Splunk

Contents

Introduction

This document outlines how to integrate Splunk with Swivel by using Syslog and/or PINsafe log files. The integration requires the PINsafe server to write log files to a location that can be read by the Splunk server.

Requirements

Swivel, running version 3.2 or later. (This article is based on Version 3.6 running on Windows XP)

Splunk server, (This article was based on Splunk running on Windows XP)

Installation

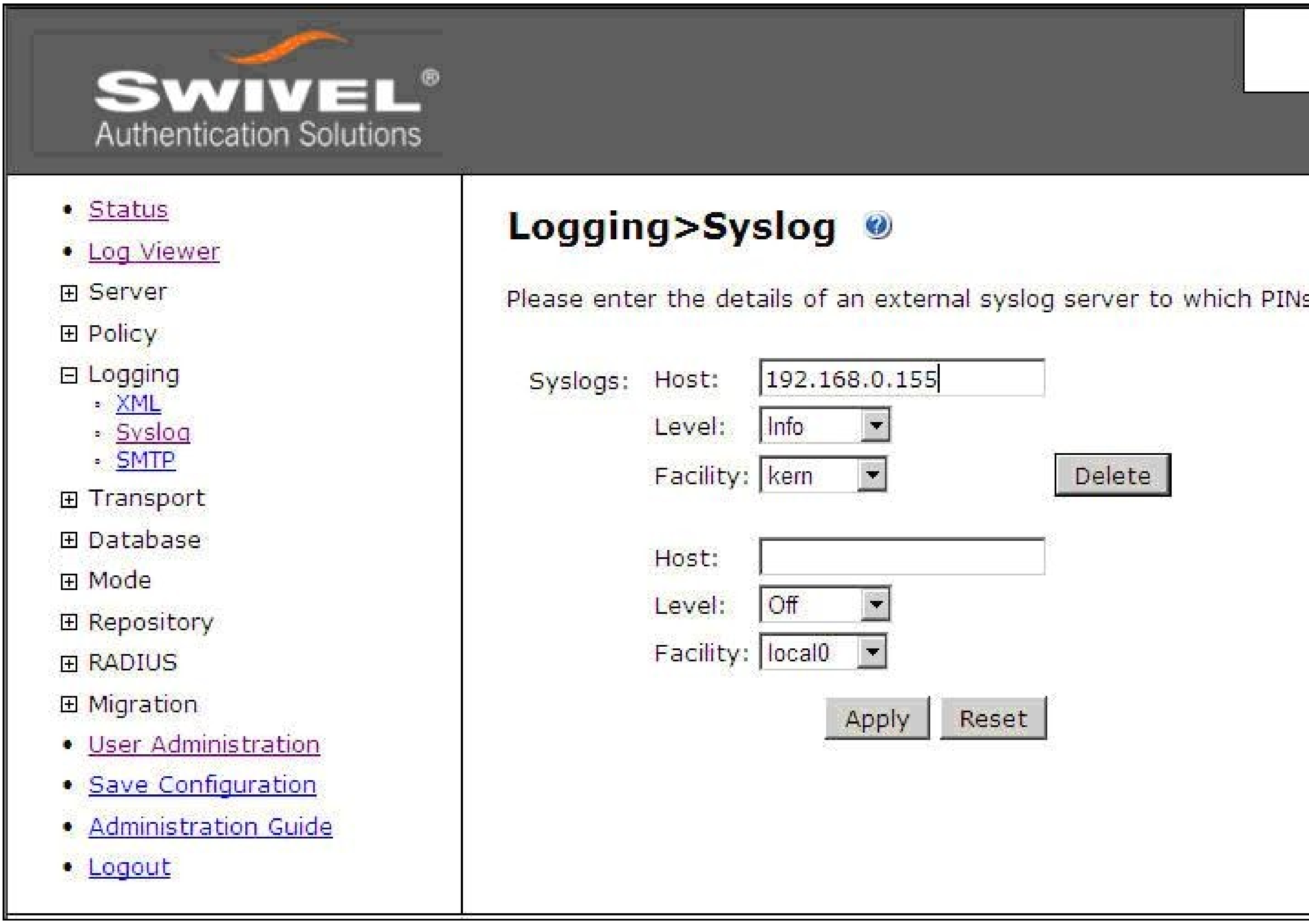
On the Swivel Administration Console, configure PINsafe to send syslog information to the Splunk server by selecting Logging/Syslog.

Enter the following information

Host: Hostname or IP address of the Splunk server

Level: The level of log information to be sent

Facility: The syslog facility in which event logs will be sent



Logging>Syslog

Please enter the details of an external syslog server to which PINs

Syslogs: Host: 192.168.0.155
Level: Info
Facility: kern

Host:
Level: Off
Facility: local0

If there is no syslog service, the PINsafe .xml log files produced by PINsafe can be imported into Splunk.

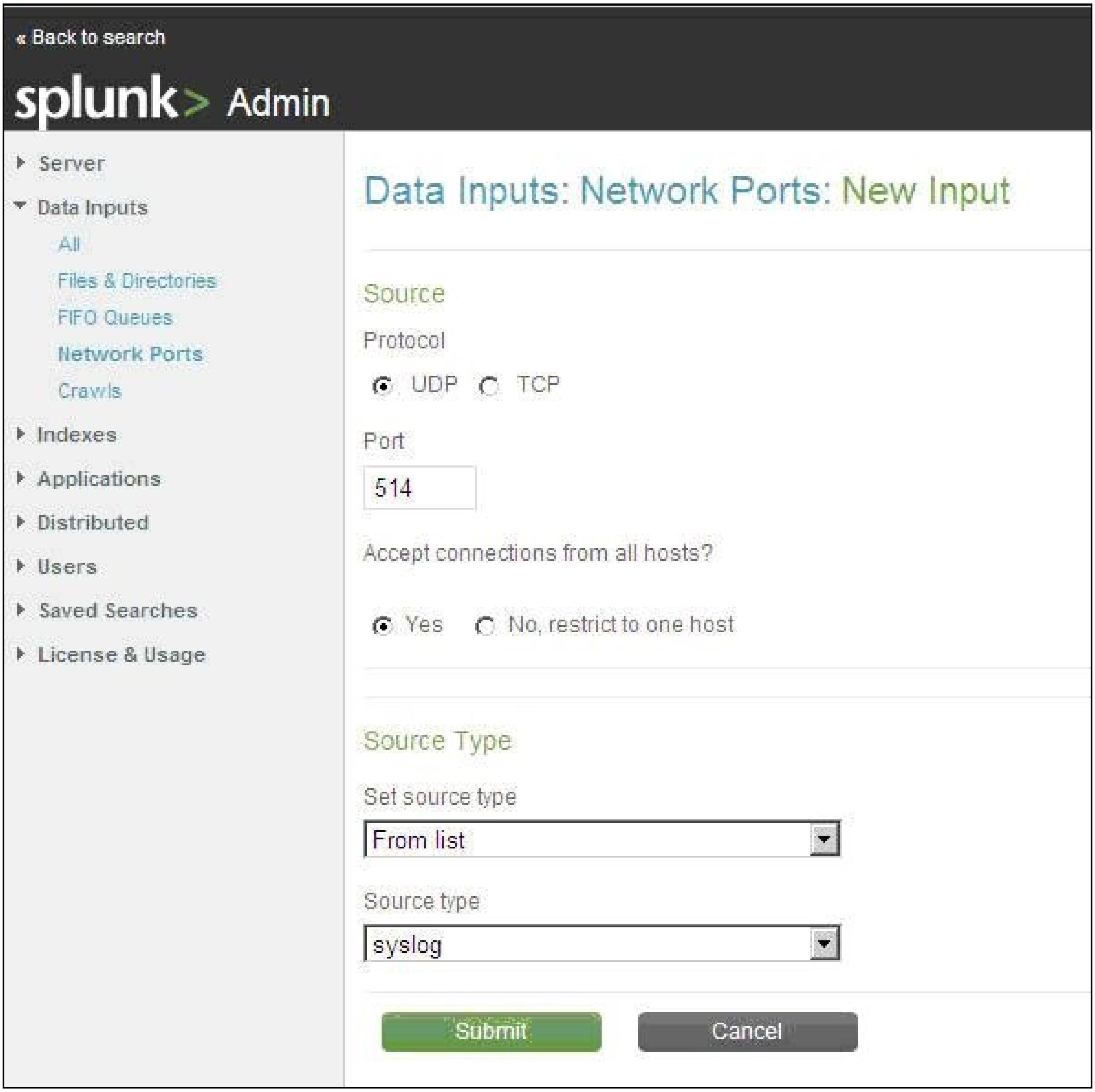
For a PINsafe appliance, they can be manually copied off to the Splunk server, see the appliance Administration guide for further details.

Alternatively a scheduled job maybe employed to copy the files across.

Splunk Syslog Configuration

On the Splunk server select Data Inputs/Network Ports then New Input, select the following options:

Source: UDP Port: 514 Accept connections from all hosts?: optional Set Source Type: From List Source Type: Syslog



Data Inputs: Network Ports: New Input

Source

Protocol

● UDP ○ TCP

Port

514

Accept connections from all hosts?

● Yes ○ No, restrict to one host

Source Type

Set source type

From list

Source type

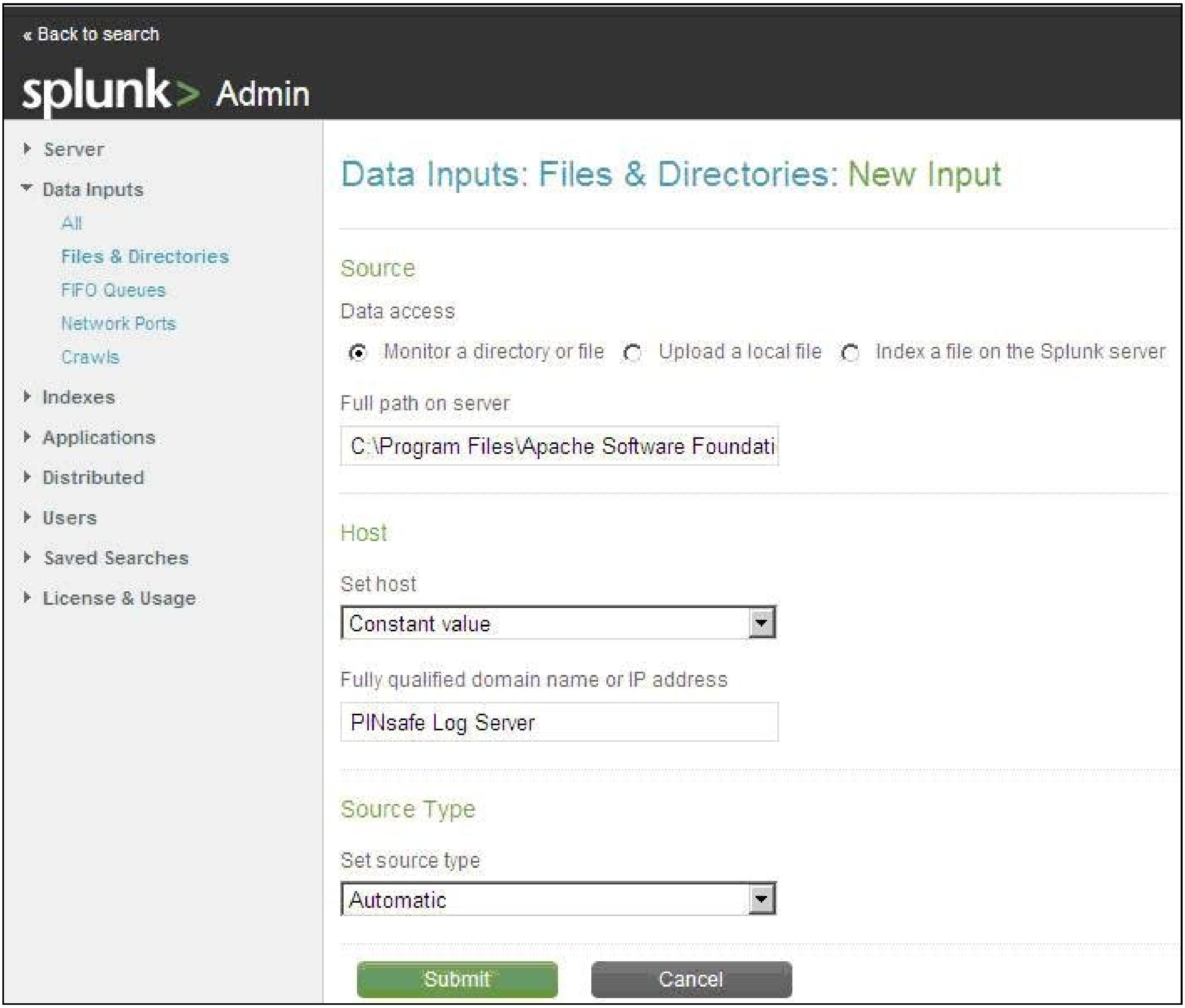
syslog

Then restart the Splunk Application by selecting Server/Control Server and Restart Now.

Splunk XML Log File Configuration

On the Splunk server select Data Inputs/Files and Directories then New Input, select the following options:

Data Access: Monitor a directory or file Full Path on server: location of log files Set Source Type: Automatic



Data Inputs: Files & Directories: New Input

Source

Data access

● Monitor a directory or file ○ Upload a local file ○ Index a file on the Splunk server

Full path on server: C:\Program Files\Apache Software Foundati

Host

Set host: Constant value

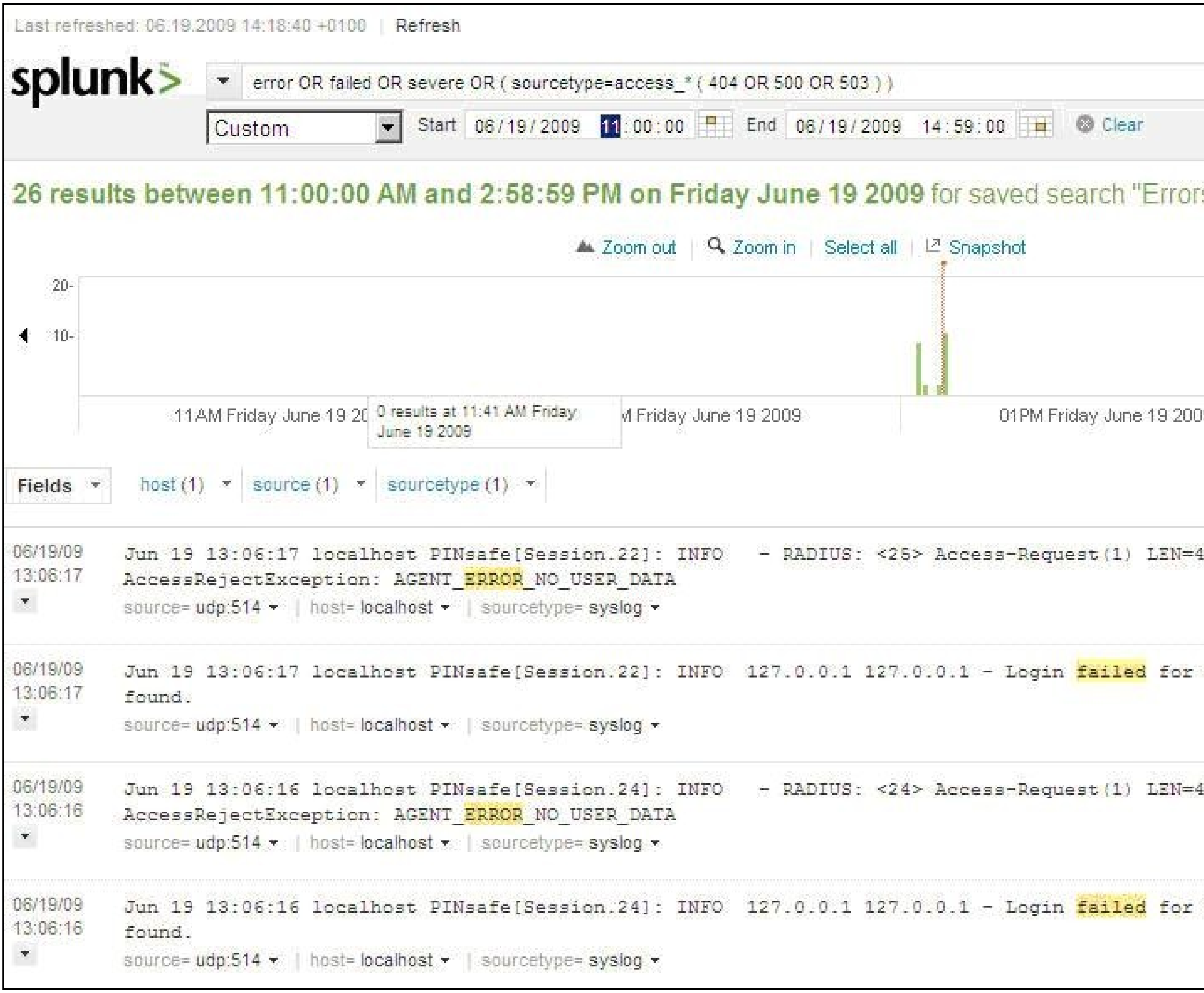
Fully qualified domain name or IP address: PINsafe Log Server

Source Type

Set source type: Automatic

Verifying the Installation

The Splunk screen should show input when PINsafe events occur or from historical logs.



Last refreshed: 06.19.2009 14:18:40 +0100

error OR failed OR severe OR (sourcetype=access_* (404 OR 500 OR 503))

Custom Start 06/19/2009 11:00:00 End 06/19/2009 14:59:00

26 results between 11:00:00 AM and 2:58:59 PM on Friday June 19 2009 for saved search "Error

```
06/19/09 13:06:17
Jun 19 13:06:17 localhost PINsafe[Session.22]: INFO  - RADIUS: <25> Access-Request(1) LEN=4
AccessRejectException: AGENT_ERROR_NO_USER_DATA
source= udp:514 | host= localhost | sourcetype= syslog

06/19/09 13:06:17
Jun 19 13:06:17 localhost PINsafe[Session.22]: INFO 127.0.0.1 127.0.0.1 - Login failed for
found.
source= udp:514 | host= localhost | sourcetype= syslog

06/19/09 13:06:16
Jun 19 13:06:16 localhost PINsafe[Session.24]: INFO  - RADIUS: <24> Access-Request(1) LEN=4
AccessRejectException: AGENT_ERROR_NO_USER_DATA
source= udp:514 | host= localhost | sourcetype= syslog

06/19/09 13:06:16
Jun 19 13:06:16 localhost PINsafe[Session.24]: INFO 127.0.0.1 127.0.0.1 - Login failed for
found.
source= udp:514 | host= localhost | sourcetype= syslog
```

These events can be filtered to display only specific events. Refer to Splunk documentation for more details.

Additional Information

For assistance in the PINsafe installation and configuration please firstly contact your reseller and then email Swivel Secure support at support@swivelsecure.com