Security Audit Log

Last Modified on 18/04/2019 10:15 am AEST

A security audit log is a tamper resistant record of security sensitive occurrences that affect a system. It is used as a deterrent to prevent administrators maliciously or accidentally abusing their privileges when they otherwise have few restrictions. It can also be used to detect malicious activity (e.g. use of a compromised account).

Unlike the existing Event Log, the audit log is mainly aimed for administrators and their auditors.

Security Audit Log Settings

This page is about viewing or configuring the security audit log.

To view or edit Security Audit Log settings:

- 1. Select Application Menu. The menu appears with available applications.
- 2. Select Administration. The application displays at the landing page.
- 3. In the Left Navigation Area, select **Security**. The Security expands to display list.
- 4. Select Security Audit Log Settings. The existing Security Audit Log Settings display.
- 5. Select **Edit** and configure the following fields as required:
 - **Maximum audit log entries** Type the maximum number of audit log entries. There is a minimum value of 1 and a maximum value of 10,000
 - **Minimum severity** Type the minimum message severity to log to the audit log
- 6. Screenshot: View security audit log setting

Security	Audit Log Settings			
Name :	Security Audit Log Settings			
Description :	The security audit log settings a configured by the tenant.			
AUDIT LOG SETTINGS DETAILS				
Maximum audit log entri	10,000			
Minimum severity :	Information			

7. Select **Save** at the top right corner.

Viewing Security Audit Log

To view Security Audit log:

- 1. Select Application Menu. The menu appears with available applications.
- 2. Select Administration. The application displays at the landing page.
- 3. In the Left Navigation Area, select **Security**. The Security expands to display list.
- 4. Select Security Audit Log. The Security Audit Log displays.

Screenshot: View security audit log

Thumboal Sizes					
Conditional Format Ic	Security Audit	Log			
Text Field Patterns	б - астюн -				T Search
	Audit log entry created date	Severity	Mecage	Saccess	User
Themes	11/20/2016 1.00 PM	Information	Legos, Dar name onadmin, Dar agent Mozilla/53 (Windows NT 13.0; WOW6); vr.503] Secko(2010101 Finifax/503).	Yes	enadmin
escurces -	11/25/2516 1048 AM	Information	Logon. User neme: tg.admin. User agent: Mobile '10 Windows NT 100; Win64: eMJ AppleWebRit 537.06 (OHTML, No. Gooks) Overnet 54.0.2940.09 Safet/157.06.	Yes	tgudmin
	11/28/2916 16/06 AM	Information	Legon, ther name tgadmin, theragent Multile/50 (Windows NT 103) Winds of) AppletMeR0(517.36 (OTTM), like Gecks) Chemro(56.5.2882)H Salas/517.36.	Yes	tgadein
ioutity "	11/35/2016 10:05 AM	Warning	Legon, Dar name: Admin, Dar agent: Mozilla/53 (Windows NT 152); WindA 369 AppleWebR0/557.38 (OPTML, Bia Gecks) Chrome/54.02840.99 Safer/537.38.	No	Administrator
Identity Providers	11/28/2816 16/02 AM	Information	Legon. User name snadmin. User agent Moolla/3-3 (Windows NII 13.0; WOM60; re30-3] Sector/2010101 Forfex/30.3.	Yes	snadmin
Identity Providers	11/20/2016/0:29 AM	Information	Legon, Dier name: sn.admin, Dier agent: Mozilla/5.0 (Windows NF 10.0; WOW69; vr.50.0] Gecko(2010)101 Findta/50.0.	Yes	studmin
Rissword Policy	11/21/2016 1/26 PM	Information	Legen. User name on admin. User agent: Mocilla/3-0 OVindovo NIT 10.0; WOVI64 AppleVieb/04/357.36 (04TML, like Decks): Chrome/340.2880.89 Safari/357.36.	Ye	anadmin
	11/21/2016 1/25 PM	Information	Legon, Daw names snadmin, Daw agent Mozilla/53 (Windows NF 10.0; WOW50; rv:503) Sector(2010)101 Finifax/503.	Yes	studnin
Security Audit Log Set	11/21/2016 1/25 PM	Information	Logon. User name: on admin. User agent: Mocilla/3/J (Windows NT 193); WOWSK rv:00/J Gecko/2010101 Findex/30/J.	Yes	anadmin
Security Audit Log 🧭	11/21/2016 1.22 PM	Information	Legon, ther names stradinist. User agent Missila/5.0 (Westows NT 10.0; WOW60; redS03) Sector/2010101 Feefax/503.	Yes	anadmin
security restricting 2	11/15/2516 2:00 PM	Information	Belete access rule. Subject name: Students, Secured type: Qualifications, Authorization report.	Yes	anadmin
User Accounts	11/18/2016 2:07 PM	Information	Change access rule permissions. Subject name Students, Secured type Qualifications, Authorisation reports, Old permissions Read, New permissions Read.	Yes	snadmin
	11/10/2016 2:07 PM	Information	Create access rule, Subject name, Students, Secured type, Qualifications.	Yes	anadmin
User Rales	11/18/2016 2:06 PM	Information	Change access rule permissions. Subject name Students, Secured type Qualifications, Authorization reports, Old permissions Read, New permissions Read.	Ye	snadmin
exection -	11/10/2016 2:06 PM	Information	Create access rule, Subject name, Budents, Secured type: Qualifications.	Yes	studmin
	11/15/2016 2:06 PM	Information	Delete access rule. Subject name: Studients, Secured type: Student, Authorization report: -	Yes	anadmin
AP6	11/18/2016 2:05 PM	Information	Change access rule permissions, Subject name Students, Secured type Student, Authorization reports, Old permissions: Real, New permissions: Real,	Yes	studenie
Sh All feet	Information	Create access rule. Subject name: Students, Secured type: Student.	Yes	anadmin	
	Information	Legen. Der name snadmin. Der agent Moolla/3-0 (Windows NF 13.0; WOM60 AppleMeldG/507.36 (04TM), Die Sector) Chrome/54.0.2003/9 Safar/507.36.	Yes	stadmin	
Import Spreadsheet	11/6/2016 3:40 PM	Warning	Legon, Dar name tgosain, Dar agent Musilia/SJ (Windows NT ILD) Wind4 x64 Appl/WabK0/SST.36 (01/TML; Bia Gaola) Chrome/S4.0.204L71 Safari/SST.36	No	Administrator
	11/6/2016 3:40 PM	Marring	Legen. User name typosis. User agent Medila/SJI Olivelova NT 152; Wedd, x64; AppleWeb60/SJI.36 (0HTM), like Geola) Chrome/S40,2843.17 Selar/SJI.36	Ne	Administrator
Import Runs	11/4/2016 1:53 PM	Information	Create user account, User names John Smith.	Yes	studmin
	11/4/2016 1:07 PM	Information	Legon, User name: an admin, User agent: Mocilla/3.0 (Westows NT 13.0; WOWSR: no40.0) Gentes/2010110 Findres/40.0.	Yes	an admin
Scheduled Import 114(021612/02 PM Inform	Information	Legon, Daw names snadmin, Daw agent Mozilla/52 (Windows NF 12.0; WOW60; rodb2) Sector/2010101 Findus/49.0.	Yes	studenin	
- 6000	134/2006 1345 AM	Information	Legon, Der name: an admin. Uber apert: Mopila/3d (Windows NIT 13.0: WOWSK rov80d) Gecks (2010)10 Findex-40.0.	Yes	madmin

- The entries are sorted by Date Time by default with most recent events first
- Custom formatting shows error entries in red and warnings in yellow
- Customers can use the export feature to get a downloadable copy
- Auditors can periodically download the audit log and clear it

Security Audit Log Messages

The following security events are captured in the security audit log. Messages include whether the event was successful, or failed, along with relevant details.

Record change events can be logged using Record Auditing, not security audit messages.

Security Event	Notes
User account creation	
User account deletion	
User account rename	
User account expiry	This is logged at the first attempt to use the expired account, not the actual time of expiry.
User account password change	

StatusChange of user account statusLogged when a user has too many incorrect attempts.LogonVotall logoffs may be audited, since a user may not explicitly log off.User role creationVotall logoffs may be audited, since a user may not explicitly log off.User role deletionVotall votall logoffs may be audited, since a user may not explicitly log off.User role renameVotall votall logoffs may be audited, since a user may not explicitly log off.User role renameVotall votall logoffs may be audited, since a user may not explicitly log off.User role renameVotall votall logoffs may be audited, since a user may not explicitly log off.User role renameVotall votall logoffs may be audited, since a user may not explicitly log off.User role renameVotall votall logoffsUser role renameVotall votall logoffsUser role renameVotall votall logoffsApplication creationVotall logoffsApplication deploymentVotall logoffsApplication publishVotall logoffsAccess rule creationVotall logoffsAccess rule query changeVotall logoffsAccess rule permission changeVotall logoffsAccess rule permissionVotall logoffsAccess rule permissionVotall logoffsAccess rule permissionVotall logoffs	Change user account อิรอเหล่ะเอลิvent	Notes
LogonLogoffNatal logoffs may be audited, since a user may not splicitly log off.User role creation-User role rename-User role rename-Sargen and splication creation-Application deletion-Application deletion-Application deletion-Application deletion-Application deletion-Application deletion-Application deletion-Application publish-Access rule creation-Access rule query change-Access rule query change-Access rule query change-Access rule permission-		
LogoffNotal logoffs may be audited, since a user may not explicitly log off.User role creationUser role deletionUser role renameUser role membership changeApplication creationApplication deletionApplication deletionApplication deletionApplication deletionApplication deletionApplication deletionApplication deletionApplication deletionApplication deletionAccess rule creationAccess rule enablingAccess rule query changeAccess rule permission	Locked user account	Logged when a user has too many incorrect attempts.
Logortexplicitly log off.User role creation	Logon	
User role deletion User role rename User role membership change Application creation Application deletion Application deletion Application publish Password policy change Access rule creation Access rule query change Access rule permission	Logoff	
User role rename User role membership change Application creation Application deletion Application deployment Application publish Password policy change Access rule creation Access rule enabling Access rule query change	User role creation	
User role membership change Application creation Application deletion Application deployment Application publish Password policy change Access rule creation Access rule enabling Access rule query change	User role deletion	
change Application creation Application deletion Application deployment Application publish Password policy change Access rule creation Access rule query change Access rule query change	User role rename	
Application deletionApplication deploymentApplication publishPassword policy changeAccess rule creationAccess rule enablingAccess rule query changeAccess rule permission		
Application deploymentApplication publishPassword policy changeAccess rule creationAccess rule enablingAccess rule query changeAccess rule permission	Application creation	
Application publishPassword policy changeAccess rule creationAccess rule enablingAccess rule query changeAccess rule permission	Application deletion	
Password policy change Access rule creation Access rule enabling Access rule query change Access rule permission	Application deployment	
Access rule creation Access rule enabling Access rule query change Access rule permission	Application publish	
Access rule enabling Access rule query change Access rule permission	Password policy change	
Access rule query change Access rule permission	Access rule creation	
Access rule permission	Access rule enabling	
	Access rule query change	
Access rule deletion	Access rule deletion	
Tenant rollback	Tenant rollback	