Mitel MiContact Center Enterprise

OPEN APPLICATION SERVER – FAULT AND SECURITY MANAGEMENT USER GUIDE

Release 9.3

NOTICE

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.

No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

TRADEMARKS

The trademarks, service marks, logos and graphics (collectively "Trademarks") appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Open Application Server Fault and Security Management User Guide
Release 9.3 – February 2018

INTRODUCTION

The OAS event reporting function detects abnormal system occurrences and security audit information. These events (alarms) are stored in the Microsoft Windows Event Log as follows:

1. The OAS object reporting an alarm or security event sends the alarm/event to the Alarm Event Channel.

   The Alarm Service, which resides on the Basic Services host, reads the alarms and security events from the Alarm Event Channel and stores them in the Microsoft Windows Event Log. Events from OAS components are normally logged into the Event Log on the server running OAS Basic Services.

2. If the Alarm Event Channel is out of service, the alarms and security events are stored in the Microsoft Windows Event Log on the host of the OAS object reporting the event.

WHAT YOU WILL LEARN

This section describes the following topics:

- OAS alarms
- Security events
- Viewing and interpreting alarms and security events (via the Micro- soft Windows Event Viewer)
- Reading and analyzing alarms

In addition, the list of alarms and security events are provided in this section.

ABOUT ALARMS

Alarms can be in one of two states: raised or cleared.

- **Raised**: Abnormal behavior is detected and an alarm describing the behavior is logged. A severity level (error, warning, or information) is assigned to each raised alarm.
- **Cleared**: The condition that previously caused an alarm to be raised is no longer evident and another alarm describing this occurrence is logged.

ABOUT SECURITY

Security management:

- allows or denies user access to OAS. User authentication validates the user and user authorization grants an authenticated user access to predefined parts of OAS.
- provides a security audit trail. The audit trail provides information about logons, logoffs, and system component accesses.

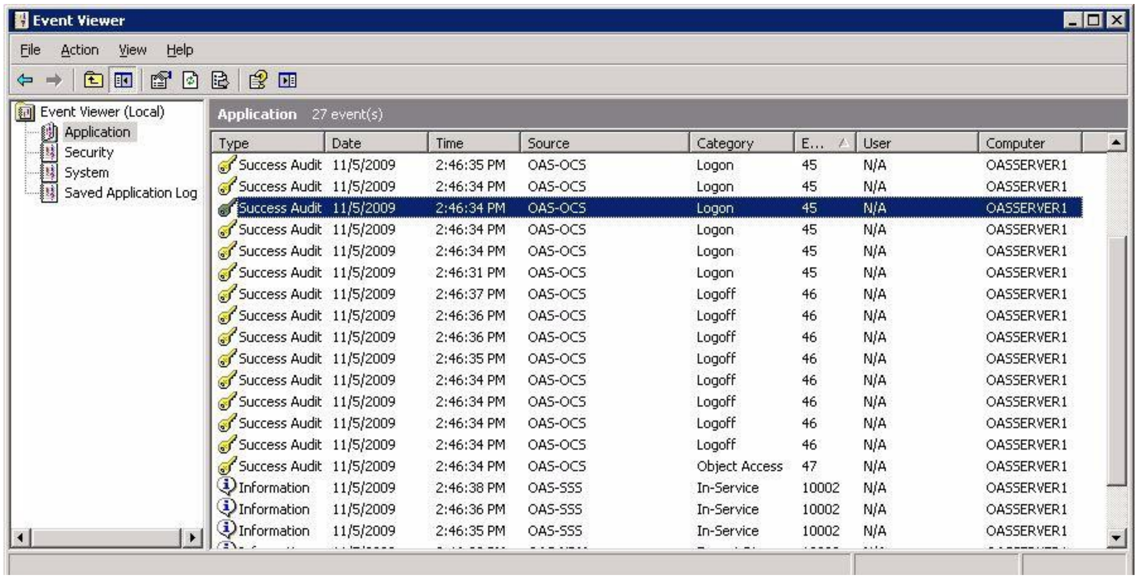
Users are assigned to Windows global user groups through the Windows Active Directory Users and Configuration Snap-in.

The global user group configured as the OAS Client Group in the OAS configuration database contains the users permitted to open a TSAPI stream with OAS. Before an OAS client application can connect to OAS, the user must be specified in the OAS Client Group.

The global group configured as the OAS Admin Group in the OAS configuration database contains the users permitted to work with the Management Console program. Before OAS can be configured, the user must be specified in the OAS Admin Group.

VIEWING AND INTERPRETING ALARMS AND SECURITY EVENTS

Using the Windows Event Viewer, you can view all the OAS alarms and security events or details about a specific alarm or security event. To view the OAS alarms and security events in the Windows Event Log, open the Windows Event Viewer and click Application Log from the tree. The Event Viewer automatically displays events as shown in the figure below. For details about the information provided in Windows Event Viewer, refer to the Online Help.

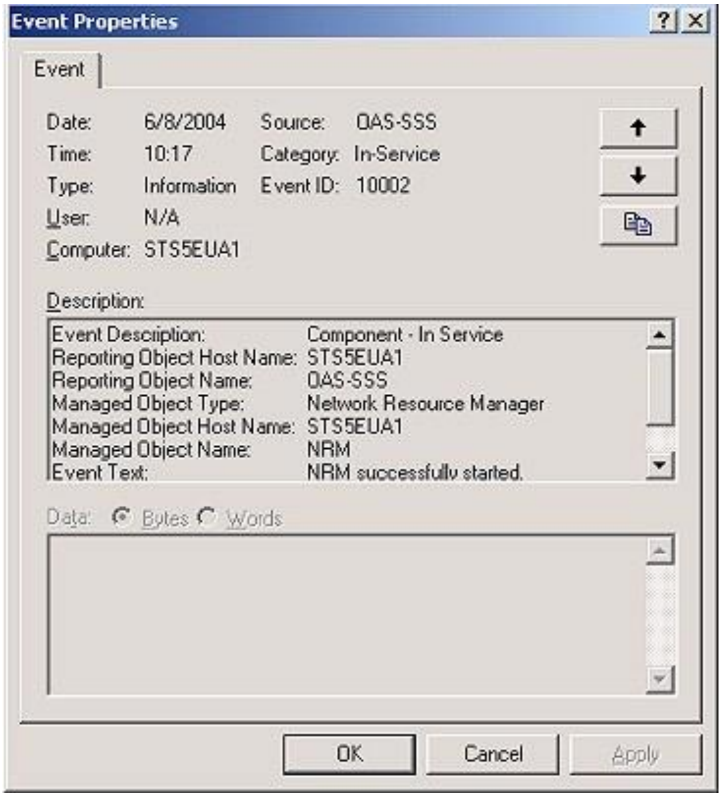


Type	Date	Time	Source	Category	E...	User	Computer
Success Audit	11/5/2009	2:46:35 PM	OAS-OCS	Logon	45	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:34 PM	OAS-OCS	Logon	45	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:34 PM	OAS-OCS	Logon	45	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:34 PM	OAS-OCS	Logon	45	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:34 PM	OAS-OCS	Logon	45	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:31 PM	OAS-OCS	Logon	45	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:37 PM	OAS-OCS	Logoff	46	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:36 PM	OAS-OCS	Logoff	46	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:36 PM	OAS-OCS	Logoff	46	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:35 PM	OAS-OCS	Logoff	46	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:34 PM	OAS-OCS	Logoff	46	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:34 PM	OAS-OCS	Logoff	46	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:34 PM	OAS-OCS	Logoff	46	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:34 PM	OAS-OCS	Logoff	46	N/A	OASSERVER1
Success Audit	11/5/2009	2:46:34 PM	OAS-OCS	Object Access	47	N/A	OASSERVER1
Information	11/5/2009	2:46:38 PM	OAS-SSS	In-Service	10002	N/A	OASSERVER1
Information	11/5/2009	2:46:36 PM	OAS-SSS	In-Service	10002	N/A	OASSERVER1
Information	11/5/2009	2:46:35 PM	OAS-SSS	In-Service	10002	N/A	OASSERVER1

VIEWING EVENT PROPERTIES

You can view more information about a selected alarm or security event in the Event Properties display. To view additional information about a specific alarm or security event:

1. Click the event in the Application Log.
2. On the **View** menu, select **Event Properties**.
   A sample Event Properties dialog is provided in the figure below.



Date: 6/8/2004
Time: 10:17
Type: Information
User: N/A
Computer: STS5EUA1
Source: OAS-SSS
Category: In-Service
Event ID: 10002

Description:

Event Description: Component - In Service
Reporting Object Host Name: STS5EUA1
Reporting Object Name: OAS-SSS
Managed Object Type: Network Resource Manager
Managed Object Host Name: STS5EUA1
Managed Object Name: NRM
Event Text: NRM successfully started.

READING AND ANALYZING ALARMS

When you read and analyze OAS alarms, it is important to note the following:

- A fault condition is currently active if an alarm describing the fault has been raised and the corresponding alarm has not been cleared.
- If an alarm is raised against a managed object that had previously raised an alarm as the reporting object, then the previously raised alarm will not clear.

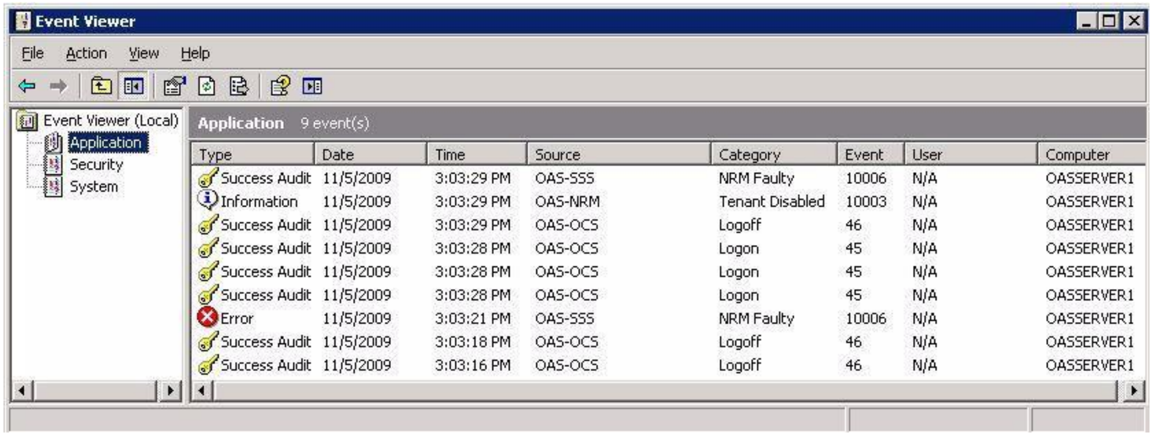
Following are two examples to consider when reading and analyzing alarms.

EXAMPLE

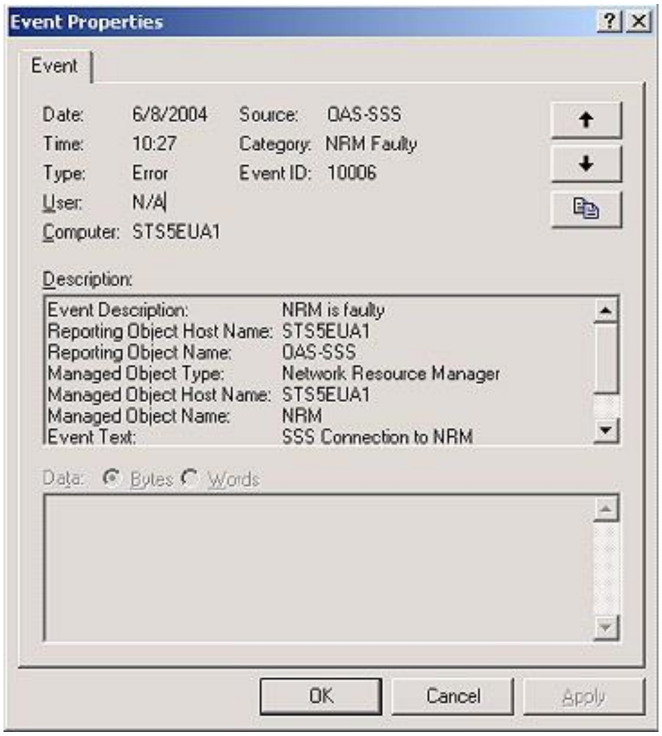
In the sample Event Viewer shown in Figure 3 below:

1. OAS-SSS raised an alarm for NRM faulty at 3:03:21 PM (Event ID: 10006)
2. OAS-SSS cleared the alarm at 3:03:29 PM through a Success Audit (Event ID: 10006)

Example Details about the events are provided in the Event Properties dialogs shown in the figures below.



Type	Date	Time	Source	Category	Event	User	Computer
Success Audit	11/5/2009	3:03:29 PM	OAS-SSS	NRM Faulty	10006	N/A	OASSERVER1
Information	11/5/2009	3:03:29 PM	OAS-NRM	Tenant Disabled	10003	N/A	OASSERVER1
Success Audit	11/5/2009	3:03:29 PM	OAS-OCS	Logoff	46	N/A	OASSERVER1
Success Audit	11/5/2009	3:03:28 PM	OAS-OCS	Logon	45	N/A	OASSERVER1
Success Audit	11/5/2009	3:03:28 PM	OAS-OCS	Logon	45	N/A	OASSERVER1
Success Audit	11/5/2009	3:03:28 PM	OAS-OCS	Logon	45	N/A	OASSERVER1
Error	11/5/2009	3:03:21 PM	OAS-SSS	NRM Faulty	10006	N/A	OASSERVER1
Success Audit	11/5/2009	3:03:18 PM	OAS-OCS	Logoff	46	N/A	OASSERVER1
Success Audit	11/5/2009	3:03:16 PM	OAS-OCS	Logoff	46	N/A	OASSERVER1

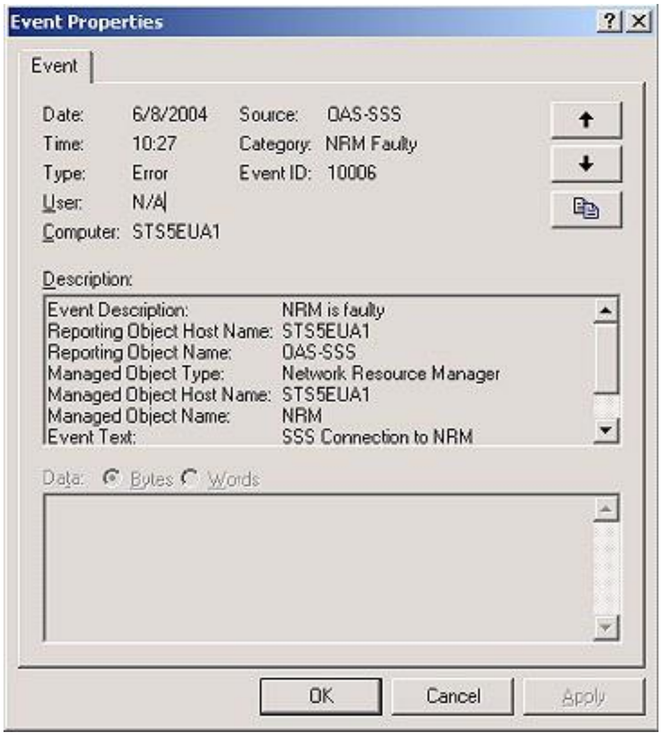


Date: 6/8/2004 Source: OAS-SSS
Time: 10:27 Category: NRM Faulty
Type: Error Event ID: 10006
User: N/A
Computer: STS5EUA1

Description:

Event Description:	NRM is faulty
Reporting Object Host Name:	STS5EUA1
Reporting Object Name:	OAS-SSS
Managed Object Type:	Network Resource Manager
Managed Object Host Name:	STS5EUA1
Managed Object Name:	NRM
Event Text:	SSS Connection to NRM

Data: ● Bytes ○ Words



Date: 6/8/2004 Source: OAS-SSS
Time: 10:27 Category: NRM Faulty
Type: Error Event ID: 10006
User: N/A
Computer: STS5EUA1

Description:

```
Event Description:          NRM is faulty
Reporting Object Host Name: STS5EUA1
Reporting Object Name:      OAS-SSS
Managed Object Type:        Network Resource Manager
Managed Object Host Name:   STS5EUA1
Managed Object Name:        NRM
Event Text:                 SSS Connection to NRM
```

LIST OF ALARMS AND SECURITY EVENTS

The following table specifies the OAS alarms. The alarms are grouped alphabetically by the severity of the raised alarm (Type): Error, Warning, and Information.

EVENT	SOURCE	REPORTING OBJECT HOST NAME	REPORTING OBJECT NAME	MANAGED OBJECT TYPE	MANAGED OBJECT HOST NAME	MANAGED OBJECT NAME	SYSTEM ACTION
Error alarms (Raised and Cleared)							
Alarm Service Faulty	SSS	Host	OAS-SSS	Alarm Service	Host	AS	Automatically restarted
Connections to MX-ONE Faulty	AppLink	Host	Call Control Server	MX-ONE	---	Call Control Server name	Automatically reconnected
AppLink faulty	SSS	Host	---	AppLink	Host	Call Control Server name	Automatically restarted
Connection to AppLink Server Faulty	NRM	Host	---	Media Server	---	Call Control Server name	Automatically reconnected

EVENT	SOURCE	REPORTING OBJECT HOST NAME	REPORTING OBJECT NAME	MANAGED OBJECT TYPE	MANAGED OBJECT HOST NAME	MANAGED OBJECT NAME	SYSTEM ACTION
Connection to Configuration Service Faulty	SSS	Host	OAS_SSS	OCS	Host	OCS	None
Connection to Media Server Faulty	NRM	Host	---	Media Server	---	Media Server name	Automatically reconnected
Connection to SQL Server Faulty	PDC	Host	---	SQL Server	Host	---	Automatically reconnected
Logical Device Fault	AppLink	Host	Call Control Server	Logical Device	---	Call Control Server name	None
Media Server Faulty	SSS	Host	OAS_SSS	Media Server	Host	Media Server name	Automatically restarted
NRM Faulty	SSS	Host	OAS_SSS	NRM	Host	Media Server name	Automatically restarted
No Media Services Available	NRM	—	CTI Server	Media Server	—	Media Server name	Automatically reconnected
Trace Service Faulty	SSS	Host	OAS-SSS	Trace Service	Host	OTS	Automatically restarted
PDC Faulty	SSS	Host	OAS-SSS	PDC	Host	PDS	Automatically restarted
Physical Device Faulty	AppLink	Host	Call Control	Physical Device	—	Call Control Server name, Device Identifier	None
Virtual Device Faulty	NRM	Host	Server	Virtual Device	—	Device identifier	Automatically restarted
Aastra Daemon not available	SSS	Host	—	Daemon	Host	Aastra	Automatically restarted
License Fault	NRM	Host	OAS-SSS	Network Resource Manager	Host	Daemon	None

EVENT	SOURCE	REPORTING OBJECT HOST NAME	REPORTING OBJECT NAME	MANAGED OBJECT TYPE	MANAGED OBJECT HOST NAME	MANAGED OBJECT NAME	SYSTEM ACTION
Warning Alarms (Raised and Cleared)							
Applink	Connection to Config. Service Faulty	Host	CTI Server	Config. Service	Host		Automatically reconnected
	Host	Call Control Server				OCS	
Media Server	---	CTI Server					
NRM	Host PDC	Host	—				
SSS	Host	OAS-SSS					
Connection to Event Channel Service Faulty	AppLink	Host	Call Control Server	Event Channel Service	Host	Event Channel	Automatically reconnected
Media Server	— NRM	Media Server Host	—				
PDC	Host	—					
SSS	Host	—					
Tenant authentication failure	NRM	Host	NRM	Network Resource Monitor	Host	—	None
Information Alarms (Never Cleared)							
In Service	SSS	Host	OAS-SSS	Alarm Service	Host	AS	None
				AppLink	Call Control Server Name	None	
				Media Server	Media Server Name	None	
				NRM	NRM	None	

EVENT	SOURCE	REPORTING OBJECT HOST NAME	REPORTING OBJECT NAME	MANAGED OBJECT TYPE	MANAGED OBJECT HOST NAME	MANAGED OBJECT NAME	SYSTEM ACTION
				Trace Service		OTS	None
				PDC		PDS	None
Out of Service	SSS	Host	OAS-SSS	Alarm Service	Host	AS	None
				AppLink	Call Control Server Name	Call Control Server Name	
				Media Server	Media Server Name	None	
				NRM		Media Server Name	None
				Trace Service		OTS	None
				PDC		PDS	None

The following table describes the OAS security events:

EVENT DESCRIPTION	CLASSIFICATION	SOURCE	REPORTING OBJECT HOST NAME	TYPE
Logoff	Platform Management	NRM OCS	Host	Success Audit
Logon Authentication	Platform Management	NRM OCS	Host	Success Audit, Failure Audit
Object Access	Read/Write	OCS	Host	Success Audit, Failure Audit