Vendor - Dell RSA

Product - SecureID

Ref	Link
Splunk Add-on	http://splunkbase.splunk.com/app/2958/
Product Manual	http://docs.splunk.com/Documentation/AddOns/latest/RSASecurID/About

Sourcetypes

sourcetype	notes
rsa:securid:syslog	Catchall; used if a more specific source type can not be identified
rsa:securid:admin:syslog	None
rsa:securid:runtime:syslog	None
nix:syslog	None

Sourcetype and Index Configuration

key	sourcetype	index	notes
dell_rsa_secureid	all	netauth	none
dell_rsa_secureid	nix:syslog	osnix	use nix index for non configured by host/port

Filter type

Must be identified by host or ip assignment. Update the filter `f_dell_rsa_secureid` or configure a dedicated port as required

NOTE: Java trace and exception will default to sys::fallback if the host ip filter or port is not configured

Setup and Configuration

* Install the Splunk Add-on on the search head(s) or the search heads for the indexes, as these contain index-time and search-time knowledge for the Dell SecureID source. CS4S does exclusively used the add-on is not required on the indexer.

* Review and apply the appropriate index-time and search-time configuration for the data source.

* Refer to the manual for the appropriate configuration details.

Options

Variable	default	description
SC4S_LISTEN_DELL_RSA_SECUREID_PORT	empty	Enable a TCP port for this specific vendor product using the number specified