), when archiving is configured, a file system will be used to store the images. When images are stored in the database, the database will be used for the archived images. When restoring archived sessions, the images that belong to the sessions will be restored to their original file folder.
- After specific sessions are archived, they will no longer occupy space in the production database/file system. These archived sessions will also no longer appear in the **Server** or **User Diary**, or in the **Search** or **Report** results. The only way to replay the archived sessions will be to use the **Diary** tab of the **Configuration > Archive** page.
- During archiving, the ObserveIT database/file system storage is locked. Although efforts have been made to minimize the lock time, it is recommended that you schedule the archive to be performed when activity on the server is minimal (for example, weekends, nights). It is also recommended to schedule the archive so that each archive does not contain too much data; that is, it is better to schedule a periodic archive, than to archive a whole year at once.

Configuring Database Archive Storage

A new ObserveIT archive database is created when the current "live" database size reaches its maximum allocated storage.

ObserveIT's archive storage feature enables you to:

- View detailed information about the currently active archive database, and the sessions that are stored in it.
- Define a threshold that will trigger a system event if the archive database reaches its maximum allocated storage.

- Create a new archive database if the current archive database size exceeds its maximum allocated storage.
- View previous data storage archive locations.

Configuring File System Archive Storage

When the file system is used to store the screen image data, ObserveIT's file system archive storage feature enables you to:

- View detailed information about the current screen capture archive data storage.
- Define a threshold that will trigger a system event if the specified file system archive file reaches its maximum allocated storage. Note that if the system event is ignored after the maximum allocated storage is reached, you may experience screen capture data loss.
- Define new file system locations in which to store archived screen capture data.

You can define multiple archive file system locations for the currently active archive database. Before the current file system archive file reaches its maximum allocated storage, it is recommended that you create a new file system location in which to store the archived screen capture data. Once committed, the active local or network path to the archive location will change to the new path, and all session screen captures will immediately be archived there. The old path will be displayed in the **Historical Data Storage Locations** section in the **Configuration > Archive > Storage Management** tab.

- View previous data storage archive locations. In the **Historical Data Storage Locations** section, you can see detailed information about local/network paths which were previously used by the system for archiving screen capture data.

Note: When using the file system, the archived screen captures are stored under the current archive database (with the related metadata) under the currently active archive path. For example, if the archive path is "\\ObserveIT_Archive\MAR-17" and the currently active archive database is "ObserveIT_Archive_3", then the screen capture data will be archived under "\\ObserveIT_Archive\MAR-17\ObserveIT_Archive_3". This enables administrators to easily correlate the archive file system data with the relevant archive database (in this example, "ObserveIT_Archive_3").

The following topics in this section describe in detail how to archive ObserveIT information, including:

- [Scheduling an Archive Job](#)
- [Managing the Archive Storage](#)
- [Viewing the Archive Log](#)

Scheduling an Archive Job

Archiving jobs can be launched manually or can be scheduled for automatic periodic archive rotation. By scheduling archiving, you can select a date range for the archived data or an "older than" parameter, and you can control which sessions will be archived, based on specific server or user names, or on specific server groups.

During archiving, the ObserveIT database/file system storage is locked, therefore, it is recommended that you schedule the archive to be performed when activity on the server is minimal (for example, weekends, nights). It is also recommended to schedule the archive so that each archive does not contain too much data; that is, it is better to schedule a periodic archive, than to archive a whole year at once.

Scheduling an archive job is done in the **Schedule Archive** page of the Web Console.

The following steps are required to schedule a job for archiving:

- 1) Enable the schedule status.
- 2) Specify a date range for the archived data.
- 3) Select the archive job frequency.
- 4) Specify the type of data that will be processed by the archive job.
- 5) Select the action to be performed on the job schedule.

Note: You can select to archive the scheduled job data or delete the scheduled data from the database (in order to release space in the archive database). Deleted sessions will no longer be displayed in the **Server/User Diaries**.

- 6) Save the job schedule.

Enabling the Schedule Status

- 1) Navigate to **Configuration > Archive**.
- 2) Click the **Schedule** tab.

The **Schedule Archive** page opens. By default, the schedule status is **Disabled**.

Admin Dashboard
Console Users
Identification
Servers
Server Groups
Server Policies
Security
Alerts
System Events
Identity Theft Detection
Messages
Ticket Integration
License
SMTP Settings
Monitor Log
LDAP Settings
Storage
Archive
Saved Sessions
Audit
System Log

Quick Help
Installation Guide
User Guide
Configuration Guide

Server Diary
User Diary
DBA Activity
Activity Alerts
Configuration
Search
Reports
Threat Detection

Schedule
Storage Management
Log
Diary
Search

Schedule Archive

Save Schedule

Schedule Status and Information

Enabled: ☒

Status: Active

Previous Running Date: -

Next Running Date: 1/1/2015 1:00 PM

Data older than 10/1/2014 12:00 AM will be affected.

Current DB time is: 12/22/2014 3:33:31 PM

Sessions to Archive: 0

Screenshots to Archive: 0

Schedule created on: 12/22/2014 12:50 PM

Date Range for archiving

☒ Older than: 3 Month(s) Data will be added to the current active archive database.

☐ Date Range: Dec 8 2014 Dec 15 2014

Note: Cutoff time is always at midnight.

Schedule

Select frequency.

Rekurs every: Months

Rekurs every: 1 Month(s)

On the 1 Day of Month.

at: 1:00 PM

Data Type

Filter data by the following servers or server groups:

Server: Add

Servers Groups: All Servers Add

Name	Type	Version	Status	Date
☐ All Servers	Group			

Check All - Clear All Remove

Note: Sessions from these servers or server groups will be archived.

Filter data by the following users:

Note: If no user is entered, the action will be performed on all users.

User: DomainUser Add

DomainUser

Check All - Clear All Remove

Note: Sessions from these users will be archived.

Action Type

Type: Archive

User Name:

Password:

Save Schedule

- 3) In the **Schedule Status and Information** section, enable the schedule status by selecting the **Enabled** check box. The status shows **Active**.

Schedule Status and Information Save Schedule

Enabled: ☒

Status: Active

Previous Running Date:

Next Running Date:

Current DB time is: 12/9/2014 2:10:49 PM

Sessions to Archive:

Screenshots to Archive:

Schedule created on: 11/18/2014 12:20 PM

Specifying a Date Range for the Archived Data

In the **Date Range for Archiving** section of the **Schedule Archive** page, you can specify a date range for the archived data, by selecting one of the following options:

- **Older than:** Select the radio button, and then select Days, Weeks, or Months, as the period of time for the data to be processed. Note that you cannot select a time range that is less than 3 days from the current time on the database.
- **Date Range:** Select the radio button, and then specify a start and end date for the data to be processed.

Date Range for archiving

☒ Older than: 3 Month(s) Data will be added to the current active archive database.

☐ Date Range: Start Date End Date

Dec 15 2014 Dec 22 2014

Note: Cutoff time is always at midnight.

Selecting the Archive Job Frequency

- 1) In the **Schedule** section of the **Schedule Archive** page, select the archive job frequency from the **Recurs every** drop-down list.

Options are **Once**, **Days**, **Weeks**, or **Months**. Depending on your selection, you may need to specify further information.

Schedule

Select frequency.

Recurs every: Months

Recurs every: 1 Month(s)

On the 1 Day of Month.

at: 1:00 PM

- 2) If you select **Once**, you can configure when you want the one-time job to run, as follows:
- Select **Run Now** if you want the job to be executed immediately after clicking the **Save Schedule** button.
 - Select **Run** if you want the job to be executed on a specified day and time.

Note: Consider the performance impact on the production database server, and make sure that you only run the job during off peak hours.

Schedule

Select frequency.

Recur every : Once

☐ Run Now (Note: Action will be executed immediately on Save)

☒ Run :

on: Sunday

at: 1:00 PM

Specifying the Type of Data to be Processed by the Archive Job

In the **Data Type** section of the **Schedule Archive** page, you select the type of data that will be processed by the archive job. By default, sessions from the **All Servers** group will be processed, but you can add or remove individual servers (or Agents) and/or server groups, according to your requirements. You can also configure the processed sessions by user accounts.

- To configure the processed sessions by servers, click the  button next to the **Server** field, select any server you want to add to the list, and then click **Add**. The server will be added to the list.
- To configure the processed sessions by user accounts, click the  button next to the **User** field, select any user you want to add to the list, and then click **Add**. The user will be added to the list.

Data Type
Filter data by the following servers or server groups:

Server  
Servers Groups  

Name	Type	Version	Status	Date
☐ All Servers	Group			

Check All - Clear All 

Note: Sessions from these servers or server groups will be archived.

Filter data by the following users:
Note: If no user is entered, the action will be performed on all users.

User  

Check All - Clear All 

Note: Sessions from these users will be archived.

Selecting the Action to be Performed on the Job Schedule

In the **Action Type** section of the **Schedule Archive** page, you can select to archive the specified job schedule or delete the scheduled data from the database.

To proceed to archive the specified job schedule

- Select **Archive** from the **Type** drop-down list.

Action Type
Type: 
User Name:
Password:

To delete the scheduled data from the database

Use this option to release space in the archive database.

- 1) Select the **Delete** option from the **Type** drop-down list.
A message appears, warning that the scheduled data is about to be deleted permanently from the ObserveIT database.
- 2) Select the **Authentication** method:
 - **AD Authentication:** When selected, you must enter the **User Name** and **Password** of an Active directory user with **role_DeleteFromObserveIT** permissions on the ObserveIT database.
 - **SQL Server Authentication:** When selected, you must enter the **User Name** and **Password** of an SQL Server login with **db_owner** permissions on the ObserveIT database.

Action Type
 Type: Delete ▼ Warning: Data will be deleted!
 Authentication: ☐ AD Authentication ☒ SQL Server Authentication

Note: To delete data using Active Directory authentication, provide credentials of an Active Directory user with "role_DeleteFromObserveIT" role permissions on the "ObserveIT" database. To delete data using SQL Server authentication, provide credentials of a SQL Server login with "db_owner" role permissions on the "ObserveIT" database.

 User Name:
 Password:

Saving the Job Schedule

- 1) When you have finished defining the archive job schedule, save it by clicking the **Save Schedule** button.

The page displays information about the job status (**Active** or **Disabled**), when the job is next scheduled to run, and the number of sessions and screenshots that will be processed in each instance.

Schedule Archive

Save Schedule

Schedule Status and Information
 Enabled: ☒

Status:	Pending
Previous Running Date:	-
Next Running Date:	2/1/2014 1:00 PM
	Data older than 11/1/2013 12:00 AM will be affected.
	Current DB time is: 1/26/2014 4:18:51 PM
Sessions to Archive:	36
Screenshots to Archive:	4616
Schedule created on:	1/26/2014 4:18 PM

- 2) After the job schedule starts, the job status will switch to **Running** and the sessions will be copied to the archive storage. After all the sessions have been copied, they will be deleted from the production database/file system storage.

Schedule Archive

Save Schedule

Schedule Status and Information

Enabled:	☒
Status:	Running [Copy to Archive (6%)]
Previous Running Date:	-
Next Running Date:	2/1/2014 1:00 PM
	Data older than 11/1/2013 12:00 AM will be affected.
	Current DB time is: 1/26/2014 4:18:51 PM
Sessions to Archive:	36
Screenshots to Archive:	4616
Schedule created on:	1/26/2014 4:18 PM

Note: If you selected an archive job schedule of **Run Once**, after the job runs, the status reverts to **Disabled**.

Managing the Archive Storage

You can manage the archive storage from the **Storage Management** tab of the **Configuration > Archive** page.

In the **Archive Storage Management** page, you can:

- Manage the currently active archive database.
- Manage the currently active screen capture archive, if the file system is used to store the screen image data.
- View previous data storage archive locations.

Note: The contents of the **Storage Management** tab differ, depending on whether the SQL Server or the file system is being used for the archive screen capture data. The following screenshot includes the **Active Screen Capture Archive** section which appears when the file system is used; if the SQL Server is used for archiving both the metadata and screen capture data, this section will not appear.

The screenshot displays the **Configuration > Archive > Storage Management** page. The **Storage Management** tab is selected. The page is titled **Archive Storage Management** and contains three main sections:

- Active Archive Database:**
 - Archive data stored in: SQL Server
 - Database server: WIN2003R2X86
 - Database name: ObserveIT_Archive_1
 - Database path: c:\program files\microsoft sql server\mssql.1\mssql\data\ObserveIT_Archive_1_...
 - Date range of included sessions: 07/29/2013 12:42 - 08/07/2013 08:32
 - Size of archive database: 0.10 GB (8 slides)
 - Low DB space notification: Not Configured [Change...](#)
 - [Add New Archive Database](#)
- Active Screen Capture Archive:**
 - Screen capture data stored in: File System
 - File system location: C:\archive (D18W3S5-2)
 - Date range of included sessions: 07/29/2013 12:42 - 08/07/2013 08:32
 - Current screen capture storage: 0.00 GB (0 screens)
 - Low disk space notification: Not Configured [Change...](#)
 - [New Screen Capture Archive Location](#)
- Historical Data Storage Locations:**
 - 1 - 1 of 1
 - 1
 - DB and Related Screen Data Locations
 - First Session Date
 - Last Session Date
 - Sessions DBSize (GB)
 - Freeze Date

Managing the Active Archive Database

In the **Active Archive Database** section, you can:

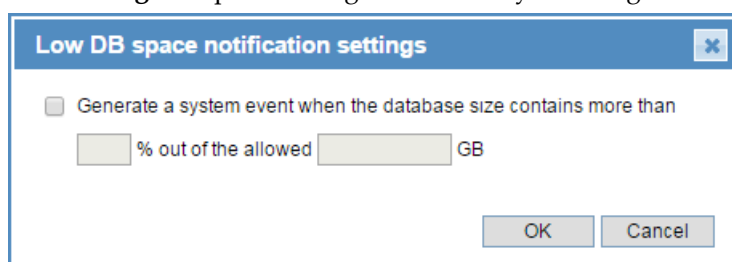
- View detailed information about the currently active archive database, and the sessions that are stored in it.
- Define a threshold that will trigger a system event if the archive database reaches its maximum allocated storage.
- Create a new archive database if the current archive database size exceeds its maximum allocated storage.

The following information is provided about the currently active archive database:

- Archive data stored in: "SQL Server".
- Database Server: Server that hosts the SQL Server database.
- Database Name: Name of the archive database.
- Database Path: Path to the location of the archive database.
- Date range of included sessions: First date (and time) to last date (and time).
- Size of archive database: Size of archive database (GB) and number of slides.
- Low DB space notification: "Not Configured"/threshold showing the maximum actual disk space allocated for the archive data. A system event will be generated when the archive database size contains more than ? % of the allowed ? GB.

To configure a threshold for a system event if the archive database reaches its maximum allocated storage

- 1) Navigate to **Configuration > Archive > Storage Management** tab.
- 2) In the **Active Archive Storage Management** section, navigate to **Low DB space notification** and click **Change** to open a dialog box that lets you configure a different threshold.



- 3) Select the check box, **Generate a system event when the disk contains more than**.

Note: To clear a system event, clear this check box, and click **OK**.

- 4) Specify the maximum disk space that you want to allocate for the archive data, by entering values in the "%" and "GB" fields.
- 5) Click **OK**.

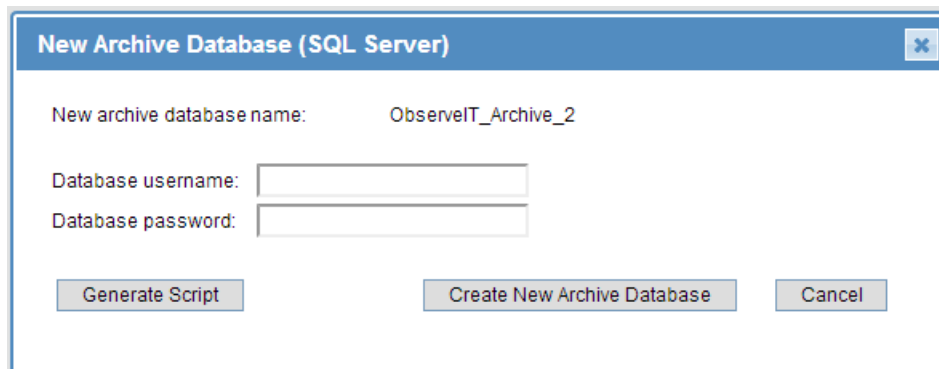
A system event is generated when the disk reaches the specified values. If the event is ignored, after the allocated disk space is reached, you may experience data loss. For further details, see [System Events](#).

Note: A message will be sent to the user after SMTP settings are configured (see [SMTP Configuration](#)) and a recipient email address is configured (see [Receiving Alert Notifications by Email](#)).

To create a new archive database on the existing server

- 1) In the **Active Archive Database** section, click the **Add New Archive Database** button.

The **New Archive Database** dialog box opens.

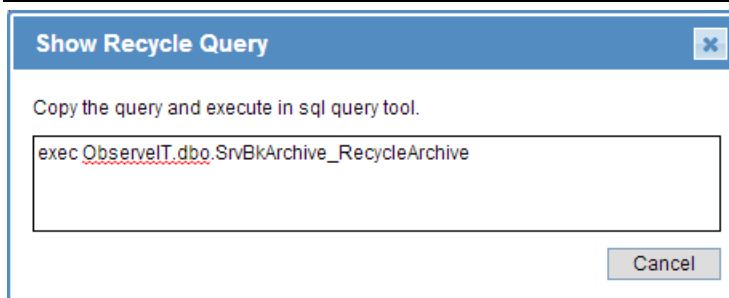


The dialog box titled "New Archive Database (SQL Server)" has a close button (X) in the top right corner. It contains the following fields and buttons:

- New archive database name: ObserveIT_Archive_2
- Database username:
- Database password:
- Buttons: Generate Script, Create New Archive Database, Cancel

- 2) Enter user credentials (username and password) for the current database.

Note: If you do not have the correct SQL server **dbcreator** permissions, click the **Generate Script** button to generate an SQL server script that may be run remotely on the target SQL server by a database administrator with permissions to create a new database on the current database server.



The dialog box titled "Show Recycle Query" has a close button (X) in the top right corner. It contains the following text and button:

- Copy the query and execute in sql query tool.
- Text box containing: `exec ObserveIT.dbo.SrvBkArchive_RecycleArchive`
- Button: Cancel

- 3) Click **Create New Archive Database**.

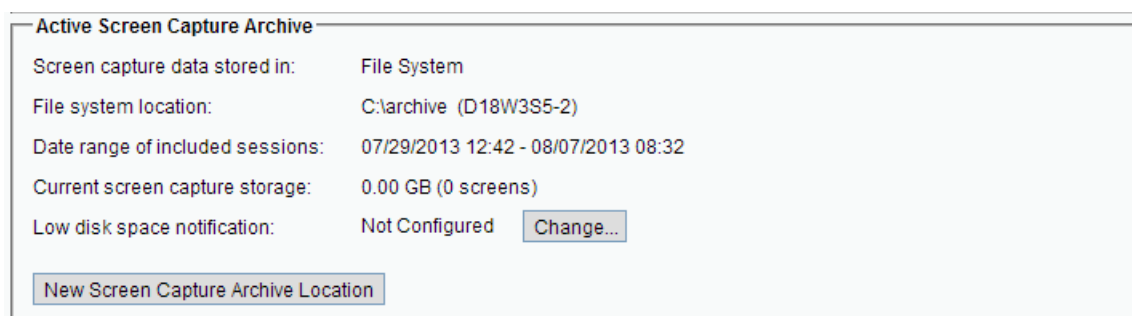
Note: An archive job always uses the most recently created archive database. As soon as the new archive database is created by the SQL Server administrator, ObserveIT will begin using it. The previously used archive database will be displayed in the **Historical Data Storage Locations** section.

Managing the Active Screen Capture Archive

Note: The **Active Screen Capture Archive** section only appears in the **Archive Storage Management** page only if the file system is being used to archive the screen image data.

In the **Active Screen Capture Archive** section, you can:

- View detailed information about the current screen capture archive data storage.
- Define a threshold that will trigger a system event if the specified archive file reaches its maximum allocated storage.
- Define new file system locations in which to store archived screen capture data.



The screenshot shows a configuration window titled "Active Screen Capture Archive". It contains the following fields and values:

Screen capture data stored in:	File System
File system location:	C:\archive (D18W3S5-2)
Date range of included sessions:	07/29/2013 12:42 - 08/07/2013 08:32
Current screen capture storage:	0.00 GB (0 screens)
Low disk space notification:	Not Configured Change...

At the bottom of the window is a button labeled "New Screen Capture Archive Location".

The following information is displayed about the currently active screen capture archive data storage:

- Screen capture data stored in: "File System".
- File system location: File system archive path (local on server, or network share).
- Date range of included sessions: First date (and time) to last date (and time).
- Current screen capture storage: Size of storage for current screen capture session (GB) and number of screens.
- Low disk space notification: "Not Configured"/threshold showing the maximum actual disk space allocated for the screen capture data. A system event will be generated when the disk size contains more than ? % of the allowed ? GB.

If required, you can click the **Change** button to open a dialog box that lets you configure/specify a different threshold.

Note: Before the current file system archive file reaches its maximum allocated storage, it is recommended that you create a new file system location in which to store the archived screen capture data.

To create a new archive location for screen capture data

- 1) In the **Active Screen Capture Archive** section, click the **New Screen Capture Archive Location** button.

The **New Screen Capture Archive Location** dialog box opens.

- 2) Enter a new file system path (local on server, or network share) to the new archive location, and click **Verify**.

The system checks that the new path exists, has not already been used, and is not a subfolder of an already used path. The system also checks that the user account used by the ObserveIT application pool on the Web Console has read and write permissions for the specified path.

- 3) If required, you can configure a threshold setting for the new path that will generate a system event.
- 4) Click **OK**.

Before the changes and data are written to the new path, a confirmation dialog box opens:

"You are about to change the screen capture data storage location from <old file system path> to <new file system path>. This action cannot be reversed. However, as long as the path to the previous location is still accessible by the system, data in it can be replayed. After you click **Yes**, all new session screen capture data will be stored in the new path. Are you sure that you want to proceed?"

- 5) Click **Yes** to proceed.

Once committed, the active local or network path to the archive location will change to the new path, and all session screen captures will immediately be archived there. The old path will be displayed in the **Historical Data Storage Locations** section.

Note: You can define multiple archive file system locations for the currently active archive database.

Viewing Previous Archive Data Storage Locations

In the **Historical Data Storage Locations** section, you can see detailed information about:

- Archive databases that were previously used by the system for archiving data.
- Local/network paths which were previously used by the system for archiving screen capture data.

Important: When using the file system, the archived screen captures are stored under the current archive database (with the related metadata) under the currently active archive path. This enables administrators to easily correlate the archive file system data with the relevant archive database. Since you can define multiple archive file system locations for each active archive database, you can also see a number of archive databases each with several file system locations.

When the file system archive is *not* active, the details of each historical archive database are displayed in a list, as shown in the following example:

Archive Storage Management

Active Archive Database

Archive data stored in: SQL Server
 Database Server: OBS-SQLDEVOIT_DEV_569
 Database Name: ObserveIT_Archive_2
 Database path: C:\Program Files\Microsoft SQL Server\MSSQL.11\MSSQL\DATA\ObserveIT_Arc...
 Date range of included sessions: N/A
 Size of archive database: 7.18 GB (0 Slides)
 Low DB space notification: When reaches 2% of the allowed 123.00 GB [Change...](#) ⓘ

[Add New Archive Database](#) ⓘ

Historical Data Storage Locations

1 - 1 of 1 1

DB and Related Screen Data Locations	First Session Date	Last Session Date	Sessions	DBSize (GB)	Freeze Date
ObserveIT_Archive_1	10/27/2013	02/03/2014	128	38	01/25/2014

When the file system archive *is* active, each archive database entry can be expanded (by clicking the  icon) to show the related file system locations, as shown in the following example:

Archive Storage Management

Active Archive Database

Archive data stored in: SQL Server
 Database Server: OBS-SQLDEVOIT_DEV_569
 Database Name: ObserveIT_Archive_2
 Database path: C:\Program Files\Microsoft SQL Server\MSSQL.11\MSSQL\DATA\ObserveIT_Arc...
 Date range of included sessions: N/A
 Size of archive database: 7.18 GB (0 Slides)
 Low DB space notification: When reaches 2% of the allowed 123.00 GB [Change...](#) ⓘ

[Add New Archive Database](#) ⓘ

Active Screen Capture Archive

Screen capture data stored in: File System ⓘ
 File system location: C:\fs1\ObserveIT_Archive_2 (OIT-BORIS)
 Date range of included sessions: N/A
 Current screen capture storage: 0.00 GB (0 screens)
 Low disk space notification: Not Configured [Change...](#) ⓘ

[New Screen Capture Archive Location](#) ⓘ

Historical Data Storage Locations

1 - 1 of 1 1

DB and Related Screen Data Locations	First Session Date	Last Session Date	Sessions	DBSize (GB)	Freeze Date
 ObserveIT_Archive_1	10/27/2013	02/03/2014	128	38	01/25/2014
 Screen Capture Location	First Session Date	Last Session Date	Disk Space (GB)	Screens	
C:\fs1\ObserveIT_Archive_1	10/27/2013	12/24/2013	112 MB	4,200	
C:\fs2\ObserveIT_Archive_1	12/24/2013	02/03/2014	103 MB	5,105	

Note: In the **Diary** tab, you can retrieve specific sessions from the archive in order to replay them.

Viewing the Archive Log

You can view archive schedule management actions in the archive log.

To view the archive log

- 1) Navigate to **Configuration > Archive**.
- 2) Click the **Log** tab.

The **Log** tab displays information about each archive job that was run. For example, you can see if a specific session in the production database was moved to the archive database by checking if it was within the specified date range of the archived sessions.

Server Diary User Diary DBA Activity Activity Alerts Configuration Search Reports Threat Detection									
Schedule Storage Management Log Diary Search									
Admin Dashboard Console Users Identification Servers Server Groups Server Policies Security Alerts System Events Identity Theft Detection Messages Ticket Integration License SMTP Settings Monitor Log LDAP Settings Storage Archive Saved Sessions Audit System Log									
Quick Help Installation Guide User Guide Configuration Guide									
Archive Log									
1 - 20 of 40 1 2 Next > Last >>									
Status	Start Time	Duration	Date Range	Created By	Sessions	Screenshots	DB Name	Action	
✗	1/9/2014 3:45 PM	00:00:00	1/9/2014 - 1/11/2014	Admin			ObserveIT_Archive_1	Archive	
✗	1/9/2014 3:35 PM	00:00:00	1/9/2014 - 1/10/2014	Admin			ObserveIT_Archive_1	Archive	
✗	1/9/2014 3:29 PM	00:00:00	1/9/2014 - 1/10/2014	Admin			ObserveIT_Archive_1	Archive	
✓	1/9/2014 9:22 AM	00:00:11	1/9/2014 - 1/10/2014	Admin	1	30	ObserveIT_Archive_1	Archive	
✓	1/8/2014 12:19 PM	00:00:04	1/8/2014 - 1/9/2014	Admin	1	46	ObserveIT_Archive_1	Archive	
✗	1/8/2014 10:22 AM	00:00:00	1/7/2014 - 1/8/2014	Admin			ObserveIT_Archive_1	Archive	
✗	1/8/2014 9:40 AM	00:00:00	1/7/2014 - 1/8/2014	Admin			ObserveIT_Archive_1	Archive	
✗	1/7/2014 2:42 PM	00:00:00	1/7/2014 - 1/8/2014	Admin			ObserveIT_Archive_1	Archive	
✗	1/7/2014 2:23 PM	00:00:00	1/7/2014 - 1/8/2014	Admin			ObserveIT_Archive_1	Archive	
✗	1/7/2014 2:19 PM	00:00:00	1/7/2014 - 1/9/2014	Admin			ObserveIT_Archive_1	Archive	
✗	1/7/2014 1:52 PM	00:00:00	1/7/2014 - 1/8/2014	Admin			ObserveIT_Archive_1	Archive	
✓	1/7/2014 1:12 PM	00:00:22	1/7/2014 - 1/8/2014	Admin	2	152	ObserveIT_Archive_1	Archive	
✓	1/5/2014 10:52 AM	00:00:06	1/1/2014 - 1/2/2014	Admin	6	81	ObserveIT_Archive_1	Archive	
✓	1/5/2014 10:24 AM	00:01:01	1/2/2014 - 1/3/2014	Admin	34	1019	ObserveIT_Archive_1	Archive	
✓	12/30/2013 3:24 PM	00:00:09	12/19/2013 - 12/20/2013	Admin	2	58	ObserveIT_Archive_1	Archive	
✓	12/11/2013 3:17 PM	00:00:10	12/1/2013 - 12/2/2013	Admin	7	229	ObserveIT_Archive_1	Archive	
✗	12/11/2013 2:20 PM	00:00:00	12/1/2013 - 12/2/2013	Admin			ObserveIT_Archive_1	Archive	
✗	12/11/2013 2:17 PM	00:00:00	12/1/2013 - 12/2/2013	Admin			ObserveIT_Archive_1	Archive	
✗	12/11/2013 1:56 PM	00:00:00	11/13/2013 - 11/14/2013	Admin			ObserveIT_Archive_1	Archive	
✓	12/11/2013 1:49 PM	00:00:14	11/13/2013 - 11/14/2013	Admin	3	129	ObserveIT_Archive_1	Archive	

Best Practices for Storage of Large Scale Deployments

ObserveIT can support large enterprise implementations comprising thousands of monitored users.

This topic provides important information about how to configure the ObserveIT database for large scale deployments.

The following sections describe how to optimize storage for the:

- Operating system on the SQL Server
- SQL databases' disks
- SQL databases
- File System for storing graphical images
- Archive configuration
- Database maintenance

SQL Server Operating System Optimization

To optimize the SQL Server's memory usage, follow the steps described in the Microsoft KB article: [Enable the Lock Pages in Memory Option \(Windows\)](#).

SQL Databases Disk Storage Optimization

The SQL Server database, which is used to store captured data and configuration settings, continuously grows as more sessions are recorded. To prevent data loss as the database becomes full, it is recommended that you optimize your database storage configuration, as follows:

- Use dedicated disk arrays for data files (MDF files), transaction logs (LDF files), and the tempdb database.
- Use Microsoft best practices when formatting and configuring disk alignment. For further details, refer to the Microsoft article: [Disk Partition Alignment Best Practices for SQL Server](#).

Databases Configuration

During installation, the ObserveIT Database Server creates the following databases on the SQL Server for storing captured data and configuration settings:

- ObserveIT
- ObserveIT_Data
- ObserveIT_Archive_1
- ObserveIT_Archive_template

The SQL Server must be configured for optimal performance so that the databases used by the server will not become a bottleneck which will affect the overall performance of the system. For details on how to configure your database for optimal performance, refer to the Microsoft article: [Pre-Configuration Database Optimizations](#).

For optimal performance of the ObserveIT and ObserveIT_Data databases, it is recommended to:

- Set the initial size for MDF files to 100GB.
- Set the initial size for LDF files to 50GB.
- Use separate disks for MDFs (Data files) and LDFs (Transaction logs).
- (Optional) Create multiple MDF files (one for each CPU core up to 8) on separate disks for the ObserveIT database (if you have enough disks).

For optimal performance of the `tempdb` database, it is recommended to:

- Create multiple MDF files (one for each CPU core, up to 8) to reduce allocation contention.
- On the SQL Server instance, set up the MSSQL Trace Flag – T1118 in the service startup parameters.
- Reduce allocation contention on the `tempdb` database by forcing uniform extent allocations. For further details, refer to the Microsoft article: [Concurrency enhancements for the tempdb database](#).

For all four ObserveIT databases, it is recommended to use the **Simple Recovery Model**; however, if the customer specified a point in time recovery option, you should use **Full Recovery Model** instead.

File System for Storing Graphical Images

In large scale deployments, the file system is the recommended method for storing graphical images, instead of the SQL Server database. For performance and scalability reasons, the recorded visual images must be stored on a file share in the network. For further details, see [Storing the ObserveIT Screenshots](#) (in the Installation Guide).

To optimize your file system storage, do the following:

- Configure file system storage for the images data during or immediately after installation.
- Use a dedicate storage for images data (that is, avoid using the same storage array as the one that was used for the SQL Server databases).
- When using multiple Application Servers, all Application Servers must be able to access the same path to store the graphical images (UNC path).
- Create a new file system when the current one reaches approximately 4 billion objects (due to NTFS file system limitations).

Archive Configuration

In large scale deployments, when archiving data, note the following:

- Archive configuration is mandatory from day 1. You should configure archiving for data older than X days immediately after the product installation, when the databases are relatively small.
- Create a new archive database when the volume of data in the active archive database reaches approximately 400-500 GB. A notice can be set for this in the Web Console.
- Schedule archiving jobs for non-busy hours on a daily basis.
- When using the file system for archiving stored images data, you should create a new archive path when the current one reaches approx. 4 billion objects (due to NTFS file system limitations).
- For further details about the ObserveIT archiving process, see [Managing the Archive Storage](#).

Database Maintenance

The ObserveIT databases should be maintained on a regular basis and kept at a manageable size in order for the system to work properly and efficiently. In addition to archiving, database maintenance is performed by the Re-indexing and Update-Statistics processes.

Database re-indexing reorganizes the data of the table's indexes to increase the performance of SQL Queries and overall performance of the database. Indexes that are fragmented are not efficient and introduce additional resources on the system, thus derogating the performance. The Update-Statistics process collects information about queries in the database and helps the Execution-Planner in the database reach better results when selecting an Execution Plan for queries. These two processes result in faster queries execution and faster data retrieval, thus providing an overall increase in Database performance.

The following procedures are recommended to increase database overall performance:

- Rebuild Indexes: Schedule "smart" index rebuild on a daily basis (after the archiving process is completed).
- Statistics Update: Schedule "stats" update with FULLSCAN on a daily basis.

For further details, refer to the documentation and maintenance scripts described [here](#).

Backing Up the ObserveIT Databases

It is important to properly back up the data stored inside the SQL databases in case the SQL server suffers a catastrophic event.

All data stored in SQL databases can utilize existing backup solutions that are built-in to Microsoft SQL Server, or 3rd party database backup solutions.

Note: If you have used the archiving feature of ObserveIT, you may have additional SQL server databases that are used by ObserveIT in addition to the default production databases. If this data is important to your organization, make sure you also include the archive databases in your backup plan.

By utilizing your existing backup solutions you can easily backup your SQL server, and thus protect your ObserveIT data and configuration.

For information on how to back up the SQL Server, refer to your backup software manual.

You can also refer to the following Microsoft Knowledge Base articles:

- [Back Up and Restore of SQL Server Databases](#)
- [Backup Overview \(SQL Server\)](#)

Saving Sessions

This topic describes how to save recorded ObserveIT sessions to view them offline.

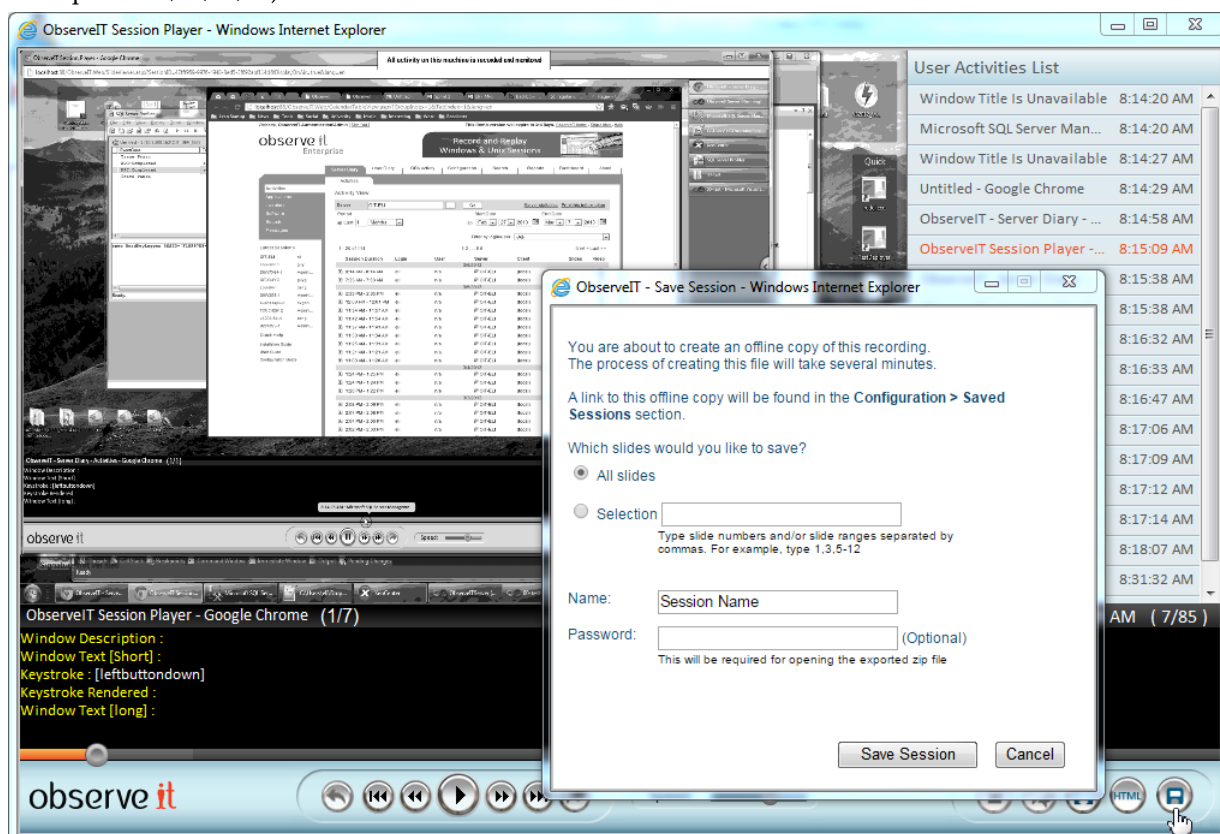
Note: Saving sessions for training purposes is not supported in this version of the product. If it is essential that your system is configured to save sessions for training purposes, contact ObserveIT support at <http://www.observeit.com/Support>.

Saving sessions for offline viewing is particularly useful when the person who is viewing the recording does not have access permissions or the possibility to use the online **Session Player**. Saved sessions can be viewed by anyone with access to the zipped file containing the saved session.

Note: Saving sessions for offline viewing does not affect the actual saved session, and data is still retained in the ObserveIT database.

To save a session for offline viewing

- 1) Navigate to **Configuration > Saved Sessions**.
- 2) In the **Server Diary**, **User Diary**, or **Search** or **Report** result, open the **Session Player** for the required Windows session, and click the **Save**  icon.
The **Save Session** dialog box opens. For further details, see Windows Session Player (in the User Guide).
- 3) In the **Save Session** dialog box, select the slides that you want to include in the saved session. You can save the entire recording (**All slides**), or select individual slides or a range of slides (for example: 1-10,15,18,22).



- 4) In the **Name** field, type a name for the session that you want to save.

- 5) (Optional) In the **Password** field, type a password to provide more security for the saved session.
- 6) Click **Save Session**.

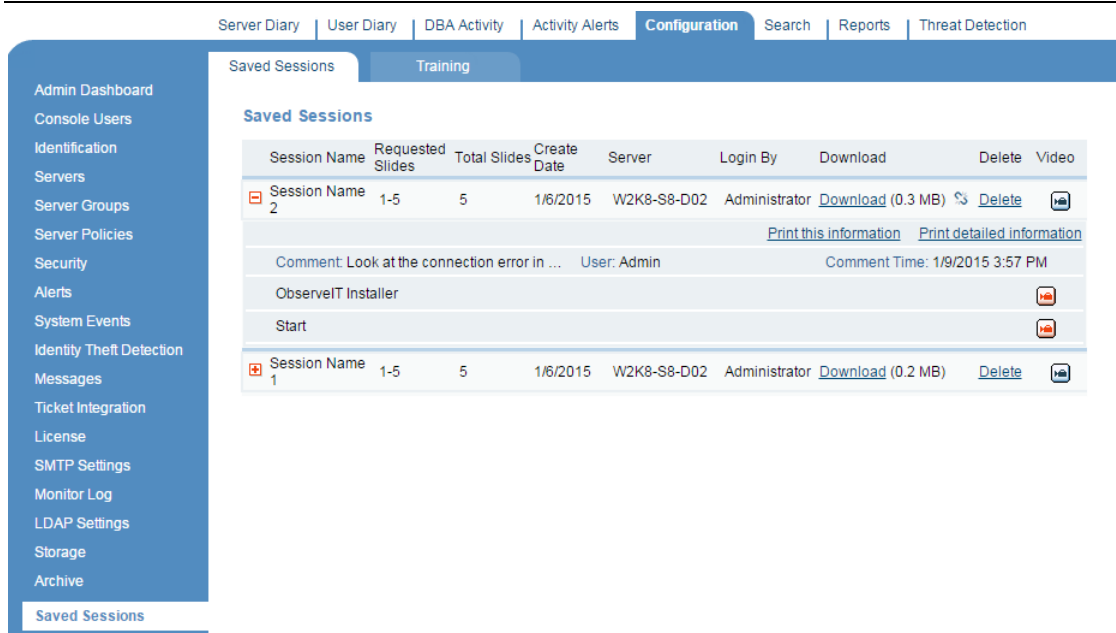
The session is saved in the **Configuration > Saved Sessions** tab.

- 7) Navigate to **Configuration > Saved Sessions**.

The **Saved Sessions** page displays a list of all previously saved sessions.

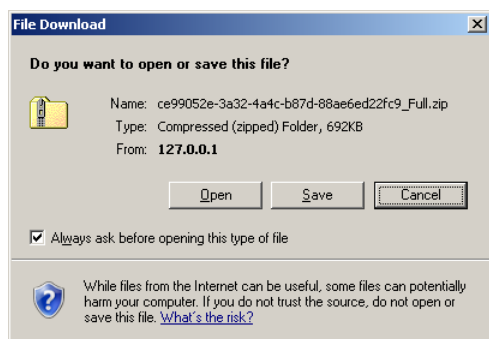
The recently saved recording is displayed in the **Saved Sessions** list initially with a "Pending" status. After some time (the file might take several minutes to generate), the status will change to indicate that the file is available for download. You can also view the number of slides that are included in the saved session, the session's date, and additional information.

Note: The appearance of a  warning icon next to a saved session indicates that some slides may be missing from the session. Even after receiving a warning about missing image data following a session integrity check, the session could still be exported. For further details, see *Windows Session Player* (in the User Guide).

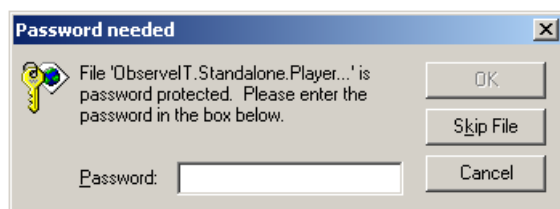


Session Name	Requested Slides	Total Slides	Create Date	Server	Login By	Download	Delete	Video
Session Name 2	1-5	5	1/6/2015	W2K8-S8-D02	Administrator	Download (0.3 MB)	Delete	
Comment: Look at the connection error in ... User: Admin Comment Time: 1/9/2015 3:57 PM ObserveIT Installer Start								
Session Name 1	1-5	5	1/6/2015	W2K8-S8-D02	Administrator	Download (0.2 MB)	Delete	

- 8) Click the **Download** link next to the saved recording. Save the file to a location on your computer.



Note: If you provided a password for the session when it was saved, you will be required to enter that password to open the exported session's zip file.



The .ZIP archive contains an application called `ObserveIT.Standalone.Players.ExportablePlayer.exe`, and a directory of slides in .screenshot file format. The number of slides corresponds to the number of slides in the ObserveIT Web Console.

- 9) Extract the contents of the .ZIP archive to a directory and run the `ObserveIT.Standalone.Players.ExportablePlayer.exe` application to view the session's slides (in the same way as when using the ObserveIT **Session Player**).

To delete the saved session (if required), click the **Delete** link next to the saved recording.

Auditing Access to the Web Console

ObserveIT has an internal auditing system. Each time a video is accessed, a log is created of the user name, IP address, the captured session, and the frames that were viewed. This log provides auditing of the administrators who accessed the Web Console, and prevents the need for an external audit mechanism. The audit trail cannot be deleted, which means that each access to the Web Console will always be visible in the audit log.

Note: You can also generate reports to provide summary information about user logins, sessions, and saved sessions in which console users were active. For further details, see [Reports](#) (in the User Guide).

To view the audit log for the Web Console

- Navigate to **Configuration > Audit**.

The **Audit** page opens displaying the following four tabs:

- **Logins**: displays details about all successful and failed logins to the Web Console.
- **Sessions**: provides information about all the sessions which were replayed by the user.
- **Saved Sessions**: provides information about recorded ObserveIT sessions that were saved for viewing offline.
- **Configuration Changes**: enables you to track configuration changes that were made while working in the Web Console. By default, this tab is disabled.

The topics in this section describe the audit log information that is displayed for each of these tabs.

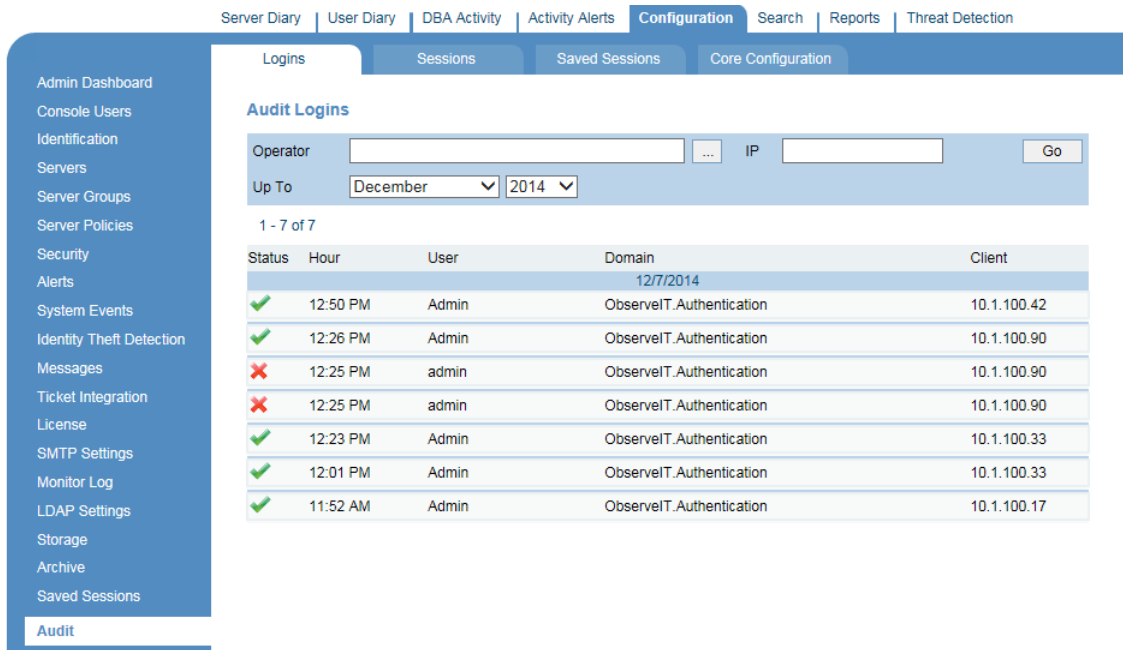
Auditing Logins

For auditing purposes, ObserveIT enables you to track details about user logins to the Web Console, including whether the login was successful.

Each time a user logs in to the Web Console, an audit entry is created.

To view the user logins to the Web Console

- 1) Navigate to the **Configuration > Audit > Logins** tab.



The screenshot shows the ObserveIT web interface. The top navigation bar includes tabs for Server Diary, User Diary, DBA Activity, Activity Alerts, Configuration (selected), Search, Reports, and Threat Detection. The left sidebar lists various system components, with 'Audit' selected at the bottom. The main content area is titled 'Logins' and contains a sub-tab 'Audit Logins'. Below this, there are search filters for 'Operator' and 'IP' with a 'Go' button, and a date range selector set to 'December 2014'. A table displays the audit logins, showing 1 - 7 of 7 entries. The table columns are Status, Hour, User, Domain, and Client.

Status	Hour	User	Domain	Client
12/7/2014				
✓	12:50 PM	Admin	ObserveIT.Authentication	10.1.100.42
✓	12:26 PM	Admin	ObserveIT.Authentication	10.1.100.90
✗	12:25 PM	admin	ObserveIT.Authentication	10.1.100.90
✗	12:25 PM	admin	ObserveIT.Authentication	10.1.100.90
✓	12:23 PM	Admin	ObserveIT.Authentication	10.1.100.33
✓	12:01 PM	Admin	ObserveIT.Authentication	10.1.100.33
✓	11:52 AM	Admin	ObserveIT.Authentication	10.1.100.17

In the **Logins** tab, you can view the following information for each user login:

- An indication of whether the login was successful or failed. For failed logins, a reason for the failure is provided.
 - The date and time of the user login.
 - The Console User that accessed the Web Console.
 - The domain name (if the Console User is configured with an external Active Directory or LDAP domain)
 - The IP address which was used to log on to the Web Console.
- 2) You can filter the display by Console User name (Operator), remote IP address of the management workstation, and date.

Auditing Session Replays

For auditing purposes, ObserveIT enables you to view information about all sessions in the Web Console which were replayed by the user. A "Session audit" entry is added whenever a user opens the Video Player for a session.

To view details about sessions that were replayed

- 1) Navigate to the **Configuration > Audit > Sessions** tab.

The screenshot displays the 'Audit Sessions' tab in the ObserveIT configuration interface. The sidebar on the left lists various system components. The main content area features a search bar with fields for 'Operator', 'IP', and a date range 'Up To' set to 'March 2014'. Below the search bar, it indicates 'Results: 1 - 6 of 6' and displays a table of audit entries. The table columns are 'Audit Hour', 'Operator', 'Client', 'Server', 'Session Login', 'Session Date', and 'Video'. The entries show sessions for 'Admin' on 'Q3-WIN8-SQL5' server, with dates ranging from 2/29/2012 to 2/28/2014. Each entry has a red square icon with a white plus sign and a video icon.

Audit Hour	Operator	Client	Server	Session Login	Session Date	Video
2/29/2012						
1:22 PM	Admin	192.168.254.105	Q3-WIN8-SQL5	Administrator	2/28/2014 1:45:20 PM	 
1:22 PM	Admin	192.168.254.105	Q3-WIN8-SQL5	Administrator	2/28/2014 1:45:20 PM	 
2/28/2012						
1:58 PM	Admin	192.168.254.105	Q3-WIN8-SQL5	Administrator	2/28/2014 1:45:20 PM	 
1:58 PM	Admin	192.168.254.105	Q3-WIN8-SQL5	Administrator	2/28/2014 1:45:20 PM	 
1:57 PM	Admin	192.168.254.105	Q3-WIN8-SQL5	Administrator	2/28/2014 1:45:20 PM	 
1:45 PM	Admin	127.0.0.1	Q3-WIN8-SQL5	Administrator	2/28/2014 1:45:20 PM	 

- 2) In the **Sessions** tab, you can filter the display by searching for sessions according to Console User name (Operator), the remote IP address of the management workstation, and date.

The following information is displayed for each audit entry:

-  : Click to open the session details for an entry.
- **Audit Hour:** The time that the audit entry was created (that is, when the user opened the Video player for the session).
- **Operator:** The Console User that accessed the Web Console.
- **Client:** The IP address which was used to log on to the Web Console.
- **Server:** The name of the server on which the session took place.
- **Session Login:** The user that logged in to the session.
- **Session Date:** The date and time that the session occurred.
- **Video**  icon: Click to replay the session. When Session Replay Privacy Protection is enabled, a lock icon appears next to the **Video**  icon. When clicking the **Video**  icon, users will be prompted to enter their Replay Privacy Protection password. For further details, see [Enabling Session Replay Privacy](#).

Auditing Saved Sessions

In the **Audit Saved Sessions** tab, you can view details about recorded ObserveIT sessions that were saved for viewing offline. These sessions were saved in the **Configuration > Saved Sessions** tab of the Web Console. Saved sessions include details of the number of slides in the recordings, the session's date, and additional information. After a recorded session is saved, it becomes available for downloading. For further details, see [Saving Sessions](#).

A "Saved Session" audit entry is created whenever the user creates a saved session.

To view details about sessions that were saved

- 1) Navigate to the **Configuration > Audit > Saved Sessions** tab.

- 2) In the **Saved Sessions** tab, you can filter the display by searching for sessions according to Console User name (**Operator**), date (**Up To**), and **Action Type** (**All**, **Download**, **Delete**).

The following information is displayed for each audit entry:

- : Click to open the session details for an entry.
- **Session Name**: The name of the saved session. You can click the icon next to **Session Name** to see the window title name of the slides.
- **Requested Slides**: When a recorded session is saved, users can specify the slides that they want to include: the entire recording, specific slides, or a range of slides. **Full** means that all slides in the session were saved.
- **Action Time**: The date and time that the session was saved.
- **Server**: The name of the server on which the session was saved.
- **Domain Name**: The domain name (if the Console User is configured with an external Active Directory or LDAP domain).
- **User Name**: The Console User that accessed the Web Console.
- **Total Slides**: The actual number of slides in the saved session.
- **Action Type**: The audit action that was detected. Options are:
- **Download**: The user downloaded the saved session.

- **Delete:** The user deleted the saved session.
- **Video**  icon: Click to replay the session. When Session Replay Privacy Protection is enabled, a lock icon appears next to the **Video**  icon. When clicking the **Video**  icon, users will be prompted to enter their Replay Privacy Protection password. For further details, see [Enabling Session Replay Privacy](#).

Auditing Configuration Changes

For enhanced security auditing, ObserveIT enables you to track configuration changes that were made while working in the Web Console. For example, if an Agent's recording was turned off or changes were made in a Server policy configuration, you can track exactly who did this, and when it happened.

An audit entry is created whenever the user makes configuration changes in one of the following **Areas** in the Web Console:

- **Server Policy** creation, modification, or remove operations. For example:
 - The Agent recording status was temporarily disabled.
 - A User Recording policy was modified in order to record only specific users.
 - Continuous recording was enabled in a Windows system policy.
- **Session Data Integrity** definition changes. For example: Image Security was enabled on the Application Server in order to protect images in the database.
- **Identification** modifications. For example: A new LDAP Target Domain Identification was added.
- **Licensing** changes. For example:
 - The total number of Registered Agents was changed.
 - The ObserveIT software version was changed from **Lite** to **Commercial**.
- **Application Server** modifications. For example:
 - A specific server is configured to require a security password when installing an Agent. In this case, "Require password to install an Agent" is changed from Disable to Enabled.
 - An Agent security installation password was changed.
- **Session Privacy** modifications. For example: Session Replay Privacy Protection was changed to Enabled.

To view configuration changes in the Web Console

- 1) Navigate to the **Configuration > Audit > Configuration Changes** tab.

The screenshot shows the 'Configuration Changes' audit page in the Web Console. The sidebar on the left contains navigation links for various system components. The main panel has tabs for Logins, Sessions, Saved Sessions, and Configuration Changes. The Configuration Changes tab is active, showing a search interface with filters for Area, Item, and Period. Below the filters, a table lists the configuration changes, including details like Time, Console User, Client IP, Area, Item, and Action.

Time	Console User	Client IP	Area	Item	Action
12/28/2014					
3:16 AM	Admin	10.1.100.133	Application Server	W12-S12-D01	Changed
				Require password to install an Agent	Changed to Enabled
				Require password to uninstall an Agent	Changed to Enabled
				Agent Installation Security Password	Changed to *****
3:16 AM	Admin	10.1.100.133	Data Integrity		Changed
				Session Data Integrity	Changed to Enabled
3:15 AM	Admin	10.1.100.133	Server Policy	Default Unix-based...	Changed
3:14 AM	Admin	10.1.100.133	Server Policy	Default Windows-b...	Changed
3:14 AM	Admin	10.1.100.133	Server Policy	Default Windows-b...	Changed
				Identification Policy - Enforce Login	Changed to Do not enforce login
				Identification Policy - Save last used login	Changed to Disabled
3:14 AM	Admin	10.1.100.133	Server Policy	Default Windows-b...	Changed
3:13 AM	Admin	10.1.100.133	Server Policy	Windows Servers P...	Changed
3:13 AM	Admin	10.1.100.133	Server Policy	Default Unix-based...	Changed
3:12 AM	Admin	10.1.100.133	Server Policy	Windows Servers P...	Added

- 2) Filter the display of audit entries by selecting the search criteria, as follows:
 - **Area:** select the relevant option from the drop-down list, or select **All** to display entries for all configuration areas.
 - **Item:** select the relevant option from the drop-down list, or select **All** to display entries for all configuration items.
 - **Period/Date range:** specify the time period/date range during which the changes were made.
- 3) After you have defined your search criteria, click **Show** to display a list of audit entries according your selected criteria.

You can click **Reset** to revert to the previously filtered display.

Entries are listed in reverse chronological order.

For each audit entry, the following information is displayed:

- - Click to view the exact configuration details that were made for the entry.
- The time that the action occurred (that is, the change was made).
- The **Console User** that was logged in to the Web Console.
- The **Client IP** address of the user that performed the action.
- The **Area** in the Web Console that was changed.
- The **Item** in the **Area** on which the configuration was changed. For example: **LDAP Target Domain**, **Default Windows-based Policy**, and so on.
- The action that was performed on the configured item. For example: **Changed**, **Removed**, **Added**.

Using Hotkeys

ObserveIT allows you to access the following features by using the F11 and F12 hotkeys:

- F11 enables you to create Sticky Notes which can be attached to resources and applications on the monitored servers.
- F12 enables the use of context sensitive searches through the database.

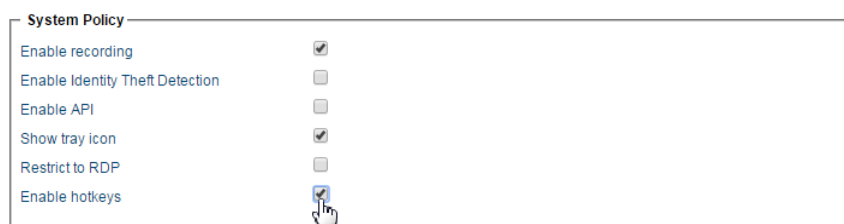
You can attach Sticky Notes at any point in a program dialog or configuration setting to provide specific information about what to do (or NOT to do) for that situation. The Sticky Note will appear whenever anyone accesses that resource or application in the future. Sticky Notes can be created for virtually any application or application property sheet, as long as the application's window title is unique.

Note: Sticky Notes will not prevent the user from continuing with their action and actually performing the task to which the Sticky Note was attached. To prevent users from performing harmful actions, you must use the built-in Windows permissions and user-rights mechanism.

Note: ObserveIT also allows you to create more advanced messages that will be displayed for users logging on to monitored servers.

The Context Sensitive Search feature allows you to easily search for the resource you are currently accessing.

By default, these hotkeys are disabled. To use the hotkeys, you must first enable the hotkeys status. You can do this manually per server (or Agent), or by using **Server Policies** to configure many servers (or Agents) simultaneously. For instructions on how to enable the use of hotkeys using **Server Policies**, see [Enabling Hotkeys](#).



See the following topics:

- [Sticky Notes](#)
- [Context Sensitive Search](#)

Sticky Notes

ObserveIT constantly monitors the resources and applications accessed by users on the monitored servers. Sticky Notes can be attached at any point in a program dialog or configuration setting to provide specific information about what to do (or NOT to do) in that situation. The Sticky Note will appear whenever anyone accesses that resource or application in the future.

The Sticky Notes feature is accessed by using the F11 Hotkey.

Note: Sticky Notes do not prevent the user from continuing with their action and actually performing the task to which the Sticky Note was attached. However, to prevent users from performing harmful actions, you must use the built-in Windows permissions and user-rights mechanism.

Note: ObserveIT also allows you to create more advanced messages that will be displayed for users logging on to monitored servers. For further details, see [Managing Messages](#).

Configuring ObserveIT Sticky Notes

Sticky Notes can be created for virtually any application or application property sheet.

To create a Sticky Note

This example will warn users about changing the time on the server.

1) Open the **Date and Time** applet.

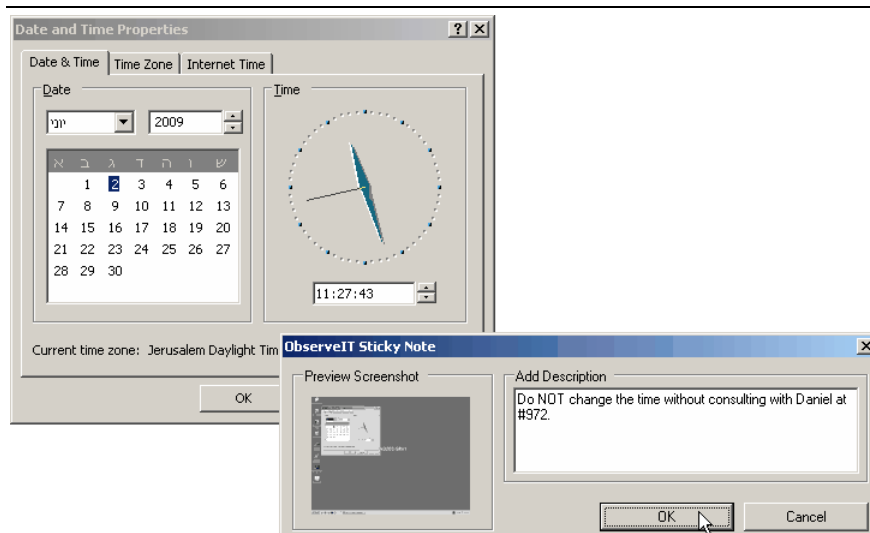
2) Press F11.

The **Sticky Note** creator window opens.

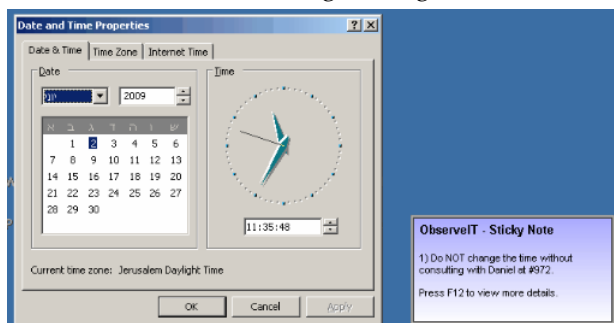
3) Type the text that you want to display in the Sticky Note.

4) Click **OK**.

Note: You can use any language supported by your version of Windows.



Henceforth, whenever someone opens the **Date and Time** applet, the Sticky Note will pop up on the screen with the warning message.



After a few seconds, the Sticky Note popup will fade away.

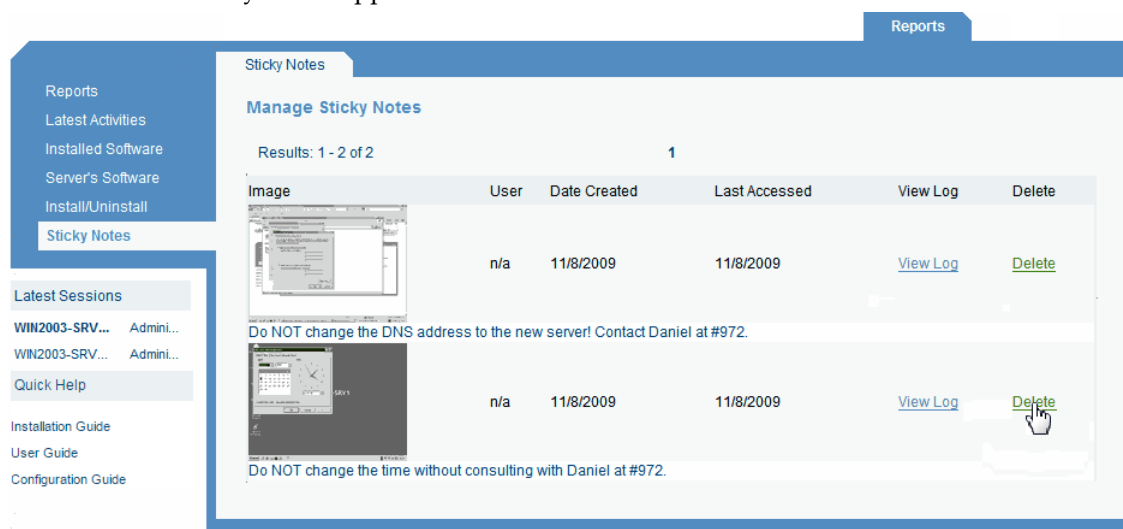
Generating a Sticky Note Report

You can generate a report of all Sticky Notes that have been created to view the resource to which the Sticky Note is attached, and who has viewed the note.

To generate a Sticky Note report

- 1) Navigate to **Reports > Sticky Notes**.

A list of all the Sticky Notes appears.



- 2) Click the **View Log** link next to the required item to view a list all the instances of when the Sticky Note was displayed in the system.

To delete a Sticky Note, click the adjacent **Delete** link (on the right of the item). You will NOT be prompted for your approval. Clicking the **Delete** link immediately deletes the Sticky Note.

Context Sensitive Search

ObserveIT constantly monitors the resources and applications accessed by users on the monitored servers. As a result, you can see all previous accesses of any particular resource or application. The Context Sensitive Search feature allows you to easily search for the resource you are currently accessing.

The Context Sensitive Search feature is accessed by using the F12 Hotkey.

By pressing F12, ObserveIT's Context Sensitive Search searches through the database and displays a list of all previous instances where the same application or resource was accessed.

In the following example, a user is using the Command Prompt. By pressing F12, ObserveIT's Context Sensitive Search will display a list of all previous sessions where the Command Prompt has been accessed.

observe it
Enterprise

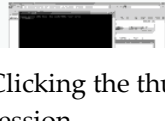
[Sign in](#) (Web Console)

Sticky Notes Results

Image	Description	User Name	Server Name	Date Created
1				

Search Results

Filter By: User Name: Login: Server:

Image	Description	Login Name	User Name	Server Name	Date
	n/a	Administrator	n/a	WIN2003-SRV1	11/08/2009
	n/a	Danielp	n/a	WIN2003-SRV1	11/08/2009
	n/a	Administrator	n/a	WIN2003-SRV1	11/04/2009
	n/a	Administrator	n/a	WIN2003-SRV2	11/04/2009
	n/a	Administrator	n/a	WIN2003-SRV1	11/02/2009
	n/a	Administrator	n/a	WIN2003-SRV1	11/02/2009

Clicking the thumbnail image launches the **Session Player** in which you can view the recorded session.

Note: To view the recorded sessions you must log in to the ObserveIT Web Console.

Managing Reports

ObserveIT provides two groups of predefined reports:

- Custom reports: Sample reports which you can run, schedule, copy, edit, and delete. You can also manually create new custom reports from these sample reports.
- System reports: Built-in reports which you can run, schedule, and copy, but you cannot edit or delete.

In the **Reports** page of the Web Console, you can:

- [Create custom reports](#)
- [Run reports](#)
- [Schedule reports](#)
- [Edit reports](#)
- [Delete reports](#)

For further information, see the Reports section in the User Guide.

Creating Custom Reports

You can create reports depending on your needs. These reports can be reviewed, edited, copied, and deleted.

Copying a custom report is useful when a report needs to be edited and you do not want to save these changes to the original report, or when the original report is used as a basis for other custom reports by using the same initial configuration and parameters.

To create a custom report

- 1) In the Web Console, click the **Reports** tab.

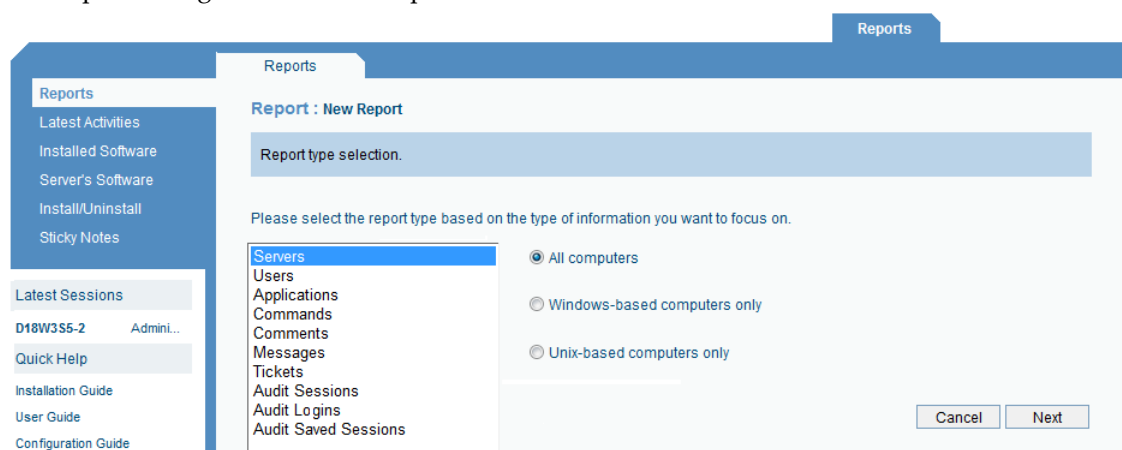
The **Reports** page opens, displaying the **Report List**.

The screenshot displays the 'Reports' section of the ObserveIT web console. On the left is a sidebar with navigation options. The main area is titled 'Report List' and features a search bar for 'Scheduled Reports for Console User:'. A button labeled 'Create New Custom Report' is visible. Below this is a table of reports. The table has columns for Name, Description, Modified, and User. A sub-header 'Custom Reports' is present. The table lists several reports, including 'Audit logins', 'Audit Saved Sessions', 'Audit Sessions', and several 'SAMPLE' reports. Each report entry includes a 'Run' button, a 'Cached' status, and links for 'Schedule', 'Copy', 'Edit', and 'Delete'.

Name	Description	Modified	User	Run	Cached	Schedule	Copy	Edit	Delete
Custom Reports									
Audit logins	Logins to the Web console during the last month	7/3/2013	Admin	Run	Cached	Schedule	Copy	Edit	Delete
Audit Saved Sessions	Recorded sessions that were exported during the last year	7/3/2013	Admin	Run	Cached	Schedule	Copy	Edit	Delete
Audit Sessions	Recorded sessions during last month	7/3/2013	Admin	Run	Cached	Schedule	Copy	Edit	Delete
SAMPLE: Admin-related tasks - Past Week	Administrative-related tasks performed on monitored servers.	2/15/2013	admin	Run	Cached	Schedule	Copy	Edit	Delete
SAMPLE: Apps usage grouped by Server Name - Past Week	All apps used on monitored servers. Grouped by Server Name.	2/15/2013	admin	Run	Cached	Schedule	Copy	Edit	Delete
SAMPLE: Apps usage per Server grouped by App Name - Past Week	Report all apps used on the monitored servers. Grouped by App Name.	2/15/2013	admin	Run	Cached	Schedule	Copy	Edit	Delete
SAMPLE: Remote Desktop Sessions - Past Week	All Remote Desktop sessions initiated from monitored servers. Grouped by Window Title and Server Name.	2/15/2010	admin	Run	Cached	Schedule	Copy	Edit	Delete
SAMPLE: Sessions Comments Report - Past Day	New comments to sessions during the last 24 hours	4/22/2012	Admin	Run	Cached	Schedule	Copy	Edit	Delete

- 2) Click the **Create New Custom Report** button.

The report configuration wizard opens.



3) To specify the report type:

1. From the list on the left, select an option to specify the type of information on which to base the report: **Servers, Users, Applications, Commands, Comments, Messages, Tickets, Audit Sessions, Audit Logins, or Audit Saved Sessions.**
2. Select an option (on the right) to specify the platform/computers to focus on in the report: **Windows-based, Unix-based, or All computers.**

For purpose of this example, select **Servers** and **All computers**.

4) Click **Next**.

The resulting report is based on the type of report you selected. For example, choosing a **Servers** type report will focus the columns and column order on the "Servers" object.

5) In step 1 of the report configuration wizard, you can select the columns to display in the new report (specifying the **Server, Session, and User**). For example, select the **User Name, Domain Name, and Login Name** for the user, as well as the **Server Name, Session Start/End Date And Time, Slides Count, and Session Video** link. Other column types can be selected, if required.

- 6) When you have finished designing your report, click **Next**.

The screenshot shows the 'Reports' configuration wizard in ObserveIT. The left sidebar contains navigation links: 'Reports', 'Latest Activities', 'Installed Software', 'Server Software', 'Install/Uninstall', 'Sticky Notes', 'Latest Sessions', 'W2K8-S8-D02', 'Admini...', 'Quick Help', 'Installation Guide', 'User Guide', and 'Configuration Guide'. The main content area is titled 'Reports' and 'Report : Report Name'. It shows 'Step 1/4 - Column selection' with a 'Jump to Step' dropdown set to 'Select Columns'. Below this, it says 'Select the columns you wish to include in your report.' The columns are organized into three sections: 'Server', 'Session', and 'User'. Each section has a 'Check All - Clear All' link. The 'Server' section includes 'Server Name' (checked), 'Recording Status', 'Sessions Count' (checked), 'Operating System Name', 'Server Policy Name', 'Server Version' (checked), 'Server Last Activity Date' (checked), 'Installation Date', 'Server Policy ID', and 'Server ID'. The 'Session' section includes 'Is Session Alive', 'Session Start Date And Time', 'Session Video', 'Session End Date And Time', 'Machine Name', 'Session Start Date', 'Session Start Time', 'Client Name', 'Session End Time', 'Client IP Address', 'Slides Count', and 'Session End Date'. The 'User' section includes 'User Name', 'User Authentication', 'Login Name', 'Domain Name', and 'User Identity'. At the bottom right are 'Preview', 'Cancel', 'Next', and 'Save' buttons.

Note: You can always return to this step and add or remove columns, and gradually obtain the report that you need by using a trial and error process. Also, at any point you can cancel the process, or advance to a different step, without having to go through all the steps in chronological order.

- 7) In step 2 of the report configuration wizard, you can specify the way the report results will be grouped, by specifying the following fields:
- **Group By:** for example, **Session Start Date**, **Session End Date**, and then by **Server Name**,
 - **Sort Order:** for example, **Ascending**
 - **Group Dates By:** for example, by **Week**.

You can always return to this step and add or remove columns, and gradually get the report that you need using a trial and error process.

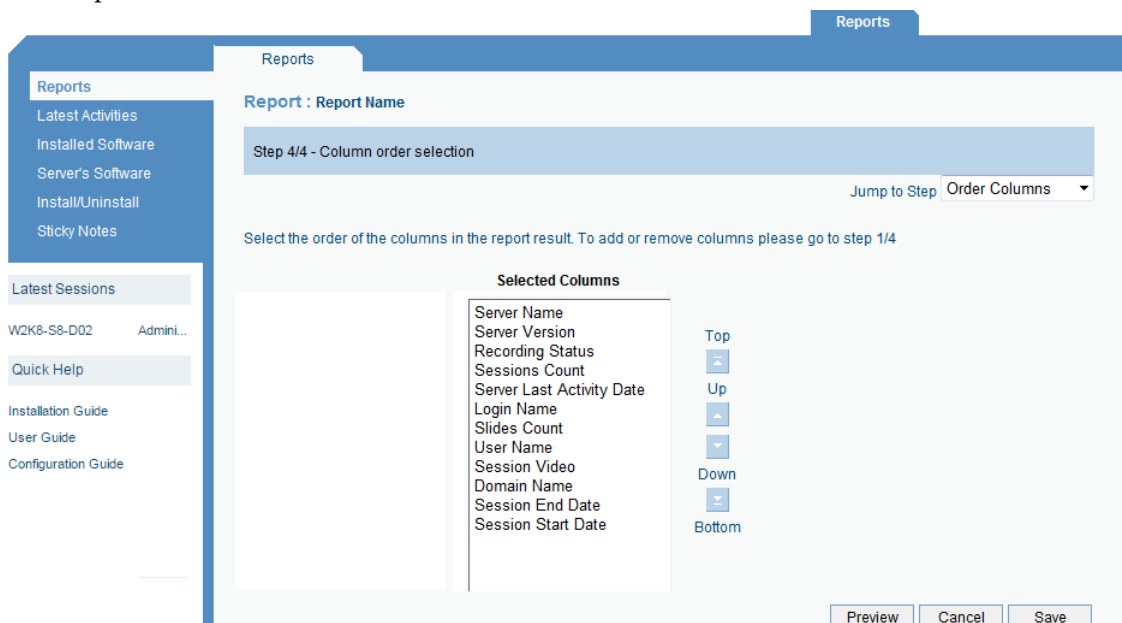
When finished, click **Next**.

- 8) In step 3 of the report configuration wizard, you can select a start and end date for the report. In this step, you can also define advanced filters by selecting any of the column items that you selected in Step 1, and display results that match, are equal/not equal to, or contain/not contain a specific string, and so on. For example, you may only want user names that include specific users, or Window Titles that only include specific words.

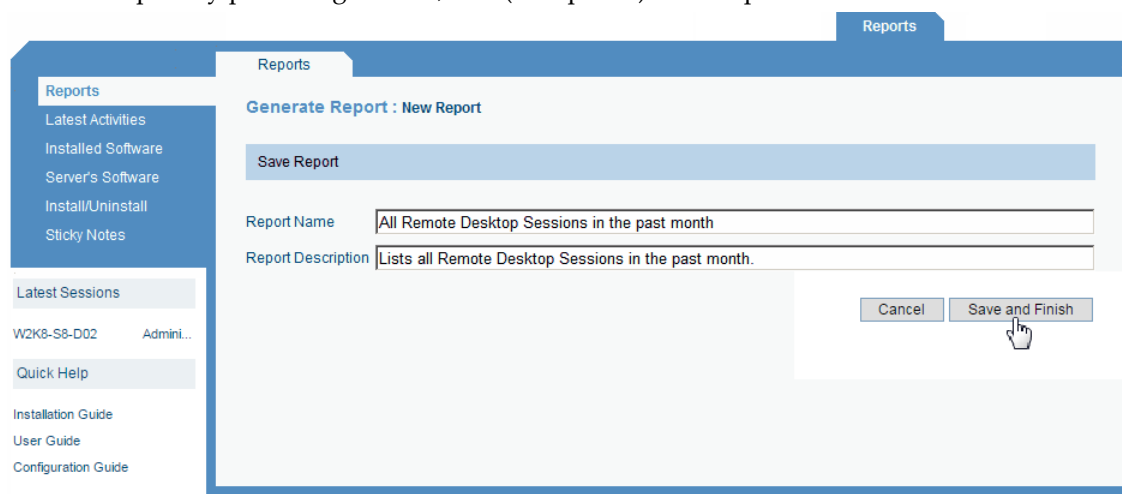
Note: Using the wildcard character "%" in the beginning of a filter phrase means that the filter will ignore anything before the text you used. Using the character "%" at the end of a filter phrase means that the filter will ignore anything after the text you have used. For example: %Remote% - will include results such as "Routing and Remote Access Server Setup Wizard", "Routing and Remote Access", "Remote Desktop Connection", and so on.

At this point, you may want to click the **Preview** button and view the results of the report, making modifications to the filter, as needed.

- 9) In step 4 of the report configuration wizard, you can choose the order of the columns and configure the appearance of the report. The list contains the same items that were selected in the first step.



- 10) Before saving the report, you can click the **Preview** button to view the results of the report, to make modifications to the filter, as needed. If required, you can go back to the first step and modify your settings. When finished, click the **Save** button.
- 11) Save the report by providing a name, and (if required) a description. Click **Save and Finish**.



- 12) In the **Reports** list, you can run the newly-created report, edit it, copy it to create a new report with the same settings (useful when you need to make a small change in the report but do not want to go through all the steps of creating it from scratch), or delete it.

Report List

Scheduled Reports for Console User:

Name	Description	Modified	User	
Custom Reports				
All Remote Desktop Sessions in the past month	Lists all Remote Desktop Sessions in the past month.	01/11/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: Admin-related tasks - Past Week	Administrative-related tasks performed on monitored servers.	28/10/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: App usage grouped by Server Name - Past Week	All apps used on monitored servers. Grouped by Server Name.	25/10/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: Apps usage per Server grouped by App Name - Past Week	Report all apps used on the monitored servers. Grouped by App Name.	25/10/09	admin	Run Cached Schedule Copy Edit Delete

Running Reports

When you run a report, the results are displayed in a separate webpage.

Note: Running a report might generate additional CPU and resource usage on the SQL server holding the ObserveIT database. To prevent this overhead while the server is working, try to run reports that will result in massive queries (such as in reports that span for a long period of time) during non-working hours. You can also view cached reports (that have been run previously).

To run a report

- 1) In the **Reports** tab, click the **Run** link next to the report you want to run.

Report List

Scheduled Reports for Console User:

Name	Description	Modified	User	
Custom Reports				
All Remote Desktop Sessions in the past month	Lists all Remote Desktop Sessions in the past month.	01/11/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: Admin-related tasks - Past Week	Administrative-related tasks performed on monitored servers.	28/10/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: App usage grouped by Server Name - Past Week	All apps used on monitored servers. Grouped by Server Name.	25/10/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: Apps usage per Server grouped by App Name - Past Week	Report all apps used on the monitored servers. Grouped by App Name.	25/10/09	admin	Run Cached Schedule Copy Edit Delete

- 2) Depending on the report type and group-by options used, you can click the **Show All Details** link to display an expanded version of the report, showing all the columns that were selected in the report creation steps.



Report Name: [All Remote Desktop Sessions in the past month](#)

Convert To: [Excel](#)

Filtered By:
Session Start DateTime Last 1 Month AND
Window Title contains Remote

[Show All Details](#) [Show Selected Details](#) [Hide Details](#)

Login Name	User Name	Domain Name	Window Title	Session Start Date	Session Start Time	Session End Time	Session Video
☐ Server Name: WIN2003-SRV1 (5 records)							
Administrator	n/a	WIN2003-SRV1	192.168.200.150 - Remote Desktop	11/01/2009	02:53PM	02:54PM	
Administrator	n/a	WIN2003-SRV1	Remote Desktop Connection	11/01/2009	02:16PM	02:38PM	
Administrator	n/a	WIN2003-SRV1	Remote Desktop Connection	11/01/2009	02:53PM	02:54PM	
Administrator	n/a	WIN2003-SRV1	Remote Shutdown Dialog	10/29/2009	04:32PM	04:32PM	
Administrator	n/a	WIN2003-SRV1	win2003-srv2 - Remote Desktop	11/01/2009	02:16PM	02:38PM	

Total: 5 records.

To help mitigate CPU and resource usage overhead, in some cases, when running reports that do not need to be current (such as a report showing all the user sessions in the previous month), you can view cached reports (instead of re-running the reports). The **Cached** link is enabled only for reports that have already been run previously.

To view cached reports

- In the **Report List**, click the **Cached** link next to the relevant report (that has already been run) to view the previous results for the report. If a report was never run before, the **Cached** link will be disabled.

Remember: You can always return to the reports creation wizard and add or remove columns, add or change sort-by options, add or change filters, and gradually generate the report you need by a trial and error process.

Scheduling Reports

Reports can be scheduled to run at specific intervals. This is useful when a report needs to be emailed to an administrator or security auditor.

Note: To schedule an email report, you must first configure the Console User with an SMTP email address. You must also configure the ObserveIT Web Console to use an SMTP server.

To schedule a report

- 1) In the **Report** tab, click the **Schedule** link next to the report that you want to schedule.

The screenshot shows the ObserveIT Reports interface. On the left is a sidebar with navigation links: Reports, Latest Activities, Installed Software, Server's Software, Install/Uninstall, Sticky Notes, Latest Sessions, MF-W8SQ8-1, Admini..., Quick Help, Installation Guide, Usage Guide, and Configuration Guide. The main content area is titled 'Report List' and contains a search bar for 'Scheduled Reports for Console User:' with a 'Go' button and a 'Create New Custom Report' button. Below this is a table of reports:

Name	Description	Modified	User	
Custom Reports				
All Remote Desktop Sessions in the past month	Lists all Remote Desktop Sessions in the past month.	01/11/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: Admin-related tasks - Past Week	Administrative-related tasks performed on monitored servers.	28/10/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: App usage grouped by Server Name - Past Week	All apps used on monitored servers. Grouped by Server Name.	25/10/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: Apps usage per Server grouped by App Name - Past Week	Report all apps used on the monitored servers. Grouped by App Name.	25/10/09	admin	Run Cached Schedule Copy Edit Delete

- 2) In the **Schedule Report** page, you can do the following:
 - Assign Console Users to receive the report results by email.

- Reports

In the **Email Report To** section in the **Contacts Userfield** type the relevant domain/username or

-



-

- 6) In the **Schedule Report** section, to schedule the report to run at a custom frequency or at a defined time range, select the radio button next to the required frequency (**Daily**, **Weekly**, **Monthly**).
- 7) To configure **Start/End Dates** for the scheduled report, select the start and end dates.
- 8) When finished, click **Save Schedule** (at the top of the page).

In the **Reports List**, a schedule icon appears next to the report's name.

To remove a schedule

- 1) In the **Reports List**, click the **Schedule** link next to the relevant report (marked by a schedule icon).
- 2) In the **Schedule Report** page of the selected report, click the **Remove Schedule** button (at the top of the page).

Editing Reports

ObserveIT's reports configuration wizard allows you to return to any step and add or remove columns, and thereby gradually obtain the report that you need by a trial and error process. Also, at any point you can cancel the process, or advance to a different step, without having to go through all the steps in chronological order.

To edit a report

- 1) In the **Reports** tab, click the **Edit** link next to the report that you want to edit.

The screenshot shows the ObserveIT Reports interface. On the left is a sidebar with navigation links: Reports, Latest Activities, Installed Software, Server's Software, Install/Uninstall, Sticky Notes, Latest Sessions, MF-W8SQ8-1 Admini..., Quick Help, Installation Guide, Usage Guide, and Configuration Guide. The main area is titled 'Reports' and contains a 'Report List' section. At the top of the Report List is a search bar for 'Scheduled Reports for Console User:' with a 'Go' button and a 'Create New Custom Report' button. Below this is a table with columns: Name, Description, Modified, and User. The table lists several reports, including 'All Remote Desktop Sessions in the past month', 'SAMPLE: Admin-related tasks - Past Week', 'SAMPLE: App usage grouped by Server Name - Past Week', and 'SAMPLE: Apps usage per Server grouped by App Name - Past Week'. Each report has a set of action links: Run, Cached, Schedule, Copy, Edit, and Delete. A mouse cursor is pointing at the 'Edit' link for the first report.

Name	Description	Modified	User	Run	Cached	Schedule	Copy	Edit	Delete
All Remote Desktop Sessions in the past month	Lists all Remote Desktop Sessions in the past month.	01/11/09	admin	Run	Cached	Schedule	Copy	Edit	Delete
SAMPLE: Admin-related tasks - Past Week	Administrative-related tasks performed on monitored servers.	28/10/09	admin	Run	Cached	Schedule	Copy	Edit	Delete
SAMPLE: App usage grouped by Server Name - Past Week	All apps used on monitored servers. Grouped by Server Name.	25/10/09	admin	Run	Cached	Schedule	Copy	Edit	Delete
SAMPLE: Apps usage per Server grouped by App Name - Past Week	Report all apps used on the monitored servers. Grouped by App Name.	25/10/09	admin	Run	Cached	Schedule	Copy	Edit	Delete

- 2) When editing a report you can freely move between the steps of the configuration wizard and make changes. For example, change the report from grouping by Server Name to grouping by Login Name.

Reports

Report : All Remote Desktop Sessions in the past month

Select the grouping for which you would like to calculate summary information - Step 2 of 4.

Jump to Step Select Grouping ▼

Select the way the report results will be grouped. You may choose up to 3 fields to group by.

Group By	Sort Order	Group Dates By
Login Name ▼	Ascending ▼	Week ▼
and then by	Sort Order	Group Dates By
None ▼	Ascending ▼	Week ▼
and then by	Sort Order	Group Dates By
None ▼	Ascending ▼	Date ▼

Preview Cancel Next Save

- 3) At this point, you can click the **Preview** button to view the results of the report, and make modifications to the filter, as required.
- 4) When finished making the changes, click **Save**.
The **Generate Report - Save Report** page opens.
- 5) In **Report Name**, type (or modify) the report name, as required.
- 6) In **Report Description**, type a description of the report (if needed).
- 7) Click **Save and Finish** to complete the process.

Deleting Reports

Custom reports can be deleted when the report is no longer needed.

Note: A custom report cannot be restored after it is deleted; built-in reports cannot be deleted.

Remember, you can always edit existing reports, so if you made a mistake when creating a custom report, you can always go back and edit it at any time.

No recorded data is lost when a report is deleted.

To delete a custom report

- 1) In the **Reports** tab, click the **Delete** link next the report that you want to delete.

The screenshot displays the 'Reports' tab of a software interface. On the left is a sidebar with a 'Reports' section containing links to 'Latest Activities', 'Installed Software', 'Server's Software', 'Install/Uninstall', and 'Sticky Notes'. Below this is a 'Latest Sessions' section with a link to 'MF-W8SQ8-1 Admini...'. The main content area is titled 'Report List' and features a search bar labeled 'Scheduled Reports for Console User:' with a 'Go' button. A 'Create New Custom Report' button is positioned below the search bar. A table lists reports with columns for Name, Description, Modified, and User. The reports include 'All Remote Desktop Sessions in the past month' and three sample reports. Each report has a row of action links: 'Run', 'Cached', 'Schedule', 'Copy', 'Edit', and 'Delete'. A mouse cursor is pointing at the 'Delete' link for the first report.

Name	Description	Modified	User	Actions
Custom Reports				
All Remote Desktop Sessions in the past month	Lists all Remote Desktop Sessions in the past month.	01/11/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: Admin-related tasks - Past Week	Administrative-related tasks performed on monitored servers.	28/10/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: App usage grouped by Server Name - Past Week	All apps used on monitored servers. Grouped by Server Name.	25/10/09	admin	Run Cached Schedule Copy Edit Delete
SAMPLE: Apps usage per Server grouped by App Name - Past Week	Report all apps used on the monitored servers. Grouped by App Name.	25/10/09	admin	Run Cached Schedule Copy Edit Delete

A message dialog box opens, prompting you to confirm.

- 2) Click **OK** to proceed.

The report is deleted.