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).

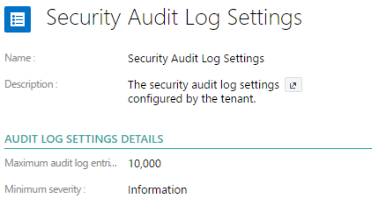
Unlike the existing Event Log , the audit log is mainly aimed for administrators and their auditors.

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 configured by the tenant.

AUDIT LOG SETTINGS DETAILS

Maximum audit log entri...	10,000
Minimum severity :	Information

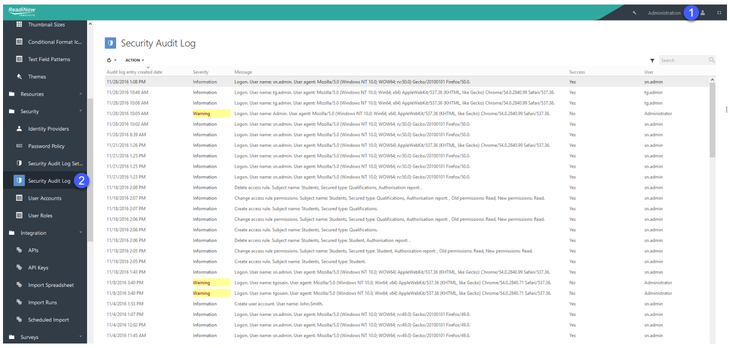
7. Select **Save** at the top right corner.

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



Security Audit Log

Audit log entry created date	Severity	Message	Success	User
11/28/2016 1:08 PM	Information	Logon. User name: sn.admin. User agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0.	Yes	sn.admin
11/28/2016 10:48 AM	Information	Logon. User name: tg.admin. User agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36.	Yes	tg.admin
11/28/2016 10:06 AM	Information	Logon. User name: tg.admin. User agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36.	Yes	tg.admin
11/28/2016 10:05 AM	Warning	Logon. User name: Admin. User agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36.	No	Administrator
11/28/2016 10:02 AM	Information	Logon. User name: sn.admin. User agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0.	Yes	sn.admin
11/28/2016 8:39 AM	Information	Logon. User name: sn.admin. User agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0.	Yes	sn.admin
11/21/2016 1:26 PM	Information	Logon. User name: sn.admin. User agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36.	Yes	sn.admin
11/21/2016 1:25 PM	Information	Logon. User name: sn.admin. User agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0.	Yes	sn.admin
11/21/2016 1:25 PM	Information	Logon. User name: sn.admin. User agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0.	Yes	sn.admin
11/21/2016 1:23 PM	Information	Logon. User name: sn.admin. User agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0.	Yes	sn.admin
11/18/2016 2:08 PM	Information	Delete access rule. Subject name: Students, Secured type: Qualifications, Authorisation report: .	Yes	sn.admin
11/18/2016 2:07 PM	Information	Change access rule permissions. Subject name: Students, Secured type: Qualifications, Authorisation report: , Old permissions: Read, New permissions: Read.	Yes	sn.admin
11/18/2016 2:07 PM	Information	Create access rule. Subject name: Students, Secured type: Qualifications.	Yes	sn.admin
11/18/2016 2:06 PM	Information	Change access rule permissions. Subject name: Students, Secured type: Qualifications, Authorisation report: , Old permissions: Read, New permissions: Read.	Yes	sn.admin
11/18/2016 2:06 PM	Information	Create access rule. Subject name: Students, Secured type: Qualifications.	Yes	sn.admin
11/18/2016 2:06 PM	Information	Delete access rule. Subject name: Students, Secured type: Student, Authorisation report: .	Yes	sn.admin
11/18/2016 2:05 PM	Information	Change access rule permissions. Subject name: Students, Secured type: Student, Authorisation report: , Old permissions: Read, New permissions: Read.	Yes	sn.admin
11/18/2016 2:05 PM	Information	Create access rule. Subject name: Students, Secured type: Student.	Yes	sn.admin
11/18/2016 1:43 PM	Information	Logon. User name: sn.admin. User agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.99 Safari/537.36.	Yes	sn.admin
11/8/2016 3:40 PM	Warning	Logon. User name: tgosain. User agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.71 Safari/537.36.	No	Administrator
11/8/2016 3:40 PM	Warning	Logon. User name: tgosain. User agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/54.0.2840.71 Safari/537.36.	No	Administrator
11/4/2016 1:53 PM	Information	Create user account. User name: John.Smith.	Yes	sn.admin
11/4/2016 1:07 PM	Information	Logon. User name: sn.admin. User agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0.	Yes	sn.admin
11/4/2016 12:02 PM	Information	Logon. User name: sn.admin. User agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0.	Yes	sn.admin
11/4/2016 11:45 AM	Information	Logon. User name: sn.admin. User agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0.	Yes	sn.admin

- 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	

Security Event	Notes
Change user account expiration	
Change of user account status	
Locked user account	Logged when a user has too many incorrect attempts.
Logon	
Logoff	Not all logoffs may be audited, since a user may not explicitly log off.
User role creation	
User role deletion	
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	
Access rule permission change	
Access rule deletion	
Tenant rollback	