

Log how to guide

Contents

- 1 Overview
- 2 Prerequisites
- 3 Swivel XML Logs
 - ◆ 3.1 Swivel Log Locations
 - ◆ 3.2 Swivel Log Settings version 3.9 and later
 - ◆ 3.3 Swivel Log Settings version 3.8 and earlier
 - ◆ 3.4 RADIUS Debug Log Settings
 - ◆ 3.5 Viewing PINsafe log Files
- 4 Swivel Syslog
 - ◆ 4.1 Syslog Settings
- 5 Swivel email alerting
- 6 Testing
- 7 Known Issues
- 8 Troubleshooting

Overview

By default Swivel logs all activity, with additional logging on Swivel appliances. This article covers Swivel logging and the options available.

Prerequisites

Swivel 3.x

Swivel XML Logs

Swivel logs data within each individual instance of Swivel. To consolidate logs from several instances of Swivel then [Syslog](#) or other log tool such as [Splunk](#) or [Sawmill](#) should be used.

Swivel Log Locations

The following article covers the log file locations and how to access the logs: [Support logs](#)

Swivel Log Settings version 3.9 and later

Level: Default: Info, options Off, Info, Warning, Error, Fatal. The lowest level of logging is Off and the highest level is Info, with decreasing log level from Warning to Error to Fatal. Each level of logging includes the level of logging above it, with the exception of OFF.

Max. single file size (KB): Default: 256. The size in KB of each log file. Care must be taken when increasing the size as a large amount of log data can cause partitions to fill up. On Swivel appliances the log data is backed up daily, and may result in large amounts of log data being backed up.

Compress log files after # days: Default: 7, compress the log files after the given number of days. If set to 0 the log files will never be compressed.

Delete log files after # days: Default: 180, automatically delete the log files after the given number of days. If set to 0 the logs will never be deleted, possibly filling the disk space.

Tidy log file schedule: Every at : Default: daily at 00:21, Specifies when the service that tidies up log files will be run. Files are tidied according to the settings above. Files older than the specified times will be compressed or deleted. Turning this option off (by setting the schedule to Never), log files will never be deleted.

Debug enabled: If enabled this logs data to the debug.log file.

Swivel Log Settings version 3.8 and earlier

The log settings are configured from the Swivel administration console under Logging/XML. The following options are available:

Level: Default: Info, options Off, Info, Warning, Error, Fatal. The lowest level of logging is Off and the highest level is Info, with decreasing log level from Warning to Error to Fatal. Each level of logging includes the level of logging above it, with the exception of OFF.

Filesize (KB): Default: 256. The size in KB of each log file. Care must be taken when increasing the size as a large amount of log data can cause partitions to fill up. On Swivel appliances the log data is backed up daily, and may result in large amounts of log data being backed up.

File count: The number of log files to be kept. Older logs are rotated out and deleted. Care must be taken when increasing the size as a large amount of log data can cause partitions to fill up. On PINsafe appliances the log data is backed up daily, and may result in large amounts of log data being backed up. Also the files are renamed each time a new log file is created the older log files are renamed. PINsafe 3.9 uses a date stamp for the file name and files do not need to be renamed.

Debug enabled: If enabled this logs data to the debug.log file.

RADIUS Debug Log Settings

These are enabled under from the Swivel administration console under RADIUS/Server. However you also need to enable debugging under Logging/XML as described above.

The location of the RADIUS debug log is:

/usr/local/tomcat/webapps/pinsafe/WEB-INF/logs/debug.log

Viewing PINsafe log Files

Log files may be viewed in the Swivel Administration Console.

A Windows utility to view Swivel log files is also available, see the [Log Viewer Application](#)

Swivel Syslog

Syslog allows consolidation of several logs into one place and with additional tools can be used for security to provide a tamper proof record.

Syslog Settings

Syslog settings

Host: Default: blank. The IP address/hostname of the syslog server.


Level: Default: Off. The level of PINsafe logging see description above for details.

Facility: Default local0. The log type to use. Leave as the default for PINsafe logs.


Syslog Example

Logging>Syslog


Please enter the details of an external syslog server to which PINsafe logging events should be delivered.

Syslogs: 

Host:	<input type="text" value="127.0.0.1"/>	
Level:	<input type="text" value="Info"/>	
Facility:	<input type="text" value="kern"/>	<input type="button" value="Delete"/>



Host:	<input type="text" value="192.168.9.157"/>	
Level:	<input type="text" value="Info"/>	
Facility:	<input type="text" value="kern"/>	<input type="button" value="Delete"/>

 [New Entry](#)

Syslog Example output

Events

EventIdx	Facility	Severity	Message
749	0	4	org.quartz.SchedulerException: The Scheduler has been shutdown.
715	0	6	PINsafe(Thread-45): INFO - The RADIUS server is shutting down
713	0	6	PINsafe(Thread-45): INFO - Shutdown started.
711	0	4	PINsafe[http-8080-1]: WARN 127.0.0.1 admin - Failed to login user admin, error: The user does not have any sec
709	0	6	PINsafe[http-8080-1]: INFO 127.0.0.1 admin - Failed to start a single channel session, error: The user account is l
707	0	4	PINsafe[http-8080-1]: WARN 127.0.0.1 admin - Failed to login user admin, error: The user does not have any sec
705	0	6	PINsafe[http-8080-1]: INFO 127.0.0.1 admin - Failed to start a single channel session, error: The user account is l

Event detail

Event ID : TimeStamp : Host name : Host IP :

Facility : Severity :

Swivel email alerting

Swivel can send an email on triggering certain events. In addition the fail over of the VIP can be configured to send email alerts, see [VIP on PINsafe Appliances](#).

The Swivel application supports the following email alerting:

- Account is locked
- Swivel email trigger for the following levels: Fatal, Error, Warning, Info
- Account creation audit
- User authenticated

Testing

Known Issues

Swivel 3.10.4 contains some fixes for previous versions where gaps may appear in the logs.

Increasing log files size may fill disk partitions and should be checked.

Increasing log file count fill disk partitions and versions prior to Swivel 3.9 may impact performance when they are renamed during file rotation.

Version 3.9 to 3.9.7, the compressed log files are deleted the day after they are compressed. To avoid this, set the log file compression to 0 so that they are never compressed.

Troubleshooting

The index file (.idx) controls the log entries. If any data is missing from the log file it may be possible to recreate the log index. Backup any of the files ending in .idx and then remove them from the log folder. This will cause a new index to be recreated. If the log files are often having to be reindexed, try setting a larger log size as this may mean that new log files are created less often.

Appliances, Swivel 3.9 onwards: /home/swivel/.swivel/log

If there are issues with the Swivel logs disappearing, try changing the log size from 256 to 257 Kb.