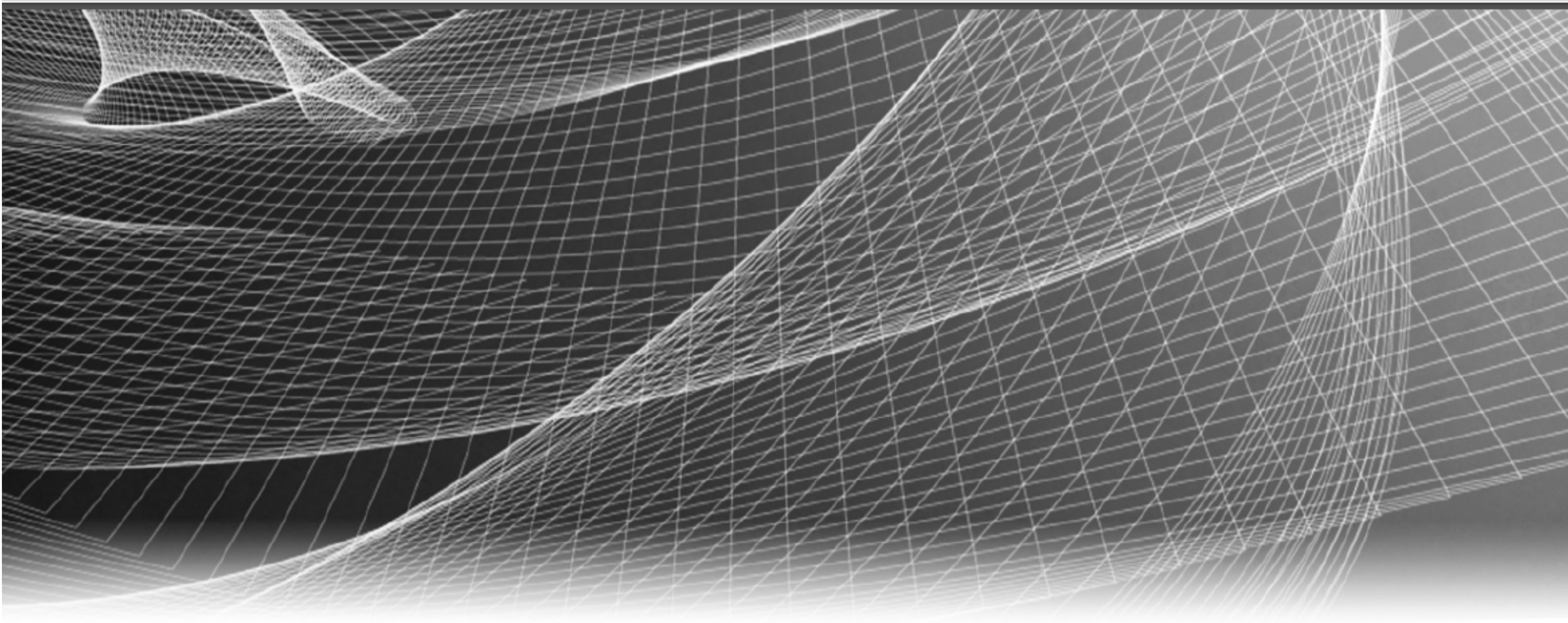


RSA Security Analytics

Hosts and Services Getting Started Guide

for Version 10.6.5

RSA EMC²

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

License Agreement

Third-Party Licenses

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

November 2017

Contents

Hosts and Services Getting Started Guide Overview 13

The Basics 15

Maintaining Hosts 16

Update Version Naming Convention 16

Updating a Host Version 16

Deploying Multiple Versions 20

Maintaining Services 20

Host Setup Procedures 21

Step 1. Add or Update a Host 22

Update a Host after an Update 22

Add a Host Manually 22

Step 2. Add a Service to a Host 24

Prerequisites 24

Procedure 24

Step 3. Review SSL Ports for Trusted Connections 27

Prerequisite 27

Encrypted SSL Ports 27

Step 4. Manage Access to a Service 29

Test a Trusted Connection 29

Prerequisites 29

Procedure 29

Host Maintenance Procedures 33

Apply Updates 34

Procedure 34

Change the Name and Hostname of a Host 37

Edit a Host 37

Create and Manage Host Groups 38

Create a Group 38

Change the Name of a Group 39

Add a Host to a Group 39

View the Hosts in a Group 40

Remove a Host from a Group 41

Delete a Group 41

Free Local Update Repository Disk Space 42

Procedure 42

Remove a Host 43

Remove a Host 43

Remove a Host and Repurpose 43

Search for Hosts 45

Search for a Host 45

Find the Host that Runs a Service 46

Update Hosts in Correct Sequence 47

Basic Update Sequence 47

Update Security Analytics in a Multiple Security Analytics Server Environment 47

Primary Security Analytics Server 48

Secondary Security Analytics Server 48

Scenario 1. Full Update, Update Order (Strongly Recommended) 48

Scenario 2. Partial Update 48

Scenario 3. Regional Update with Multiple Brokers 49

First Update Session at Site 1 49

Second Update Session at Site 2 49

Scenario 4. Regional Update with Multiple Security Analytics Servers 49

First Update Session at Site 1 49

Second Update Session at Site 2 49

Host Procedures from the Task List Dialog 51

Execute a Task From the Host Task List 52

Add and Delete a Filesystem Monitor 55

Configure the Filesystem Monitor 56

Delete a Filesystem Monitor 57

Reboot a Host 58

Shut Down and Restart a Host from the Hosts View 58

Shut Down and Restart a Host from the Host Task List 58

Set Host Built-In Clock 60

Set the Time on the Local Clock 60

Set Network Configuration 61

Specify the Network Address for a Host 61

Set Network Time Source 63

Specify the Network Clock Source 63

Set SNMP 65

Toggle SNMP Service on the Host 65

Set Syslog Forwarding 67

Set Up and Start Syslog Forwarding 67

Show Network Port Status 69

Display the Network Port Status 69

Show Serial Number 71

Show the Serial Number 71

Shut Down Host 72

Shut Down the Physical Host 72

Stop and Start a Service on a Host 73

Stop a Service on a Host 73

Start a Service on a Host 74

Service Procedures 75

Add, Replicate or Delete a Service User 76

Replication and Migration Considerations 76

Procedures 77

Access the Security View 77

Add a Service User 78

Replicate a User to Other Services 79

Delete a Service User 80

Add a Service User Role 81

Procedure 81

Change a Service User Password 83

Procedure 83

Create and Manage Service Groups 85

Create a Group 85

Change the Name of a Group 86

Add a Service to a Group 86

View the Services in a Group 87

Remove a Service from a Group 87

Delete a Group 88

Duplicate or Replicate a Service Role 89

Procedures 89

Duplicate a Service Role 89

Replicate a Role 90

Edit Core Service Configuration Files 91

Edit a Service Configuration File 91

Revert to a Backup Version of a Service Configuration File 92

Push a Configuration File to Other Services 93

Configure the Task Scheduler 94

The scheduler File 94

Scheduler Task Syntax 94

Task Line Parameters 94

Messages 95

Sample Task Line 96

Edit a Service Index File 97

Index and Custom Index Files 97

Enable Crash Reporter Service 99

The crashreporter.cfg File 99

Configure the Crash Reporter Service 102

Start and Stop the Crash Reporter Service 103

Maintain the Table Map Files 104
Prerequisites 104
Procedure 104
Edit or Delete a Service 106
Procedures 106
Edit a Service 106
Delete a Service 107
Explore and Edit Service Property Tree 108
Procedures 108
Display or Edit a Service Property 108
Send a Message to a Node 109
Kill a Connection to a Service 110
End a Session on a Service 110
End an Active Query in a Session 111
Search for Services 112
Search for a Service 112
Filter Services by Type 113
Find the Services on a Host 114
Start, Stop or Restart a Service 116
Start a Service 116
Stop a Service 116
Restart a Service 116
View Service Details 117
Purpose of Each Service View 117
Access a Service View 117
References 121
Administration System View 122
Features 122
System Logging Panel 123
Features 123
Historical Tab 125

Features 126

Search Log Entries 128

Show Details of a Log Entry 128

Page Through the Entries 129

Export 129

Realtime Tab 130

Features 131

Toolbar 131

Log Grid Columns 132

Settings Tab 133

Features 133

Log Settings 134

Package Configuration 134

URL Integration Panel 136

Components 136

Service Configuration Settings 138

Appliance Service Configuration 139

Settings 139

Archiver Service Configuration 140

Archiver Configuration Settings 140

Broker Service Configuration 141

Broker Configuration Settings 141

Aggregation Configuration Nodes 142

Aggregation Configuration Settings 142

Concentrator Service Configuration 145

Concentrator Configuration Settings 145

Core Service Logging Configuration 146

Core Service-to-Service Configuration 149

Core Service System Configuration 150

Settings 150

Decoder Service Configuration 152

Decoder Configuration Settings 152

Decoder and Log Decoder Common Configuration 153

Decoder Configuration Settings 153

Log Decoder Service Configuration 158

Log Decoder Configuration Settings 158

Log Tokenizer Configuration Settings 159

REST Interface Configuration 163

Settings 163

Security Analytics Core Service system.roles Modes 164

system.roles 164

Hosts View 165

Features 166

Hosts Panel 166

Groups Panel 169

Hosts Panel Toolbar 171

Features 171

Groups Panel Toolbar 173

Features 173

Services View 174

Features 175

Services Panel 176

Groups Panel 177

Add Service or Edit Service Dialog 179

Features 180

Groups Panel Toolbar 182

Features 182

Services Panel Toolbar 183

Features 183

Services Config View 186

Services Config View - Appliance Service Configuration Tab 188

Features 188

Grid 188

Data Retention Scheduler Tab 190

Features 191

Files Tab 192

Files Tab Toolbar 193

Services Explore View 195

Features 196

The Node List 196

The Monitor Panel 197

Properties Dialog 199

Features 200

Services Logs View 201

Features 202

Services Security View 203

Features 204

Roles and Service Access 204

Roles Tab 206

Features 207

Role Name Panel 207

Role Information Panel 208

Service User Roles and Permissions 209

Service User Roles 209

Service User Permissions 211

Aggregation Role 213

Settings Tab 215

Features 216

SDK Meta Role Permissions Options 216

Users Tab 218

Features 219

User List Panel 219

User Definition Panel 221

Services Stats View 224

Features 226

Summary Stats Section 226

Gauges 229

Timelines 229

Historical Timelines 229

Chart Stats Tray 230

Chart Stats Tray 231

Components 232

Gauges 233

Features 233

Timeline Charts 234

Services Stats View - Malware Analysis 236

Features 237

Events Tab 237

Analysis Threads Tab 238

Services System View 240

Features 241

Services System View Toolbar 241

Services Summary Information 242

Session Information Grid 243

Host Task List Dialog 244

Features 244

Host Task Selection List 245

Decoder Services System View 247

Features 248

Services Info Toolbar 248

Services System View 250

Features 251

Services System View Toolbar 251
Services Summary Information 252
Session Information Grid 253
Troubleshooting Host Updates 255
Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors 256
Pre-Update Warnings 256
Pre-Update Conflicts 257
Update Errors 259
Troubleshooting 10.6 Update Service Log Messages 261
System Management Service (SMS) 261
Java Version 261
Disk Space 261
Services 262
Log Collector Service (nwlogcollector) 263
Lock Box Verification Logs 263
Event Stream Analysis (ESA) 264
Pre-Update Check 264
Post-Update Check 265
Reporting Engine Service 266
Update Check 266

Hosts and Services Getting Started Guide

Overview

This guide gives administrators the standard procedures for adding and configuring hosts (appliances) and services in Security Analytics. After introducing you to the basic purpose of hosts and services and how they function within in the Security Analytics network, this guide covers:

- The minimum tasks you must complete to configure hosts and services in your network.
- Additional procedures that you complete based on the long-term and daily, operational needs of your enterprise
- Reference topics that describe the user interface

The Basics

A host is the machine on which a service runs and a host can be a physical or virtual machine.

A service performs a unique function, such as collecting logs or archiving data. Each service runs on a dedicated port and is modeled as a plugin to enable or disable, according to the function of the host.

You must configure the following Core services first:

- Decoder
- Concentrator
- Broker
- Log Decoder

All the services are listed below and each service except the Log Collector has its own guide or shares a guide in the *Host and Services Configuration Guides*. The Log Collector has its own set of configuration guides to handle the configuration for all the supported event collection protocols. For Log Collector information, see *Log Collection Guides*.

- Archiver
- Broker
- Concentrator
- Decoder
- Event Stream Analysis
- Context Hub
- Incident Management
- IPDB Extractor
- Log Collector
- Log Decoder
- Malware Analysis
- Reporting Engine
- Warehouse Connector
- Workbench

You must configure hosts and services to communicate with the network and each other so they can perform their functions such as storing or capturing data.

Maintaining Hosts

You use the Host view to add, edit, delete, and perform other maintenance tasks for the hosts in your deployment. See:

- Host Setup Procedures - minimum tasks you must complete to set up a host in Security Analytics.
- Host Maintenance Procedures - host maintenance tasks that you perform from the Hosts view.
- Host Procedures from the Task List Dialog - tasks relating to a host and its communications with the network that you perform from the Task List dialog.

After your initial implementation of Security Analytics, the major task you perform from the Host view is updating your Security Analytics deployment to a new version.

Update Version Naming Convention

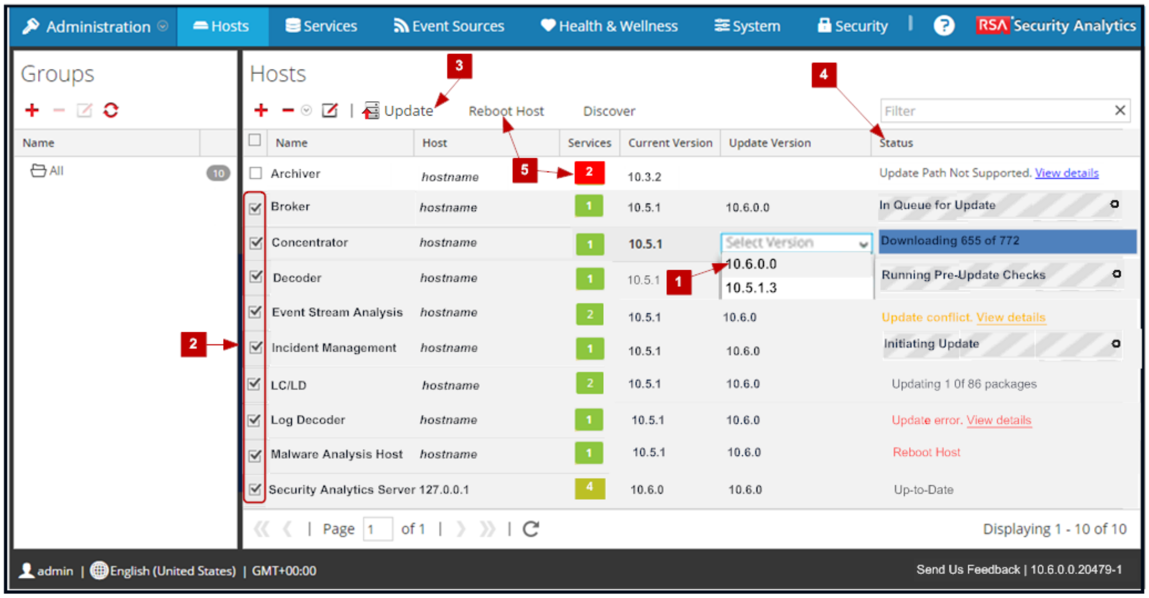
You use the Hosts view to apply the latest version updates from your Local Update Repository (see the **Manage Security Analytics Updates** topic in *System Maintenance* for more information on your Local Update Repository). You must understand the update version naming convention to know which version you want to apply to the host. The naming convention is ***major-release.minor-release.service-pack.patch***. For example, if you choose 10.6.1.2, you would be applying the following version to the host.

- 10 = major release
- 6 = minor release
- 1 = service pack
- 2 = patch

Updating a Host Version

You use the Hosts view to update a host to a new version. The following example illustrates how to do this. When there are version updates available for a host, Update Available is displayed in the **Status** column and you choose the update from the **Select Version** column. See Apply Updates for detailed instruction on how to apply a new version update to a host.

> **Note:** If you cannot find a version, you may need to populate your local update repository. For more information, see the **Populate Local Update Repository** topic in *System Maintenance*.



	Name	Host	Services	Current Version	Update Version	Status
□	Archiver	hostname	2	10.3.2		Update Path Not Supported. View details
☑	Broker	hostname	1	10.5.1	10.6.0.0	In Queue for Update
☑	Concentrator	hostname	1	10.5.1	Select Version 10.6.0.0 10.5.1.3	Downloading 655 of 772
☑	Decoder	hostname	1	10.5.1		Running Pre-Update Checks
☑	Event Stream Analysis	hostname	2	10.5.1	10.6.0	Update conflict. View details
☑	Incident Management	hostname	1	10.5.1	10.6.0	Initiating Update
☑	LC/LD	hostname	2	10.5.1	10.6.0	Updating 1 0f 86 packages
☑	Log Decoder	hostname	1	10.5.1	10.6.0	Update error. View details
☑	Malware Analysis Host	hostname	1	10.5.1	10.6.0	Reboot Host
☑	Security Analytics Server	127.0.0.1	4	10.6.0	10.6.0	Up-to-Date

Page 1 of 1

Displaying 1 - 10 of 10

1 Select the version from the **Update Version** column.

- If you do not have enough disk space in your Local Update Repository to download a version update, the **Repository Space Management** dialog is displayed with the contents and disk space status of the repository (see Free Local Update Repository Disk Space for instructions on how to free disk space). You can delete a version or version that you do not need to free enough disk space to download the version you want. (See Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors).

Note: You can only update to the latest minor release or a patch.

2 Select the host, or hosts, that you want to update.

- The Security Analytics (SA) Server Host must be updated to the latest version in your deployment before you can apply that version to any other host.
- If you select multiple hosts for an update, Security Analytics updates the SA Server Host first.
- If you try to update one or more hosts other than the SA Server Host to the latest version in your deployment before the SA Server Host, Security Analytics will not allow you to do this.
- If a host is currently on a version that is not a valid update path, Security Analytics tells you to contact Customer Care for instructions on how to update the host to a valid path.

> **Note:** If you have conflicts updating any of the non-SA Server hosts, the SA Server Host remains grayed out until other host conflicts are resolved.

3 Click **Update** to start the update process.

4

Monitor monitor the progress of the update in the **Status** column. During the update process, Security Analytics:

1. Downloads the update package for the selected version if that package does not exist in your Local Update Repository.
2. If you select multiple hosts to update, displays **In Queue for Update** while it applies the version to each host.
3. Displays **Running Pre-Update Checks** while it validates your current version configuration.
   - Displays **Update warning. View details** if there is an issue in your existing configuration that does not prevent you from updating to the new version.
   - Displays **Update conflict. View details** if there is a conflict in your existing configuration that blocks you from updating to the new version.

   See Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors for instructions on how to resolve these configuration warnings and conflicts.
4. Initiates the update if there are no conflicts.
5. Applies each package for the selected update version.
6. Monitors the update. If there is an error that blocks the update, Security Analytics displays **Update error. View details.** See Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors for instructions on how to resolve these errors.
7. Prompts you to **Reboot Host** after the host has been updated.

5

Click **Reboot Host**.

- When you are updating multiple hosts, after each host is updated and running, Security Analytics displays **Up-to-Date**.
- If the host is updated, but all the services are not restarted after reboot, Security Analytics displays the services in red. Services may take several minutes to come online. Contact Customer Care if the host does not come back online.

Deploying Multiple Versions

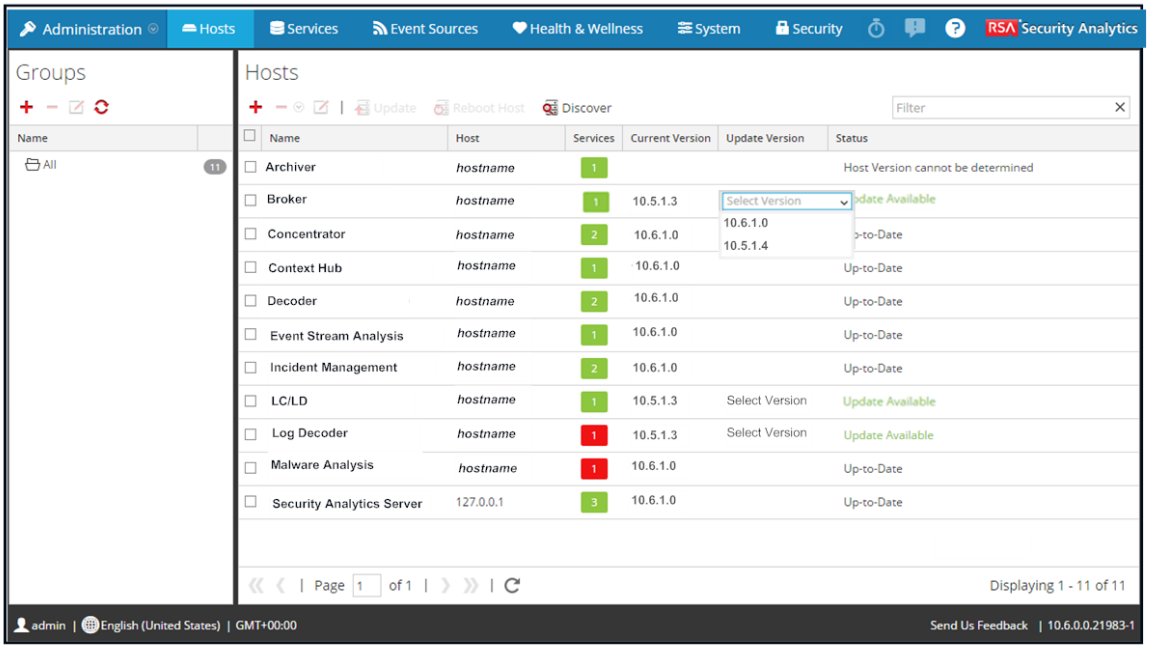
Security Analytics supports multiple versions in your deployment. The Security Analytics (SA) Server Host is updated first and all other hosts must have the same or earlier version as the SA Server Host.

Note: The Hosts view ensures that the SA Server Host is updated first and that all other hosts have the same or earlier version as the SA Server Host.

In the following example of a multiple version deployment.

- Version updates currently available in your Local Update Repository are 10.6.1.0 and 10.5.1.4 for the Broker, LC/LD, and Log Decoder hosts.
- The SA Server Host and all the other hosts are currently updated to 10.6.1.

This means that you have the option to update the Broker, LC/LD, and Log Decoder hosts to 10.6.1.0 or 10.5.1.4.



□	Name	Host	Services	Current Version	Update Version	Status
□	Archiver	*hostname*	1			Host Version cannot be determined
□	Broker	*hostname*	1	10.5.1.3	Select Version 10.6.1.0 10.5.1.4	pdate Available
□	Concentrator	*hostname*	2	10.6.1.0		p-to-Date
□	Context Hub	*hostname*	1	10.6.1.0		Up-to-Date
□	Decoder	*hostname*	2	10.6.1.0		Up-to-Date
□	Event Stream Analysis	*hostname*	1	10.6.1.0		Up-to-Date
□	Incident Management	*hostname*	2	10.6.1.0		Up-to-Date
□	LC/LD	*hostname*	1	10.5.1.3	Select Version	Update Available
□	Log Decoder	*hostname*	1	10.5.1.3	Select Version	Update Available
□	Malware Analysis	*hostname*	1	10.6.1.0		Up-to-Date
□	Security Analytics Server	127.0.0.1	3	10.6.1.0		Up-to-Date

Maintaining Services

You use the Services view to add, edit, delete, monitor, and perform other maintenance tasks for the services in your deployment. See Service Procedures for detailed instructions on the tasks you perform from the Hosts view.

Host Setup Procedures

The following topics describe the minimum tasks you must complete to set up a host in Security Analytics.

Topics

- Step 1. Add or Update a Host
- Step 2. Add a Service to a Host
- Step 3. Review SSL Ports for Trusted Connections
- Step 4. Manage Access to a Service

Step 1. Add or Update a Host

Your Security Analytics environment determines how you add a host.

Security Analytics Environment	High-Level Steps
10.6 Update	1. Download the RSA Security Analytics v10.6 Documentation from SCOL (https://knowledge.rsasecurity.com/). 2. Follow the instructions in the RSA Security Analytics v10.6 Update Instructions.
10.6 Security Analytics Server Host	1. Click ✚ to open the Add Host dialog. 2. In the **Name** field, type a name for the host and in the **Hostname** field, type the 127.0.0 for the IP address of the host. 3. Click **Save**.

There is a detailed, step-by-step procedure for each type of environment.

Update a Host after an Update

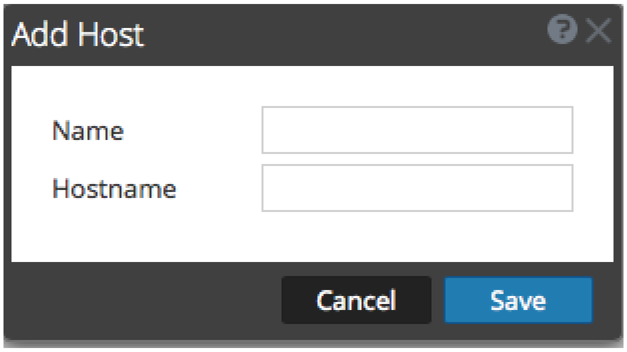
Caution: Before you attempt to update a host to v10.6, you must:
1. Download the RSA Security Analytics v10.6 Documentation from SCOL (https://knowledge.rsasecurity.com).
2. Follow the instructions in the RSA Security Analytics v10.6 Update Instructions.

1. Perform the tasks that apply to the all services running on this host as described in the following sections in RSA Security Analytics v10.6.x.x Update Instructions:
   - Update Preparation Tasks
   - Update Tasks
   - Post-Update Task

Add a Host Manually

1. In the Security Analytics menu, click **Administration** > **Hosts**.
   The Hosts view is displayed.

2. In the Hosts panel toolbar, select +. The **Add Host** dialog is displayed.



3. In the **Name** field, type a name for the host.
4. In the **Hostname** field, type the **IP-address** or **hostname** of the host.
5. Click **Save**.

Step 2. Add a Service to a Host

Each service is modeled as a plugin to enable or disable according to the function of the host.

Prerequisites

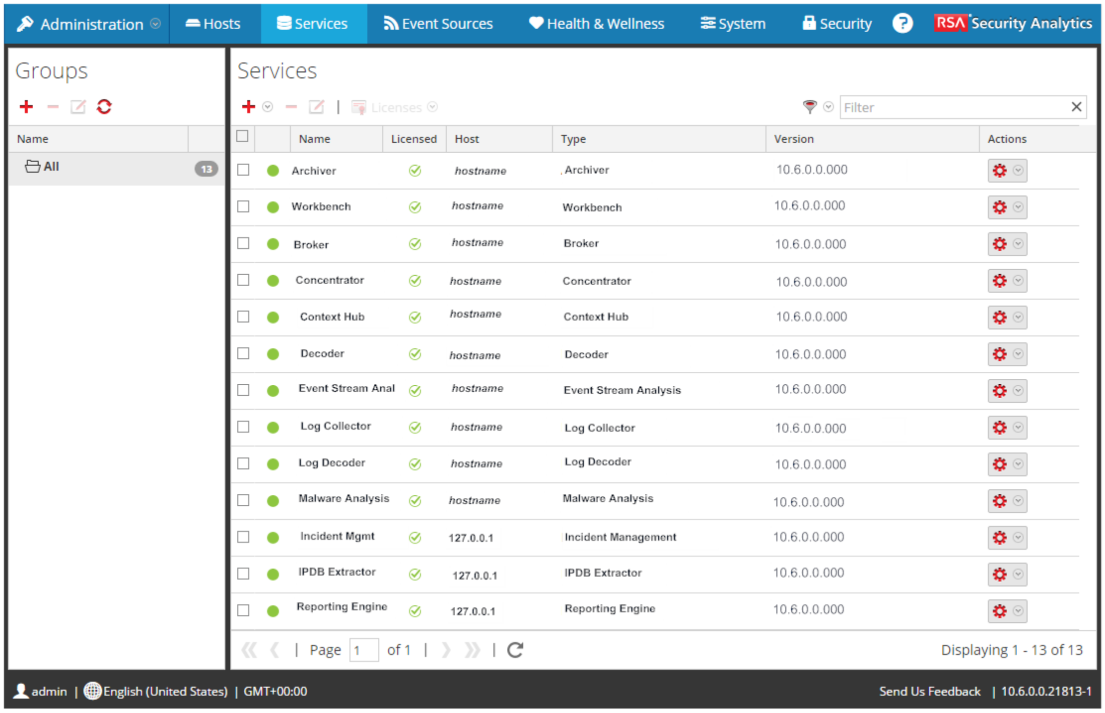
Equipment, which can be physical or virtual, must be installed: Security Analytics server, Broker, Concentrator, Decoder, Log Decoder, Archiver, Warehouse, Malware Analysis server, or Event Stream Analysis server.

Procedure

Perform the following steps to add a Service to a Host:

1. In the Security Analytics menu, select **Administration** > **Services**.

   The Administration Services view is displayed.

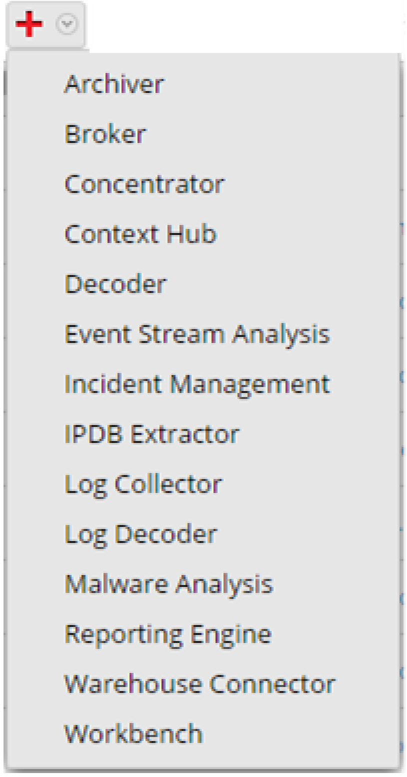


□		Name	Licensed	Host	Type	Version	Actions
□	●	Archiver	✓	*hostname*	Archiver	10.6.0.0.000	
□	●	Workbench	✓	*hostname*	Workbench	10.6.0.0.000	
□	●	Broker	✓	*hostname*	Broker	10.6.0.0.000	
□	●	Concentrator	✓	*hostname*	Concentrator	10.6.0.0.000	
□	●	Context Hub	✓	*hostname*	Context Hub	10.6.0.0.000	
□	●	Decoder	✓	*hostname*	Decoder	10.6.0.0.000	
□	●	Event Stream Anal	✓	*hostname*	Event Stream Analysis	10.6.0.0.000	
□	●	Log Collector	✓	*hostname*	Log Collector	10.6.0.0.000	
□	●	Log Decoder	✓	*hostname*	Log Decoder	10.6.0.0.000	
□	●	Malware Analysis	✓	*hostname*	Malware Analysis	10.6.0.0.000	
□	●	Incident Mgmt	✓	127.0.0.1	Incident Management	10.6.0.0.000	
□	●	IPDB Extractor	✓	127.0.0.1	IPDB Extractor	10.6.0.0.000	
□	●	Reporting Engine	✓	127.0.0.1	Reporting Engine	10.6.0.0.000	

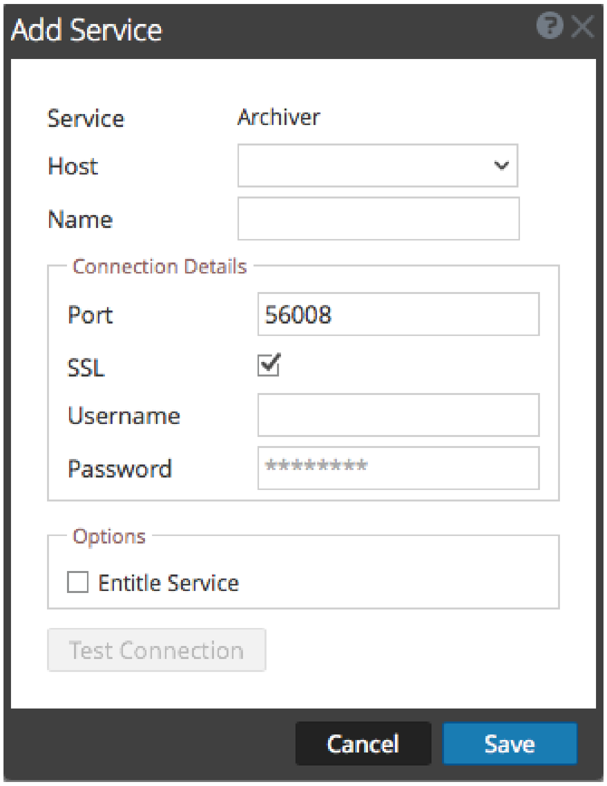
Page 1 of 1 | Displaying 1 - 13 of 13

admin | English (United States) | GMT+00:00 | Send Us Feedback | 10.6.0.0.21813-1

2. In the Administration Services view, select + in the **Services panel toolbar**.



The Add Service dialog is displayed.


Add Service

Service	Archiver
Host	
Name	

Connection Details

Port	56008
SSL	☑
Username	
Password	*********

Options

☐ Entitle Service

3. From the drop-down list, select the host the server will run on.
4. Type the name of the service.

   > **Note:** An understandable naming convention can make administrative tasks easier. Some administrators find it convenient to use the hostname or IP address (specified in the Host field) for the Name as well.

5. (Optional) In the **Connection Details** section:
   - **Port -** If you want to use a port other than the default, type the number in the **Port** field. See the Step 3. Review SSL Ports for Trusted Connections.
   - **SSL -** If you use a trusted connection, select **SSL**.
   - **Username** and **Password -** Type the credentials assigned to the user on Security Analytics Server.
6. (Optional) In the **Options** section, to activate and apply a license select **Entitle Service**. This option appears only for services that require a license.
7. Click **Save**. The service is added and the dialog closes.

Step 3. Review SSL Ports for Trusted Connections

To support trusted connections each core service has two ports, an unencrypted non-SSL port and an encrypted SSL port. Trusted connections require the encrypted SSL port.

Prerequisite

To establish a trusted connection, each Security Analytics Core service must be upgraded to 10.4 or later. Trusted connections are not backwards compatible with Security Analytics Core 10.3.x or earlier.

Encrypted SSL Ports

When you install or upgrade to 10.4 or later, trusted connections are established by default with two settings:

1. SSL is enabled.
2. The core service is connected to an encrypted SSL port.

Each Security Analytics Core service has two ports:

- Unencrypted **non-SSL port**
  Example: Archiver 50008
- Encrypted **SSL port**
  Example: Archiver 56008

The SSL port is the non-SSL port + 6000.

The following table lists all Security Analytics services with their respective ports and shows that each core service has two ports. All port numbers listed are TCP.

Service	Unencrypted Non-SSL Port	Encrypted SSL Port
Archiver	50008	56008
Broker	50003	56003
Concentrator	50005	56005
Context Hub	N/A	50022

Service	Unencrypted Non-SSL Port	Encrypted SSL Port
Decoder	50004	56004
Event Stream Analysis	N/A	50030
Incident Management	N/A	50040
IPDB Extractor	50025	56025
Log Collector	50001	56001
Log Decoder	50002	56002
Malware Analysis	N/A	60007
Reporting Engine	N/A	51113
Warehouse Connector	50020	56020
Workbench	50007	56007

Step 4. Manage Access to a Service

In a trusted connection, a service explicitly trusts Security Analytics Server to manage and authenticate users. With this trust, services in Administration > Services no longer require credentials to be defined for every Security Analytics Core service. Instead, users who have been authenticated by the server can access the service without entering another password.

Test a Trusted Connection

Prerequisites

1. A role must be assigned to the user.

   For details, see **Add a User and Assign a Role** topic in the *System Security and User Management Guide*.

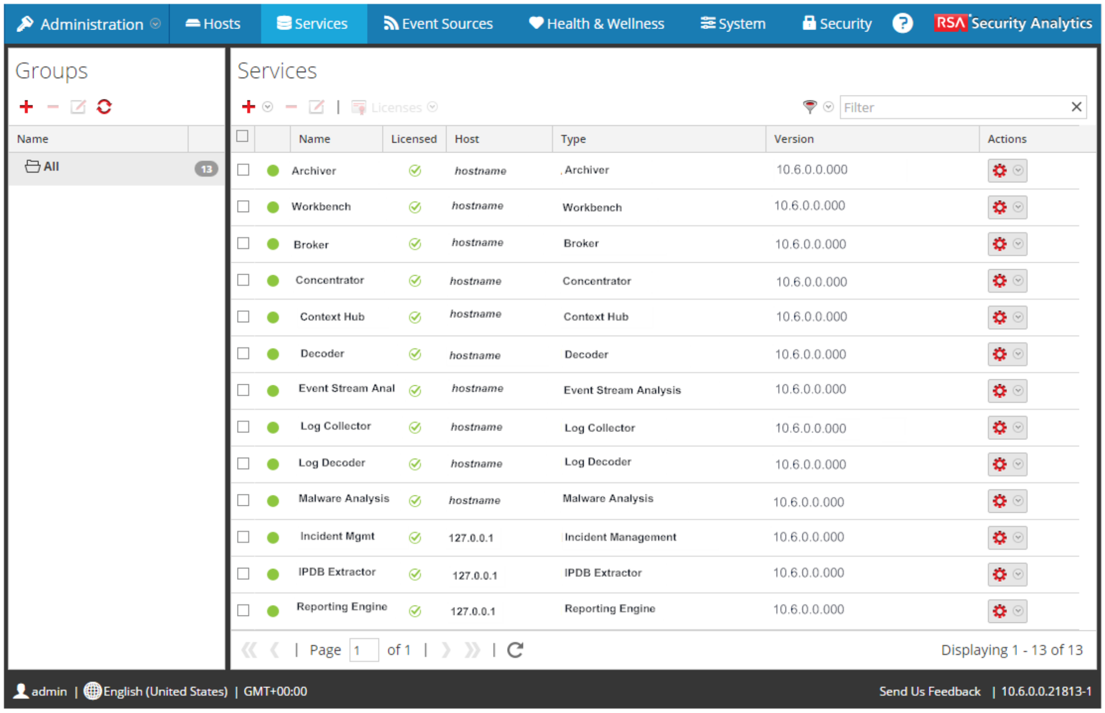
2. The user must:

   - Log on to Security Analytics to be authenticated by the server
   - Have access to the service

Procedure

1. In the Security Analytics menu, select **Administration > Services**.

   The Services view is displayed.



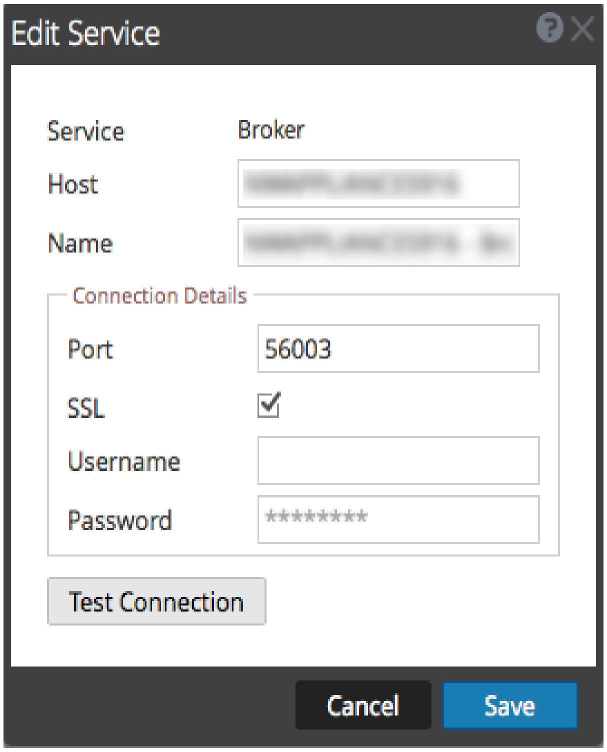
☐		Name	Licensed	Host	Type	Version	Actions
☐	●	Archiver	✓	*hostname*	Archiver	10.6.0.0.000	⚙
☐	●	Workbench	✓	*hostname*	Workbench	10.6.0.0.000	⚙
☐	●	Broker	✓	*hostname*	Broker	10.6.0.0.000	⚙
☐	●	Concentrator	✓	*hostname*	Concentrator	10.6.0.0.000	⚙
☐	●	Context Hub	✓	*hostname*	Context Hub	10.6.0.0.000	⚙
☐	●	Decoder	✓	*hostname*	Decoder	10.6.0.0.000	⚙
☐	●	Event Stream Anal	✓	*hostname*	Event Stream Analysis	10.6.0.0.000	⚙
☐	●	Log Collector	✓	*hostname*	Log Collector	10.6.0.0.000	⚙
☐	●	Log Decoder	✓	*hostname*	Log Decoder	10.6.0.0.000	⚙
☐	●	Malware Analysis	✓	*hostname*	Malware Analysis	10.6.0.0.000	⚙
☐	●	Incident Mgmt	✓	127.0.0.1	Incident Management	10.6.0.0.000	⚙
☐	●	IPDB Extractor	✓	127.0.0.1	IPDB Extractor	10.6.0.0.000	⚙
☐	●	Reporting Engine	✓	127.0.0.1	Reporting Engine	10.6.0.0.000	⚙

Page 1 of 1

Displaying 1 - 13 of 13

2. Select the service to test and click ✎.

   The **Edit Service** dialog is displayed.



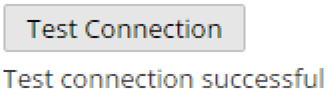
Service	Broker
Host	[redacted]
Name	[redacted]
Port	56003
SSL	☑
Username	
Password	*********

3. If you did a fresh 10.6 install, the port is correct. No action is required in the **Port** field. Go to the next step.

   If you upgraded to 10.6 or have a mixed environment of a 10.6 server and 10.3 hosts, you must update the **Port** by deselecting and re-selecting **SSL**. Then, the **Port** number changes to the encrypted SSL port for the service.

4. Remove the **Username** to test the connection without credentials.

5. Click **Test Connection**.

   Test connection successful

   The message **Test connection successful** confirms the trusted connection is established. The previously authenticated user can access the service without typing a username and password on the service.

6. Click **Save**.

Host Maintenance Procedures

The following topics describe the basic host maintenance tasks that you perform from the Hosts view.

Topics

- Apply Updates
- Change the Name and Hostname of a Host
- Create and Manage Host Groups
- Free Local Update Repository Disk Space
- Remove a Host
- Search for Hosts
- Update Hosts in Correct Sequence

Apply Updates

The Hosts view displays the software version updates available in your Local Update Repository and you choose and apply the updates you want from the Host view. See the **Populate Local Update Repository** topic in *System Maintenance* for information on how the Local Update Repository gets populated.

Procedure

This procedure tells you how to update a host to a new version of Security Analytics.

> **Note:** When you update the Security Analytics (SA) Server Host, Security Analytics backs up the System Management Service (SMS) configuration files (excluding the `wrapper.conf` file) from the `/opt/rsa/sms/conf` directory to`/opt/rsa/sms/conf_%timestamp%` directory. This is a precautionary measure for the rare occasion when you may need to restore the SMS configuration from backup. To do this, replace the files in the `/opt/rsa/sms/conf` directory with the files backed up to the `/opt/rsa/sms/conf_%timestamp%` directory after the update.

1. **(Conditional) For Multiple Security Analytics Server deployments only**, SSH to each Secondary SA Server Host and make sure the the puppetmaster is enabled using the following commands:

   ```
   chkconfig --add puppetmaster
    chkconfig --level 3 puppetmaster /etc/init.d/puppetmaster start
   ```

   For more information, see the **Multiple Security Analytics Server Deployment** topic in the *Deployment Guide*.

2. Log in to Security Analytics.

3. In the Security Analytics menu, select **Administration** > **Hosts**.

> **Note:** If you have a non-Security Analytics Server host running a version that is earlier than the 10.6.0 update path (that is, earlier than 10.4.1) and you updated your Security Analytics Server Host to 10.6.0, the non-Security Analytics Server host will display "**Update Path Not Supported**" in the **Status** column of the Hosts view and you cannot update it from this view. Contact Customer Care to update the non-Security Analytics Server host on the unsupported path.

4. Update hosts in the sequence recommended in Update Hosts in Correct Sequence.

   a. Select the version you want to apply from the **Update Version** column. If you want to update more than one host to that version, select the checkbox to the left of the hosts. Update Available is displayed in the **Status** column if you have an version update in your Local Update Repository for the selected hosts.
   If you:

      - Cannot find the version you want, populate your Local Update Repository. For more information, see the **Populate Local Update Repository** topic in *System Maintenance*.

      - Do not have enough disk space in your Local Update Repository to download a version update, the **Repository Space Management** dialog is displayed with the contents and disk space status of the repository. You can delete versions that you do not need to free enough disk space to download the version you want. See Free Local Update Repository Disk Space for instructions.

   b. Click **Update** from the toolbar. The **Status** column tells you what is happening in each of the following stages of the update:

      - Downloading update packages.

      - Checking your current version configuration to ensure that it has no conflicts. Displays:

         - Update warning. View details if there is a potential conflict.

         - Update conflict. View details if there is a conflict.
         See Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors for instructions on how to address these configuration warnings and conflicts.

      - Initiating the update if there are no conflicts.

      - Updating update packages.
      Displays Error in Update. View details if there is an error applying a package that blocks the update. See Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors for instructions on how to resolve these errors.

   c. After the host is updated, Security Analytics prompts you to **Reboot Host**.

   d. Click **Reboot Host** from the toolbar.
   Security Analytics shows the status as **Rebooting...** until the host comes back online. After the host comes back online, the **Status** shows **Up-to-Date**. Contact Customer Care if the host does not come back online.

Note: If you have DISA STIG enabled, opening Core Services can take approximately 5 to 10 minutes. This delay is caused by the generating of new certificates.

Change the Name and Hostname of a Host

The Administration Hosts view enables you to change the Name and Hostname of the host on the Security Analytics user interface. For information on updating a host, see Step 1. Add or Update a Host.

Edit a Host

1. In the Security Analytics menu, select **Adminstration** > **Hosts**.
2. In the **Hosts** view, select a host that you want to edit, and in the toolbar, select ✎.
3. In the **Edit Host** dialog, you can update the **Name** at any time.
4. If the actual hostname changes, update the **Hostname** field.
   Use the `changePuppetMaster.py` Python script to change the IP Address or hostname of the Security Analytics Server Host or any other host in your Security Analytics deployment. You run this script from the command line on the Security Analytics Server Host. Refer to the **Change IP Address or Hostname of a Host** topic in *System Maintenance* for instructions on how to use this script.
5. Click **Save**.

Create and Manage Host Groups

The Administration Hosts view provides options for creating and managing groups of hosts. The Groups panel toolbar includes options for creating, editing, and deleting host groups. Once groups are created, you can drag individual hosts from the Hosts panel into a group.

Groups may reflect functional, geographical, project-oriented, or any other organization principle that is useful. A host may belong to more than one group. Here are some examples of possible groupings:

- Group different host types to make it easier to configure and monitor all Brokers, Decoders, or Concentrators.
- Group hosts that are part of the same data flow; for example, a Broker, and all associated Concentrators and Decoders.
- Group hosts according to their geographic region and location within the region. If a major power outage occurs in a location, potentially affected hosts are easily identifiable.

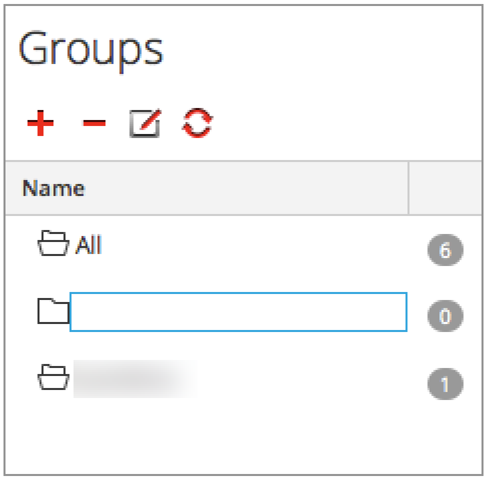
Create a Group

1. In the **Security Analytics menu**, select **Administration** > **Hosts**.

   The Administration Hosts view is displayed.

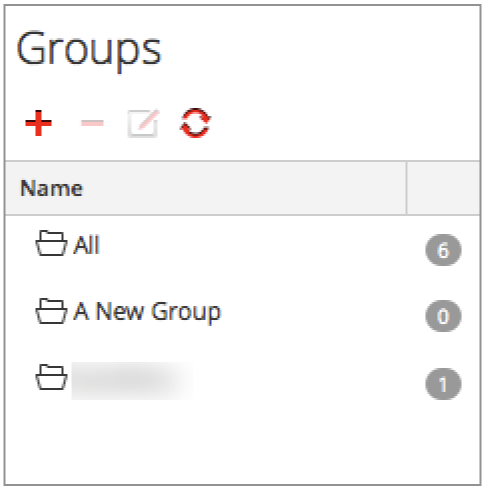
2. In the **Groups** panel toolbar, click >+.

   A field for the new group opens with a blinking cursor.

3. Type the name of the new group in the field (for example, **A New Group**) and press **Enter**.

   The group is created as a folder in the tree. The number next to the group indicates the number of hosts in that group.



Change the Name of a Group

1. In the Hosts view **Groups panel**, double-click the group name or select the group and click ✎.

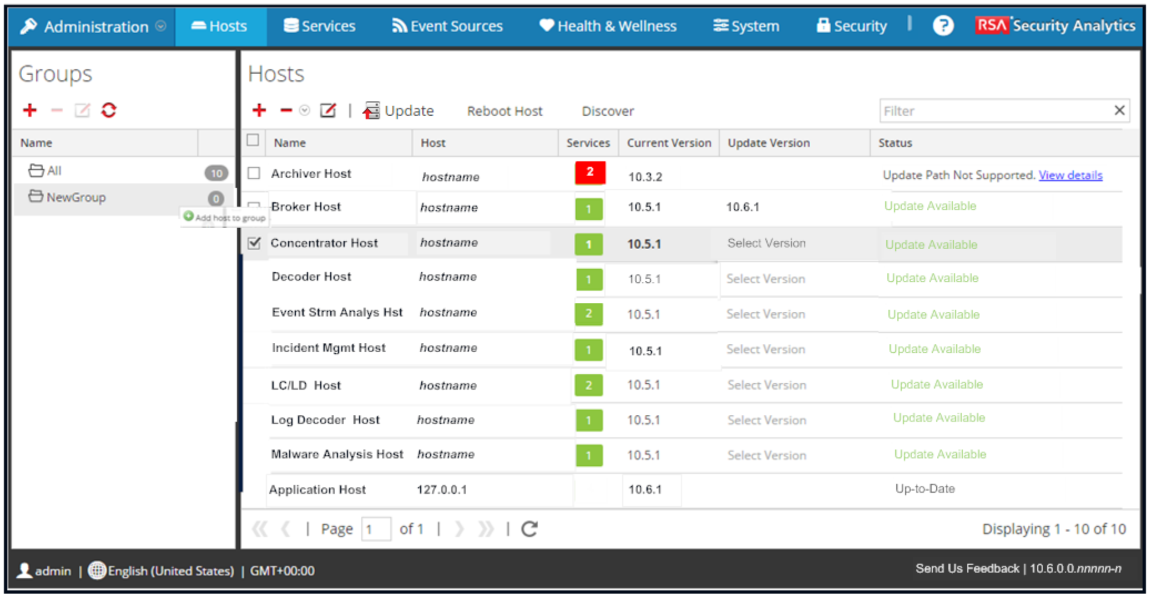
   The name field opens with a blinking cursor.

2. Type the new name of the group and press **Enter**.

   The name field closes and the new group name is displayed in the tree.

Add a Host to a Group

In the Hosts view **Hosts panel**, select a host and drag the host to a group folder in the Groups panel; for example, **NewGroup**.



Name	Count
All	10
NewGroup	0

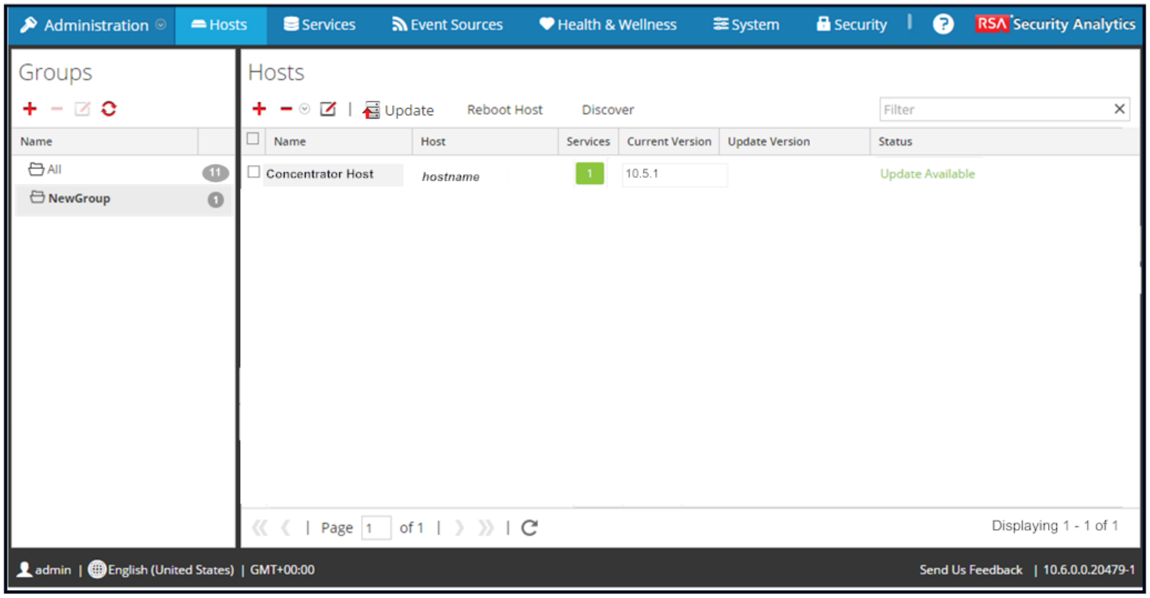
☐	Name	Host	Services	Current Version	Update Version	Status
☐	Archiver Host	hostname	2	10.3.2		Update Path Not Supported. View details
☐	Broker Host	hostname	1	10.5.1	10.6.1	Update Available
☑	Concentrator Host	hostname	1	10.5.1	Select Version	Update Available
	Decoder Host	hostname	1	10.5.1	Select Version	Update Available
	Event Strm Analys Hst	hostname	2	10.5.1	Select Version	Update Available
	Incident Mgmt Host	hostname	1	10.5.1	Select Version	Update Available
	LC/LD Host	hostname	2	10.5.1	Select Version	Update Available
	Log Decoder Host	hostname	1	10.5.1	Select Version	Update Available
	Malware Analysis Host	hostname	1	10.5.1	Select Version	Update Available
	Application Host	127.0.0.1		10.6.1		Up-to-Date

Displaying 1 - 10 of 10

The host is added to the group.

View the Hosts in a Group

To view the hosts in a group, click the group in the **Groups panel**.
The **Hosts panel** lists the hosts in that group.



Name	Count
All	11
NewGroup	1

☐	Name	Host	Services	Current Version	Update Version	Status
☐	Concentrator Host	hostname	1	10.5.1		Update Available

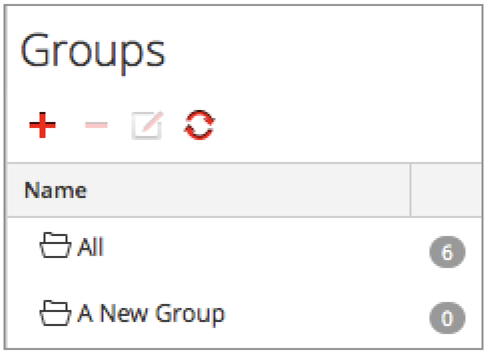
Displaying 1 - 1 of 1

Remove a Host from a Group

1. In the Hosts view **Groups panel**, select the group that contains the host that you want to remove. The hosts in that group appear in the Hosts panel.
2. In the **Hosts panel**, select one or more hosts that you want to remove from the group, and in the toolbar, select − ⌄ > **Remove fromGroup**.

   The selected hosts are removed from the group, but are not removed from the Security Analytics user interface. The number of hosts in the group, which is listed near the group name, decreases by the number of hosts removed from the group. The **All** group contains the hosts that were removed from the group.

   In the following example, the host group called **A New Group** does not contain any hosts, since the host in that group was removed.



Groups

Name	
All	6
A New Group	0

Delete a Group

1. In the Hosts view **Groups panel**, select the group that you want to delete.
2. Click −.

   The selected group is removed from the Groups panel. The hosts that were in the group are not removed from the Security Analytics user interface. The **All** group contains the hosts from the deleted group.

Free Local Update Repository Disk Space

If you do not have enough disk space in your Local Update Repository to download a version update, the Security Analytics Update Repository dialog is displayed with the contents and disk space status of the repository. You can delete a version or version that you do not need to free enough disk space to download the version you want.

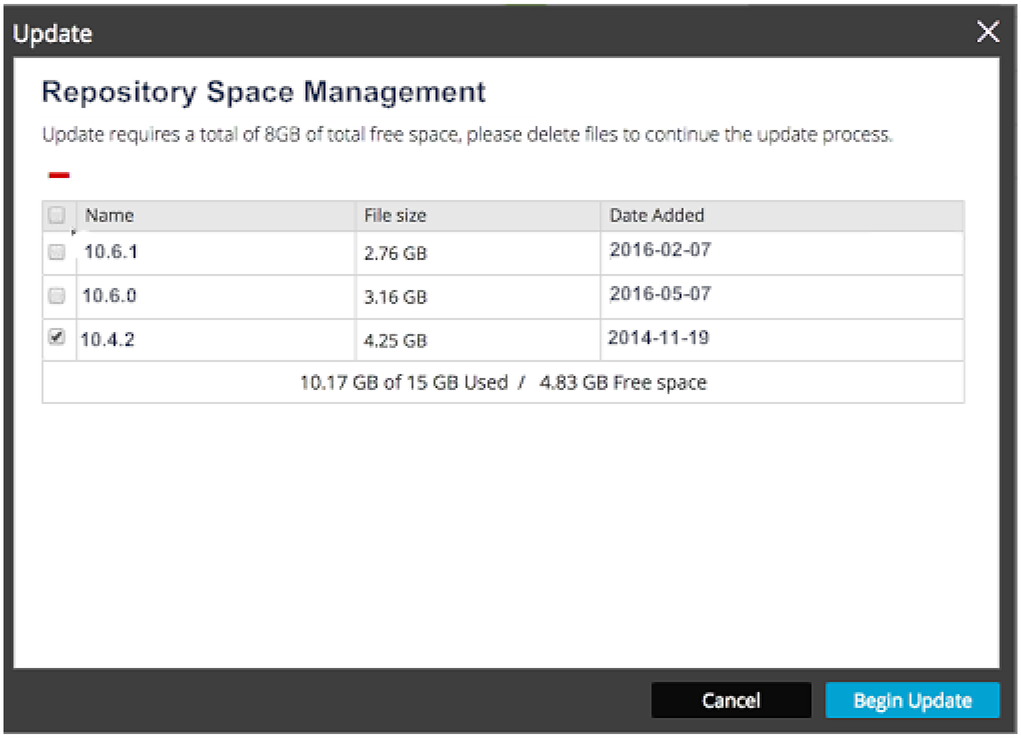
Procedure

To free disk space in your Local Update Repository:

1. Select the version you want from the Hosts view.

   If you do not have enough disk space in your Local Update Repository to download the version, the Repository Space Management dialog is displayed.

2. Select a version, or versions, to delete.



Update

Repository Space Management

Update requires a total of 8GB of total free space, please delete files to continue the update process.

▬

□	Name	File size	Date Added
□	10.6.1	2.76 GB	2016-02-07
□	10.6.0	3.16 GB	2016-05-07
☑	10.4.2	4.25 GB	2014-11-19

10.17 GB of 15 GB Used / 4.83 GB Free space

3. Click ▬ .

4. Click **Begin Update**.

Remove a Host

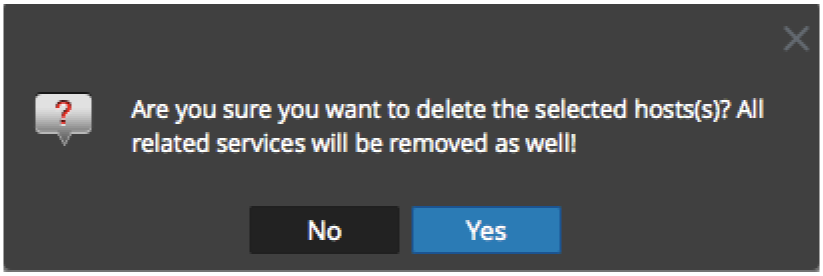
Removing a host is a host management task that you can complete in the Administration Hosts view. Hosts View provides additional information about the host management features available in the Hosts view.

Remove a Host

Follow this procedure to remove a host that is no longer needed from the Security Analytics user interface along with its associated services. If you remove a host, you can no longer view the host and its associated services from within Security Analytics.

1. In the Security Analytics menu, select **Administration > Hosts**.
2. In the **Hosts** view, select a host that you want to remove, and in the toolbar, select − ⌄ > **Remove Host**.

   A warning dialog is displayed.

   Are you sure you want to delete the selected hosts(s)? All related services will be removed as well!

3. To remove the host, click **Yes**.

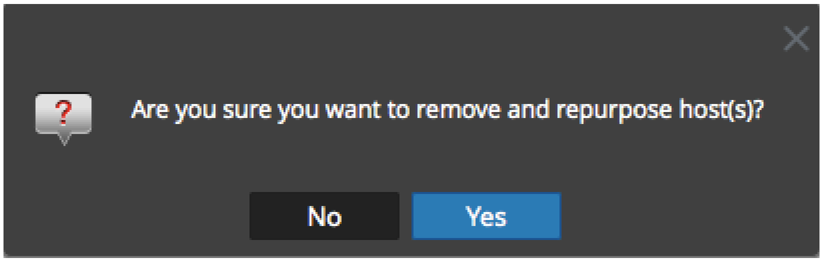
   The selected host and its associated services are removed and you can no longer view them from within Security Analytics.

Remove a Host and Repurpose

Follow this procedure when you want to completely rebuild a host. This option is only available on the Primary Security Analytics server of the host.

1. In the Security Analytics menu, select **Adminstration > Hosts**.
2. In the **Hosts** view, select a host that you want to remove and repurpose, and in the toolbar, select − ⌄ > **Remove and Repurpose Host**.

A warning dialog is displayed.



Are you sure you want to remove and repurpose host(s)?

3. To remove and repurpose the host, click **Yes**.

Search for Hosts

You can search for hosts from a list of hosts in the Administration Hosts view. The Hosts view enables you quickly filter the list of hosts by Name and Host. It is possible to have numerous Security Analytics hosts in use for various purposes. Instead of scrolling through the host list, you can quickly filter the host list to locate the hosts that you want to administer.

In the Administration Services view, you can search for a service and quickly find the host that runs that service.

Search for a Host

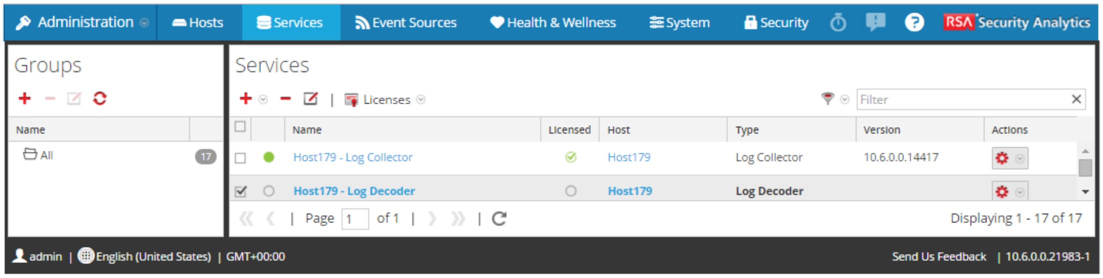
1. In the Security Analytics menu, select **Administration > Hosts**.
2. In the **Hosts panel** toolbar, type a host **Name** or **Hostname** in the **Filter** field.

   The Hosts panel lists the hosts that match the names entered in the Filter field.

Find the Host that Runs a Service

1. In the Security Analytics menu, select **Administration** > **Services**.

2. In the Services view, select a service. The associated host is listed in the **Host** column for that service.

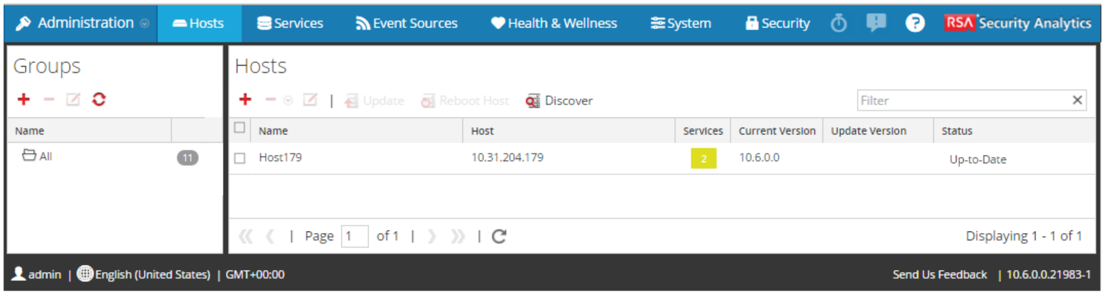


Name	
All	17

☐		Name	Licensed	Host	Type	Version	Actions
☐	●	Host179 - Log Collector	✓	Host179	Log Collector	10.6.0.0.14417	
☑	○	Host179 - Log Decoder	○	Host179	Log Decoder		

Displaying 1 - 17 of 17

3. To administer the host in the Hosts view, click the link in the **Host** column for that service. The host associated with the selected service is displayed in the Hosts view.



Name	
All	11

☐	Name	Host	Services	Current Version	Update Version	Status
☐	Host179	10.31.204.179	2	10.6.0.0		Up-to-Date

Displaying 1 - 1 of 1

Update Hosts in Correct Sequence

You must follow a specific sequence when you update hosts to a new version. RSA recommends that you follow the guidelines described in this topic.

Basic Update Sequence

RSA strongly recommends that customers:

- Update all hosts at the same time (during the same session).

> **Note:** If you stagger the update over multiple sessions:
> - You will not lose data.
> - You may not have all the features operational until you update your entire deployment.

- Update hosts in a the following order:

   1. Security Analytics Servers

      > **Note:** The Security Analytics Server is the host the on which the Security Analytics Server resides.

   2. Event Stream Analysis (ESA), Malware
   3. Decoders
   4. Concentrators
   5. Archivers
   6. Brokers

- Avoid mixed-modes (for example, one host at 10.4.x, another host at 10.5.x, and another host 10.6.x in the same Security Analytics deployment).

> **Caution:** If you deploy multiple Security Analytics Servers, you must determine which host is the Primary Security Analytics Server and which hosts are the Secondary Security Analytics Servers.

Update Security Analytics in a Multiple Security Analytics Server Environment

The following section describes how to update a Multiple Security Analytics Server deployment.

Primary Security Analytics Server

After you apply updates to a Security Analytics Server, that Security Analytics Server becomes the Primary Security Analytics Server for your deployment. All other Security Analytics Servers are the secondary Security Analytics Servers. The Primary Security Analytics Server has all the Security Analytics server functionally including:

1. Fully functional **Hosts** view including the **Updates** column.
2. Access to Health & Wellness views.
3. Full use of the trusted connections feature.

Secondary Security Analytics Server

A Secondary Security Analytics Server has the following limitations:

1. The **Update Version** and **Status** columns on the **Hosts** view are valid for the Primary Security Analytics Server exclusively. They reflects the wrong status for a Secondary Security Analytics Server so **you must not interact with them**.
2. You cannot use the Health & Wellness views.
3. You cannot use the trusted connections feature.

Scenario 1. Full Update, Update Order (Strongly Recommended)

Customer v10.x deployment – 1 Security Analytics Server, 2 Decoders, 2 Concentrators, 1 Archiver, 1 Broker, 1 ESA, 1 Malware Analysis

1. Update the Security Analytics Server.
2. Update ESA and Malware Analysis.
3. Update 2 Decoders.
4. Update 2 Concentrators and Archiver.
5. Update 1 Broker.

Scenario 2. Partial Update

Customer v10.x deployment – 1 Security Analytics Server, 2 Decoders, 2 Concentrators, 1 Broker, 1 ESA, 1 Malware Analysis

1. Update the Security Analytics Server.
2. Update ESA and Malware Analysis.

3. Update 1 Decoder and 1 Concentrator.

   Time elapses during which Security Analytics processes a significant amount of data.

4. Update 1 Decoder, 1 Concentrator, and 1 Broker.

Scenario 3. Regional Update with Multiple Brokers

Customer v10.x deployment – 4 Decoders, 4 Concentrators, 2 Brokers, 1 Security Analytics Server, 1 ESA, 1 Malware Analysis (2 sites, each with 2 Decoders, 2 Concentrators, and 1 Broker)

First Update Session at Site 1

1. Update the Security Analytics Server.
2. Update ESA and Malware Analysis.
3. Update 2 Decoders, 2 Concentrators, and 1 Broker at site 1.

Second Update Session at Site 2

Update 2 Decoders, 2 Concentrators, and 1 Broker at site 2.

Scenario 4. Regional Update with Multiple Security Analytics Servers

Customer v10.x deployment – 2 Security Analytics Servers, 4 Decoders, 4 Concentrators, 2 Brokers, 1 ESA, 1 Malware Analysis (2 sites, each with 1 Security Analytics Server, 2 Decoders, 2 Concentrators, and 1 Broker)

First Update Session at Site 1

1. Update the Primary Security Analytics Server.
2. Update ESA and Malware Analysis.
3. Update 2 Decoders, 2 Concentrators, and 1 Broker at site 1.

Second Update Session at Site 2

1. Update the Secondary Security Analytics Server.
2. Update 2 Decoders, 2 Concentrators, and 1 Broker at site 2.

Host Procedures from the Task List Dialog

You use the Host Task List dialog to manage tasks that relate to a host and its communications with the network. Several service and host configuration options are available for Core hosts. The following topics describe:

- How to use the Host Task List Dialog.
- The tasks you can perform from the Host Task List dialog.

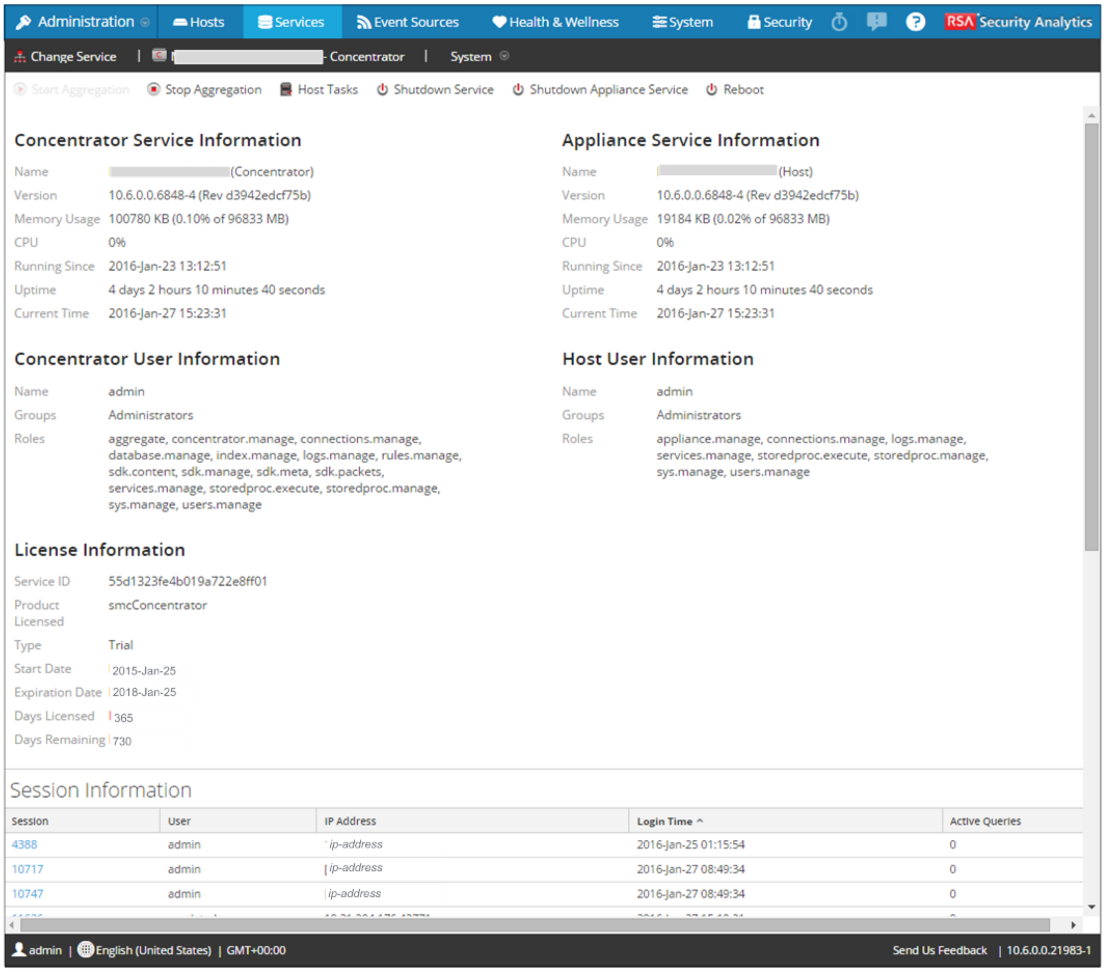
Topics

- Execute a Task From the Host Task List
- Add and Delete a Filesystem Monitor
- Reboot a Host
- Set Host Built-In Clock
- Set Network Configuration
- Set Network Time Source
- Set SNMP
- Set Syslog Forwarding
- Show Network Port Status
- Show Serial Number
- Shut Down Host
- Stop and Start a Service on a Host

Execute a Task From the Host Task List

1. In the **Security Analytics menu**, select **Administration >Services**.
2. In the **Services** grid, select a service and ⚙ ⌄ > **View> System**.

   The System view for the service is displayed.



Concentrator Service Information

Name	[redacted] (Concentrator)
Version	10.6.0.0.6848-4 (Rev d3942edcf75b)
Memory Usage	100780 KB (0.10% of 96833 MB)
CPU	0%
Running Since	2016-Jan-23 13:12:51
Uptime	4 days 2 hours 10 minutes 40 seconds
Current Time	2016-Jan-27 15:23:31

Appliance Service Information

Name	[redacted] (Host)
Version	10.6.0.0.6848-4 (Rev d3942edcf75b)
Memory Usage	19184 KB (0.02% of 96833 MB)
CPU	0%
Running Since	2016-Jan-23 13:12:51
Uptime	4 days 2 hours 10 minutes 40 seconds
Current Time	2016-Jan-27 15:23:31

Concentrator User Information

Name	admin
Groups	Administrators
Roles	aggregate, concentrator.manage, connections.manage, database.manage, index.manage, logs.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Host User Information

Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

License Information

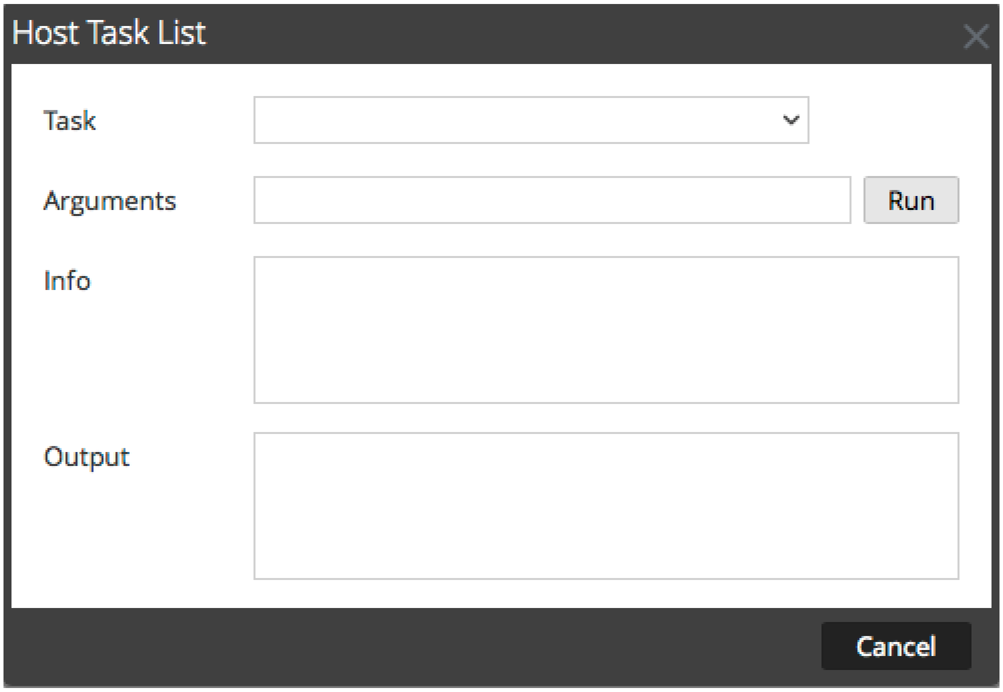
Service ID	55d1323fe4b019a722e8ff01
Product Licensed	smcConcentrator
Type	Trial
Start Date	2015-Jan-25
Expiration Date	2018-Jan-25
Days Licensed	365
Days Remaining	730

Session Information

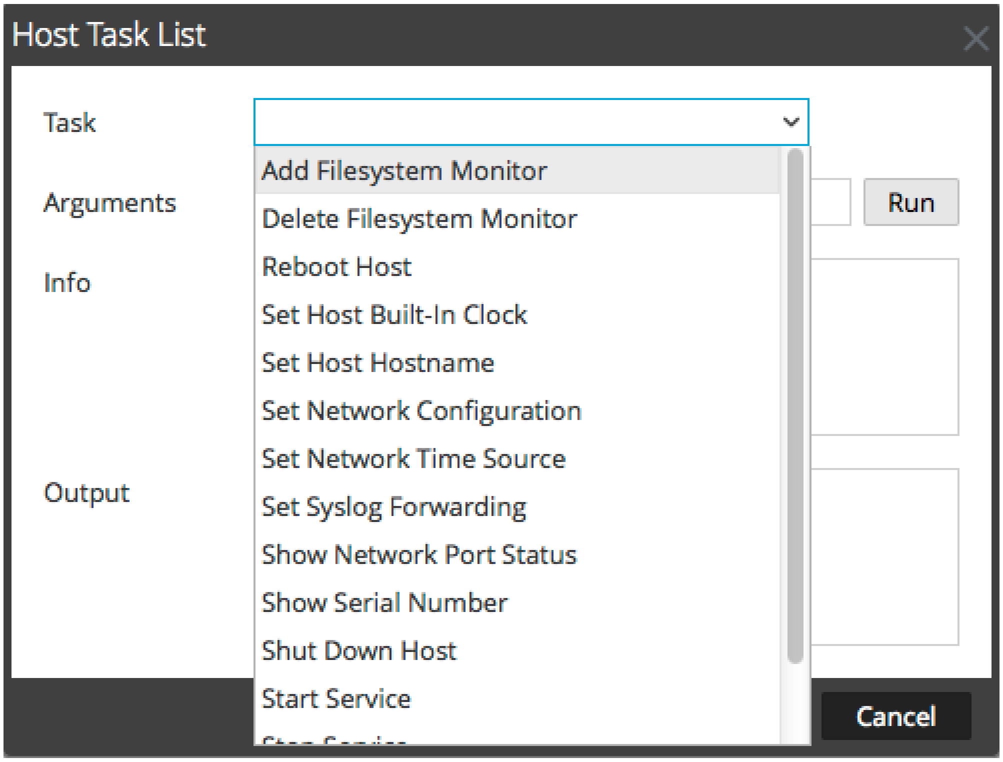
Session	User	IP Address	Login Time ^	Active Queries
4388	admin	*ip-address*	2016-Jan-25 01:15:54	0
10717	admin	*ip-address*	2016-Jan-27 08:49:34	0
10747	admin	*ip-address*	2016-Jan-27 08:49:34	0

admin | English (United States) | GMT+00:00
Send Us Feedback | 10.6.0.0.21983-1

3. In the **Services System view** toolbar, click **Host Tasks**.

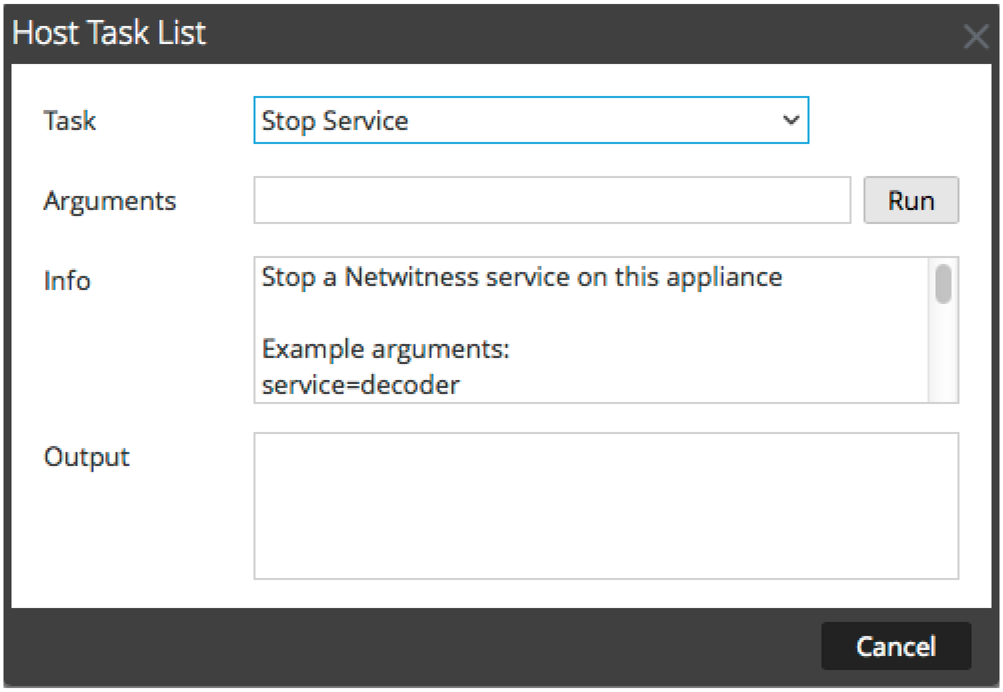


4. In the **Host Task List,** click in the **Task** field to display a drop-down list of tasks that run on a host.



5. Select a task; for example, click **Stop Service**.

   The task is displayed in the **Task** field and task description, example arguments, security roles, and parameters are displayed in the **Info** area.



Task: Stop Service

Info: Stop a Netwitness service on this appliance

Example arguments:
service=decoder

6. Type arguments if necessary and click **Run**.

   The command executes and the result is displayed in the **Output** section.

Add and Delete a Filesystem Monitor

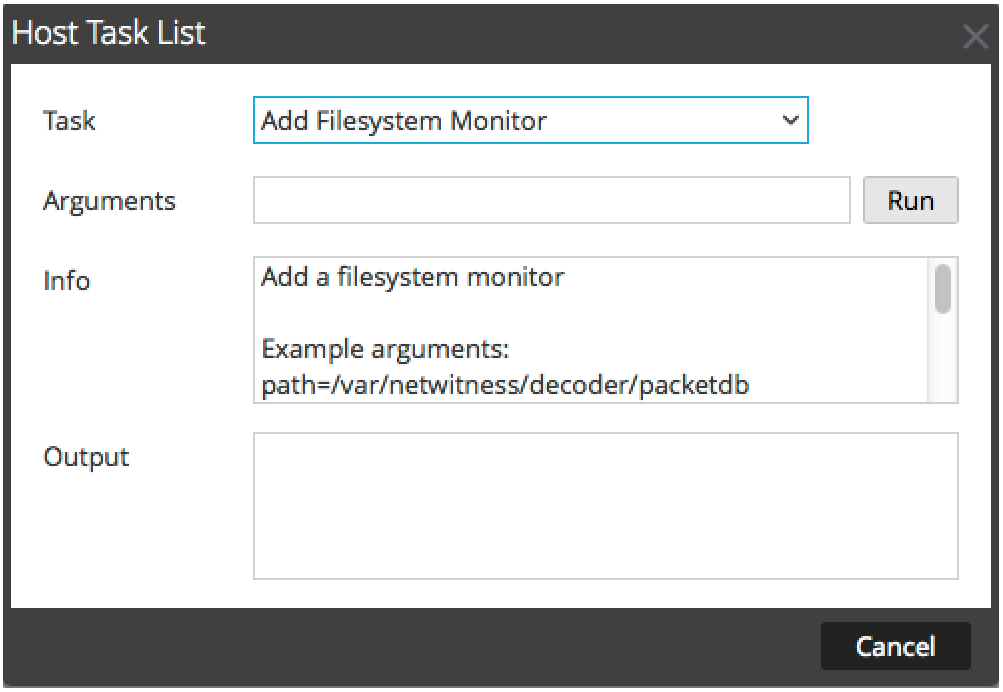
When you want a service to monitor traffic on a specific file system, you can select the service and then specify the path. Security Analytics adds a file system monitor. Once a file system monitor is added to a service, the service continues to monitor traffic on that path until the file system monitor is deleted.

Configure the Filesystem Monitor

1. In the **Security Analytics menu**, select **Administration >Services**.
2. In the **Services** grid, select a service and ⚙ > **View** > **System**.

   The System view for the service is displayed.
3. In the **Services System view** toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **Add Filesystem Monitor**.

   In the **Info** area, a brief explanation of the task and the task arguments is displayed.



Task: Add Filesystem Monitor

Info: Add a filesystem monitor

Example arguments:
path=/var/netwitness/decoder/packetdb

5. To identify the filesystem to monitor, type the path in the **Arguments** field. For example:

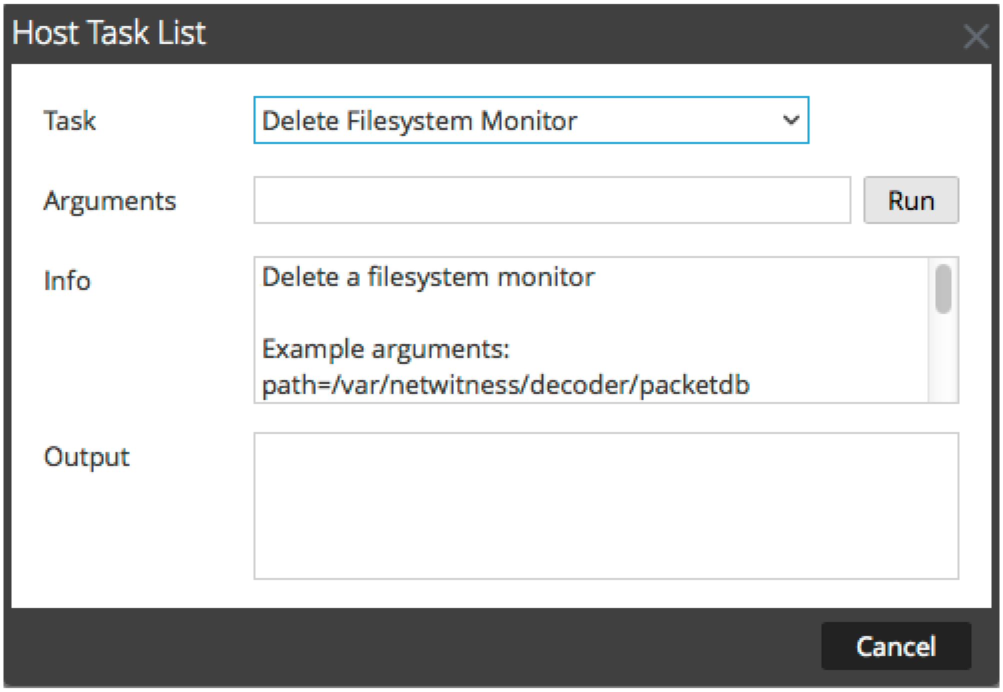
   path=/var/netwitness/decoder/packetdb
6. Click **Run**.

   The result is displayed in the **Output** area. The service begins to monitor the file system and continues to monitor it until you delete the filesystem monitor.

Delete a Filesystem Monitor

1. Navigate to the **Host Task List** dialog.
2. In the **Host Task List**, select **Delete Filesystem Monitor**.

   In the **Info** area, a brief explanation of the task and the task arguments is displayed.



Host Task List

Task: Delete Filesystem Monitor

Arguments

Info: Delete a filesystem monitor

Example arguments:
path=/var/netwitness/decoder/packetdb

Output

3. To identify the filesystem to stop monitoring, type the path in the **Arguments** field. For example:

   path=/var/netwitness/decoder/packetdb
4. Click **Run**.

   The result is displayed in the **Output** area. The service stops monitoring the file system.

Reboot a Host

Under certain conditions it is necessary to reboot a host; for example, after installing a software upgrade. This procedure uses a Host Task List message to shut down and restart a host.

Security Analytics also offers other options for shutting down a host:

- To shut down and restart a host through an attached service, go to the Hosts view from a service in the Services view (see Search for Hosts) and then follow the *Shut Down and Restart a Host from the Hosts View* procedure below.
- To shut down the physical host without restarting, see Shut Down Host.

Shut Down and Restart a Host from the Hosts View

1. In the **Security Analytics menu**, select **Administration** > **Hosts**.
2. In the **Hosts** panel, select a host.
3. Select Reboot Host from the toolbar.

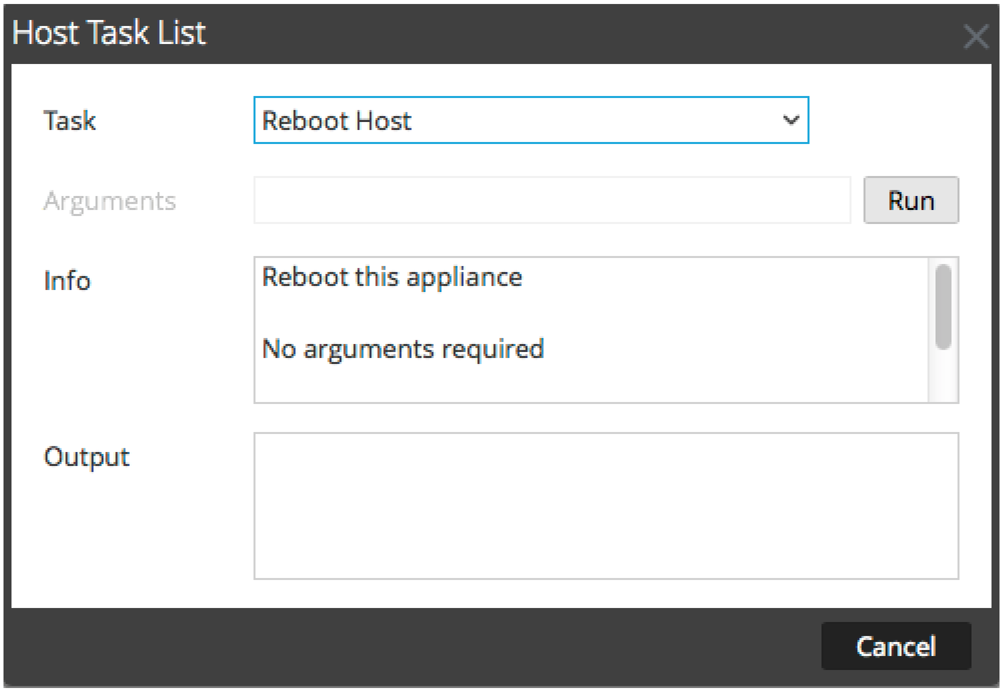
Shut Down and Restart a Host from the Host Task List

1. In the **Security Analytics menu**, select **Administration** >**Services**.
2. In the **Services** panel, select a service and ⚙ ⌄ > **View**> **System**.

   The System view for the service is displayed.
3. In the **Services System view** toolbar**,** click **Host Tasks**.

4. In the **Host Task List**, select **Reboot Host** in the **Task** field.

   No arguments are required.



Task: Reboot Host

Info: Reboot this appliance

No arguments required

5. Click **Run**.

   The host is rebooted and the result is displayed in the **Output** area.

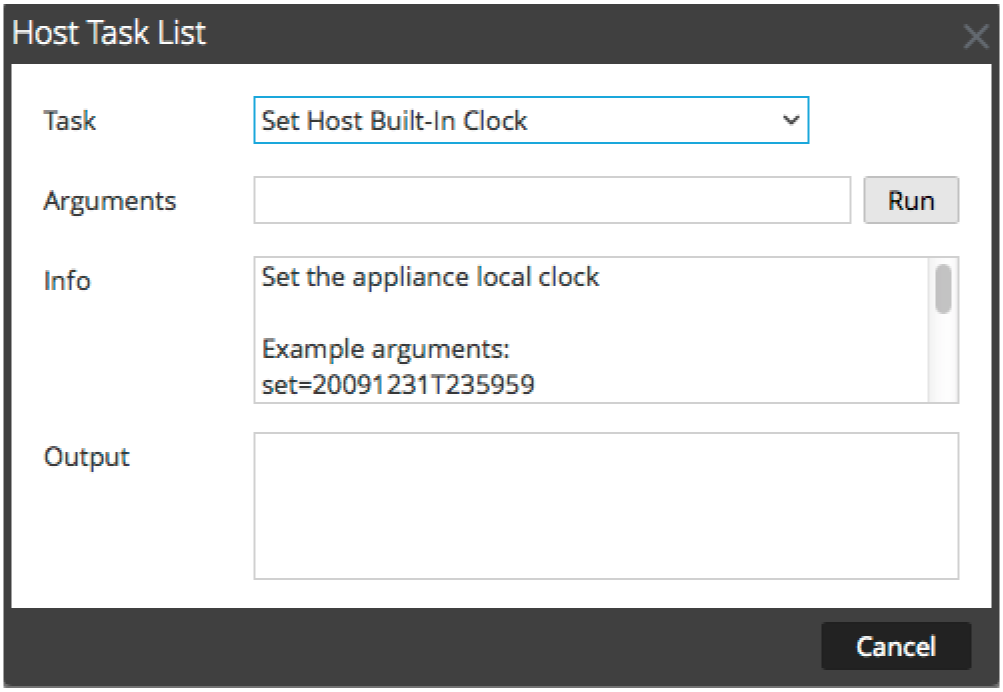
Set Host Built-In Clock

After a shutdown or battery failure, it may be necessary to set the local clock on a host. The Set Host Built-In Clock task resets the clock time.

Set the Time on the Local Clock

1. In the **Security Analytics menu**, select **Administration >Services**.
2. In the **Services** grid, select a service and ⚙ > **View> System**.

   The System view for the service is displayed.
3. In the **Services System view** toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **Set Host Built-In Clock**. Help for the task is displayed in the **Info** area.



Task: Set Host Built-In Clock

Info: Set the appliance local clock

Example arguments:
set=20091231T235959

5. Enter the date and time arguments in the **Arguments** field; for example, to specify October 7, 2014 at 11:59:59 PM, type:

   set=20141007T235959
6. Click **Run**.

   The clock is set to the specified time and a message is displayed in the **Output** area.

Set Network Configuration

When a configured Core host needs its address changed, you can set a new network address, subnet mask, and gateway for the host using the **Set Network Configuration** message in the **Host Task List**.

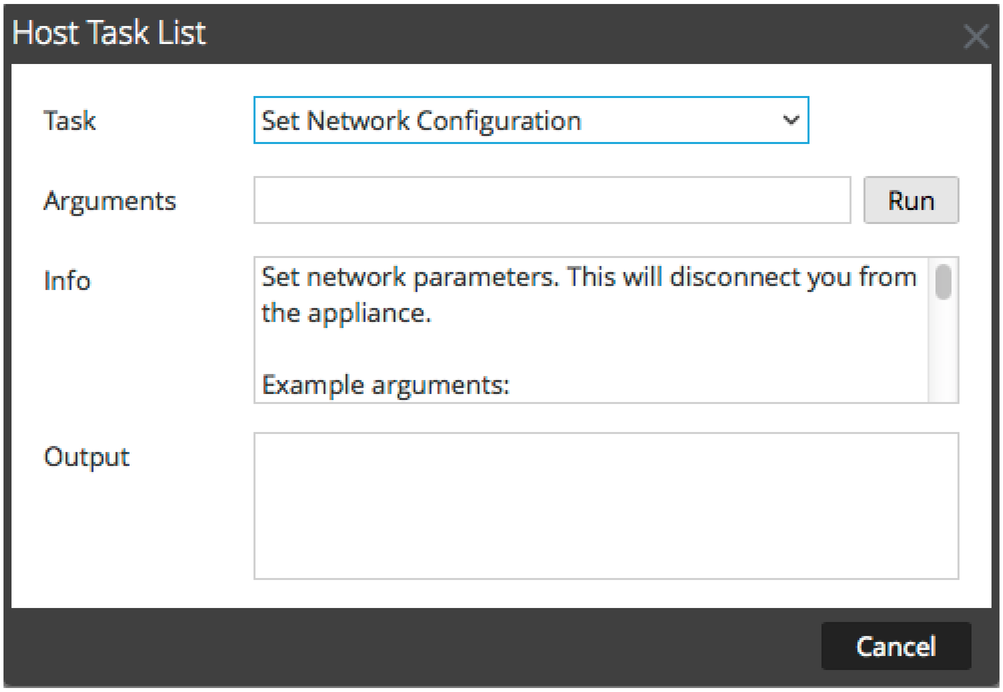
Caution: The change goes into effect immediately, and the host is disconnected from Security Analytics. You must then add the host to Security Analytics again using the new network address.

Specify the Network Address for a Host

1. In the **Security Analytics menu**, select **Administration >Services**.
2. In the **Services** grid, select a service and ⚙ > **View> System**.

   The System view for the service is displayed.
3. In the **Services System view** toolbar**,** click **Host Tasks**.
4. In the **Host Task List**, click **Set Network Configuration**.

   The task is displayed in the **Task** field and help is displayed in the **Info** area.



Task: Set Network Configuration

Info: Set network parameters. This will disconnect you from the appliance.

Example arguments:

5. Enter the arguments in the **Arguments** field. For example:

   mode=static address=192.168.0.20 netmask=255.255.255.0 gateway=192.168.0.1

6. Click **Run.**

   The task executes and the result is displayed in the **Output** area. The host is disconnected from Security Analytics. You must add the host again with the new address.

Note: If the mode is DHCP, there may be no way to determine the new address. You may have to connect to the host directly to determine the new address.

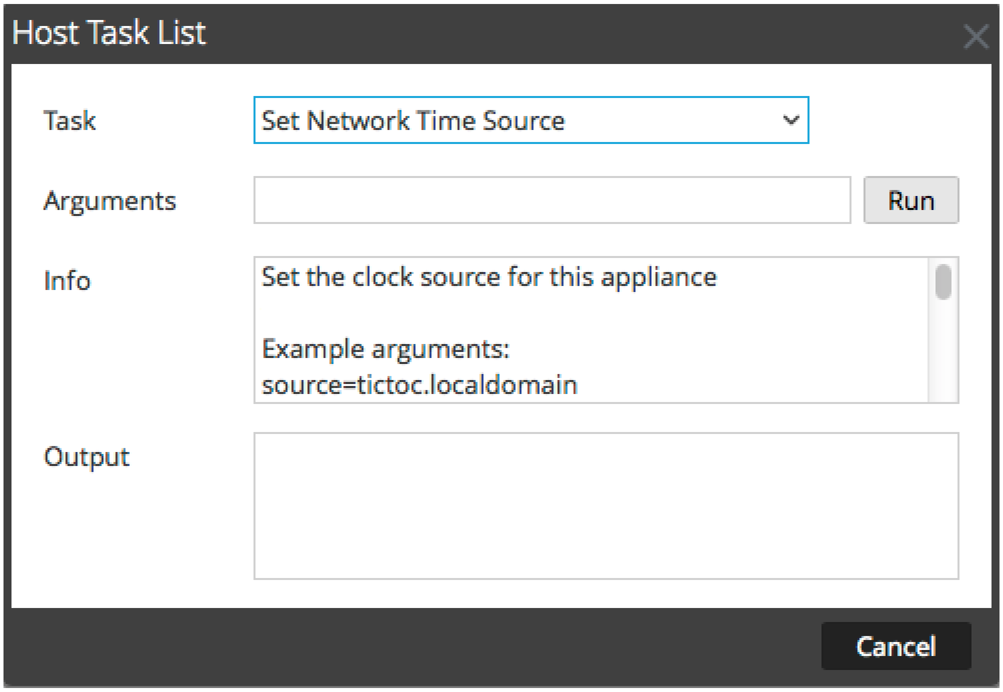
Set Network Time Source

When setting the clock source for a host, set the hostname or address of an NTP server to be the network clock source for the host. If the host is using a local clock source, you must specify **local** here to allow **Set the Local Clock Source** to be effective.

Specify the Network Clock Source

1. In the **Security Analytics menu**, select **Administration >Services**.
2. In the **Services** grid, select a service and ⚙ ⌄ **View> System**.

   The System view for the service is displayed.
3. In the **Services System view** toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **Set Network Time Source**.



Task Set Network Time Source

Arguments

Info Set the clock source for this appliance

Example arguments:
source=tictoc.localdomain

Output

5. Do one of the following:
   - Type the hostname or address of the NTP server to serve as the clock source for this host; for example: **source=tictoc.localdomain**
   - If you want to use the host clock as a clock source, type:

     source=local

6. Click **Run**.

   The clock source is set and a message is displayed in the **Output** area.

Note: If you specified a NTP clock source of **local**, the host clock serves as the clock source and the time is configured using Set Host Built-In Clock.

Set SNMP

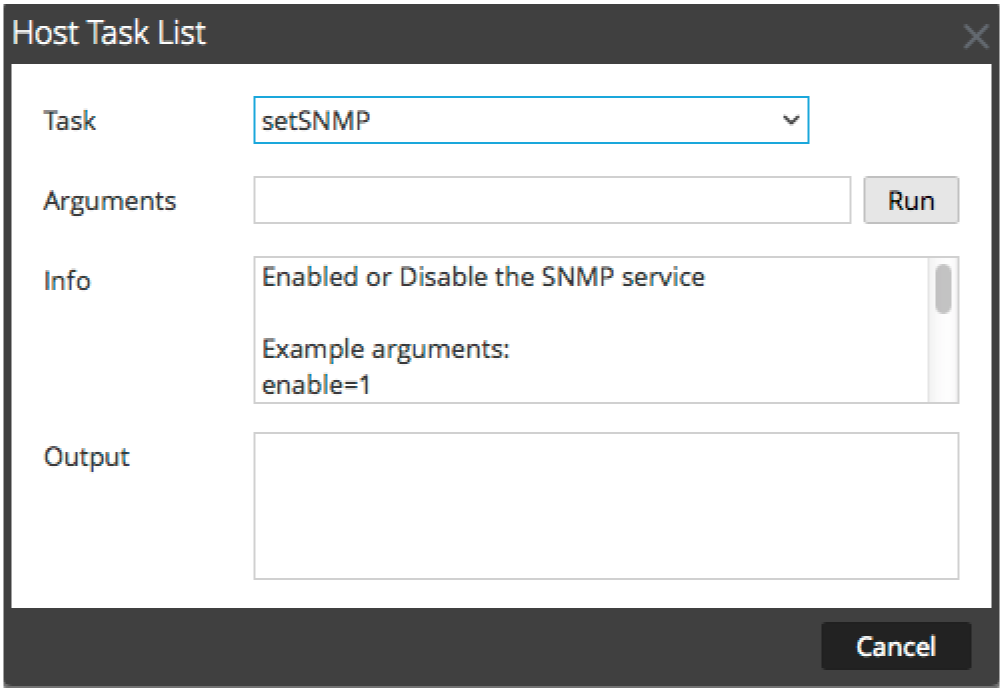
Set SNMP in the Host Task List enables or disables the SNMP service on a host. In order for a host to receive SNMP notifications, the SNMP service needs to be enabled. If you are not using SNMP for Security Analytics notifications, it is not necessary to enable the service.

Toggle SNMP Service on the Host

1. In the **Security Analytics menu**, select **Administration** >**Services**.
2. In the **Services** grid, select a service and ⚙ ⌄ > **View**> **System**.

   The System view for the service is displayed.
3. In the **Services System view** toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **setSNMP**.

   In the **Info** area, a brief explanation of the task and the task arguments is displayed.



Task: setSNMP

Arguments:

Info: Enabled or Disable the SNMP service

Example arguments:
enable=1

Output

5. Do one of the following:
   - If you want to disable the service, type **enable=0** in the **Arguments** field.
   - If you want to enable the service, type **enable=1** in the **Arguments** field.

6. Click **Run**.

   The result is displayed in the **Output** area.

Set Syslog Forwarding

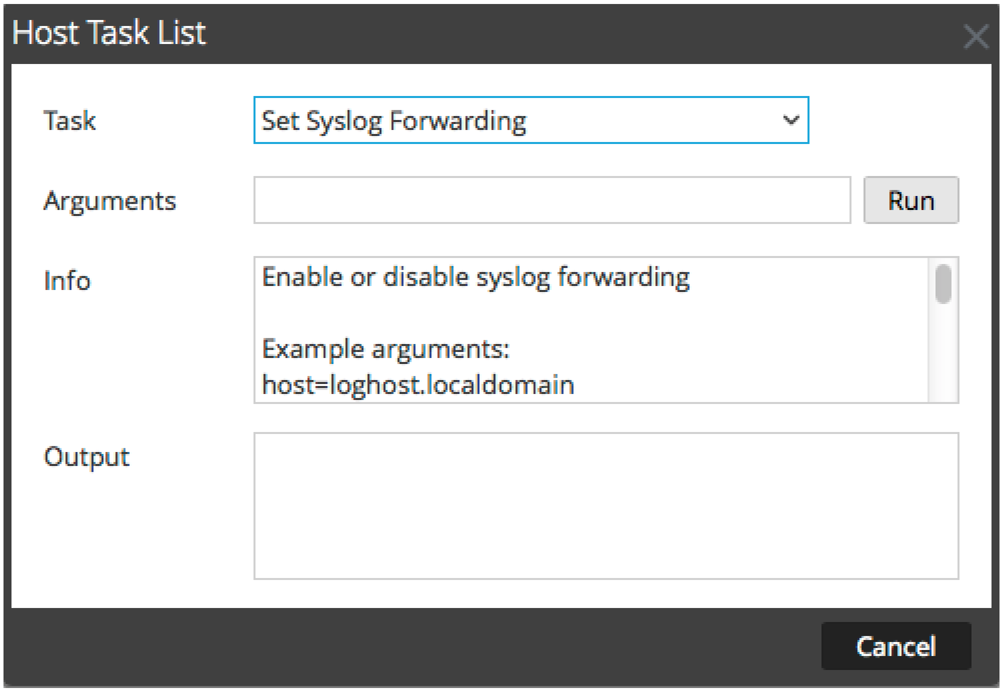
You can configure Syslog forwarding to forward the operating system logs of your Security Analytics Hosts to a remote syslog server. You can use the Set Syslog Forwarding task in the Host Task List to enable or disable syslog forwarding.

Set Up and Start Syslog Forwarding

1. In the **Security Analytics menu**, select **Administration >Services**.
2. In the **Services** grid, select a service and ⚙ >**View**> **System**.

   The System view for the service is displayed.
3. In the **Services System view** toolbar**,** click **Host Tasks**.
4. In the **Host Task List**, select **Set Syslog Forwarding**.

   In the **Info** area, a brief explanation of the task and the task arguments is displayed.



Host Task List

Task: Set Syslog Forwarding

Arguments:

Info: Enable or disable syslog forwarding

Example arguments:
host=loghost.localdomain

Output:

5. In the **Arguments** field, do any one of the following.
   - To enable syslog forwarding, specify any one of the following formats:
     - **host=<loghost>.<localdomain>** (for example, host=syslogserver.local).
     - **host=<loghost>.<localdomain>:<port>** (for example, host=syslogserver.local:514).

- **host=<IP>** (for example, host=10.31.244.244).
- **host=<IP>:<port>** (for example, host=10.31.244.244:514).

  The following table lists the parameters used to enable syslog forwarding and its descriptions.

Parameter	Description
loghost	The host name of the remote syslog server.
localdomain	The domain of the remote syslog server.
port	IP address of the remote syslog server.
IP	The port number on which the remote syslog server receives a syslog messages.

- To disable syslog forwarding, type **host=disable**.

6. Click **Run**.

   The result is displayed in the **Output** area.

Once syslog forwarding is enabled or disabled, the /etc/rsyslog.conf file is updated automatically to enable or disable syslog forwarding to the remote syslog destination and the syslog service is restarted.

If you enable syslog forwarding, the logs from the configured service are forwarded to the defined syslog server and continues forwarding until disabled.

Note: You can now log in to the remote syslog server and verify if the messages are being received from the Security Analytics services configured for syslog forwarding.

Show Network Port Status

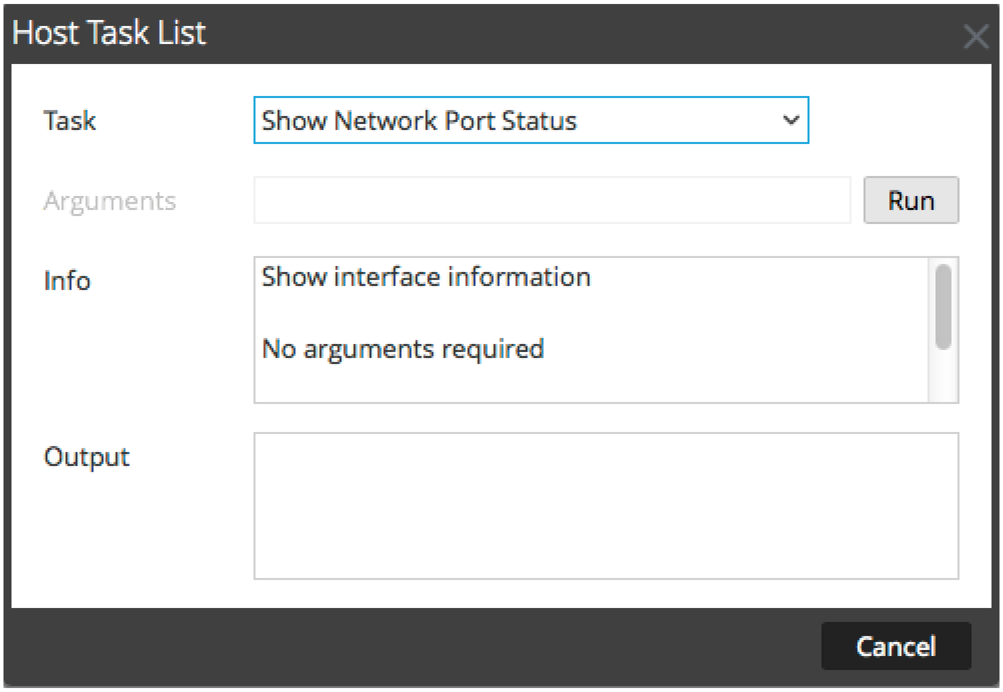
The Show Network Port Status task in the Host Task List gives you the status of all configured ports on the host.

Display the Network Port Status

1. In the **Security Analytics menu**, select **Administration** >**Services**.
2. In the **Services** grid, select a service and ⚙ ⌄ > **View**> **System**.

   The System view for the selected service is displayed.
3. In the **Services System view** toolbar, click **Host Tasks**.
4. In the **Host Task List**, click **Show Network Port Status**.

   The task is displayed in the **Task** field, and information about the task is displayed in the **Info** area.



Host Task List

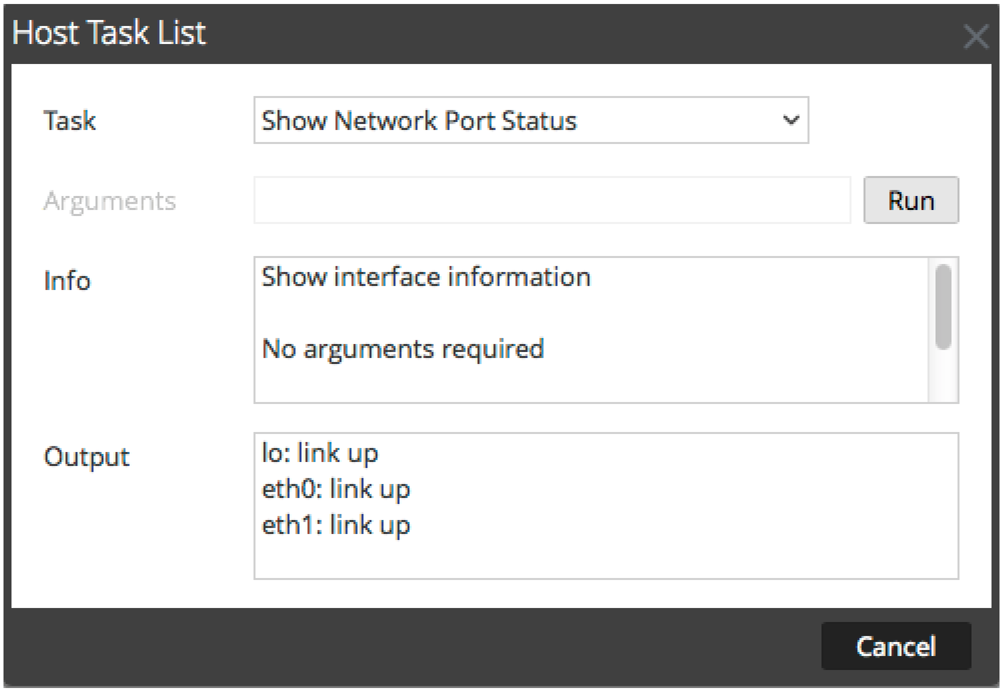
Task: Show Network Port Status

Info: Show interface information

No arguments required

5. To execute the task, click **Run**.

   The status for each port on the host is displayed in the **Output** area.



Task Show Network Port Status

Arguments

Info Show interface information

No arguments required

Output

```
lo: link up
eth0: link up
eth1: link up
```

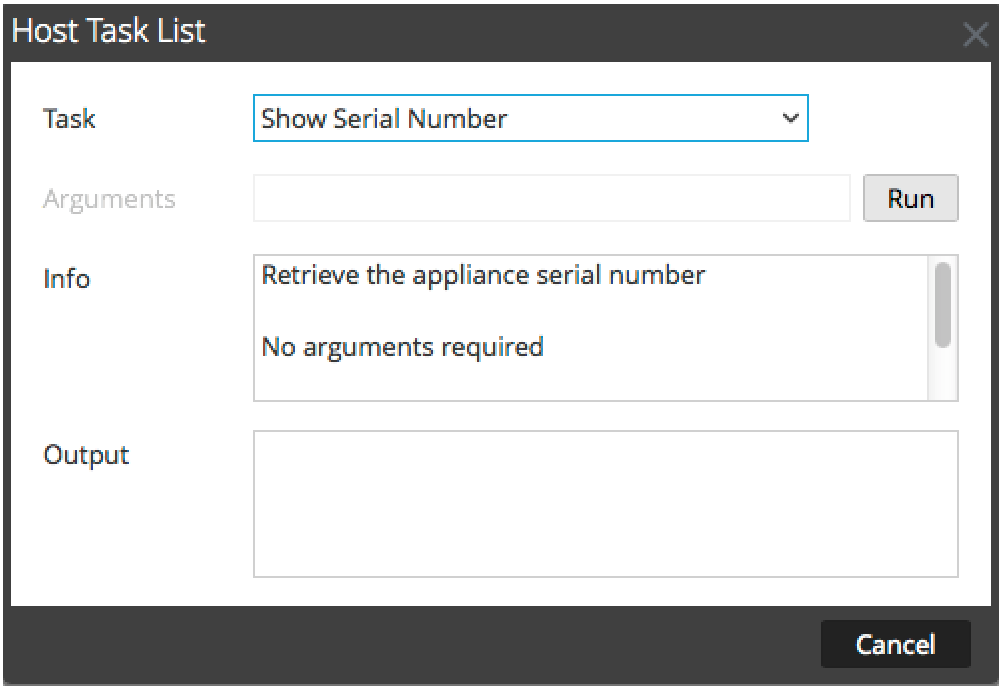
Show Serial Number

The Show Serial Number task in the Host Task List gives you the serial number of a host.

Show the Serial Number

1. In the **Security Analytics menu**, select **Administration** >**Services**.
2. In the **Services** grid, select a service and ⚙ > **View**> **System**.

   The System view for the service is displayed.
3. In the **Services System view** toolbar, click **Host Tasks**.
4. In the **Host Task List**, select **Show Serial Number**.
5. In the **Info** area, a brief explanation of the task and the task arguments is displayed.



Host Task List

Task Show Serial Number

Arguments

Info Retrieve the appliance serial number

No arguments required

Output

6. No arguments are required for this task. Click **Run**.

   The serial number of the selected host is displayed in the **Output** area.

Shut Down Host

Under certain circumstances; for example, a hardware upgrade or an extended power outage that exceeds backup power capacity, it may be necessary to shut down a physical host. When you shut down a host, all services running on the host are stopped and the physical host turns off.

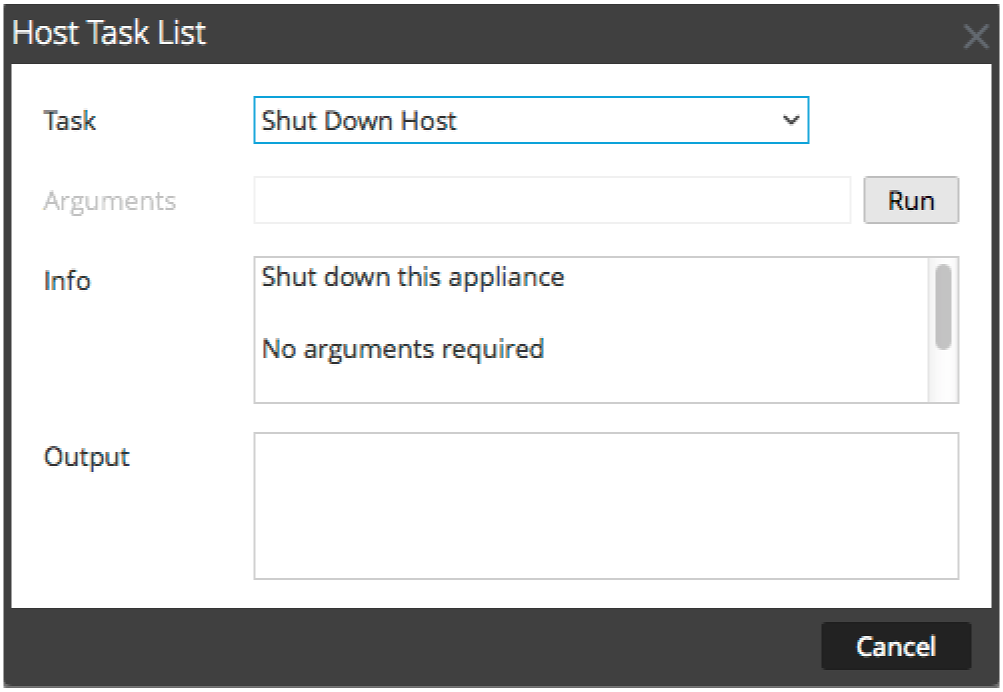
The physical host does not restart automatically; instead the power switch must be used to restart the host. Once the physical host restarts, the host and services are configured to restart automatically.

Security Analytics offers other options for starting and stopping a host that do not shut down the physical host:

- To shut down and restart a host through an attached service, see Reboot a Host.
- To shut down and restart a host using a host task, see Reboot a Host.

Shut Down the Physical Host

1. In the HostTask List dialog, select **Shut Down Host** in the **Task** field.



Task: Shut Down Host

Info: Shut down this appliance

No arguments required

2. To execute the task, click **Run**.

   The host shuts down, and the physical host turns off.

Stop and Start a Service on a Host

The Host Task List has two options for stopping and starting a service on a host. When you stop a service using the **Stop Service** message, all processes of the service are stopped and users connecting to the service are disconnected. Unless there is a problem with the service, it restarts automatically. This is the same as the **Shutdown Service** option in the Services System View.

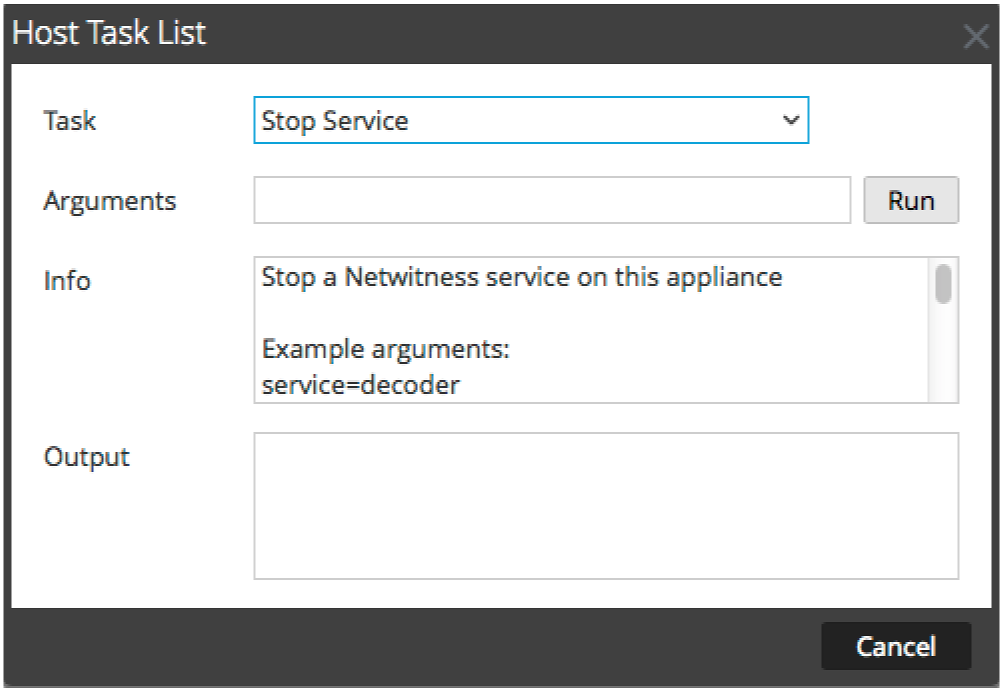
If a service does not restart automatically after being stopped, you can restart it manually using the **Start Service** message.

Stop a Service on a Host

1. In the **Security Analytics menu**, select **Administration** >**Services**.
2. In the **Services** grid, select a service and ⚙ > **View**> **System**.

   The System view for the service is displayed.
3. In the **Services System view** toolbar, click **Host Tasks**.
4. In the **Host Task List**, click **Stop Service**.

   The task is displayed in the **Task** field, and information about the task is displayed in the **info** area.



Task: Stop Service

Info: Stop a Netwitness service on this appliance

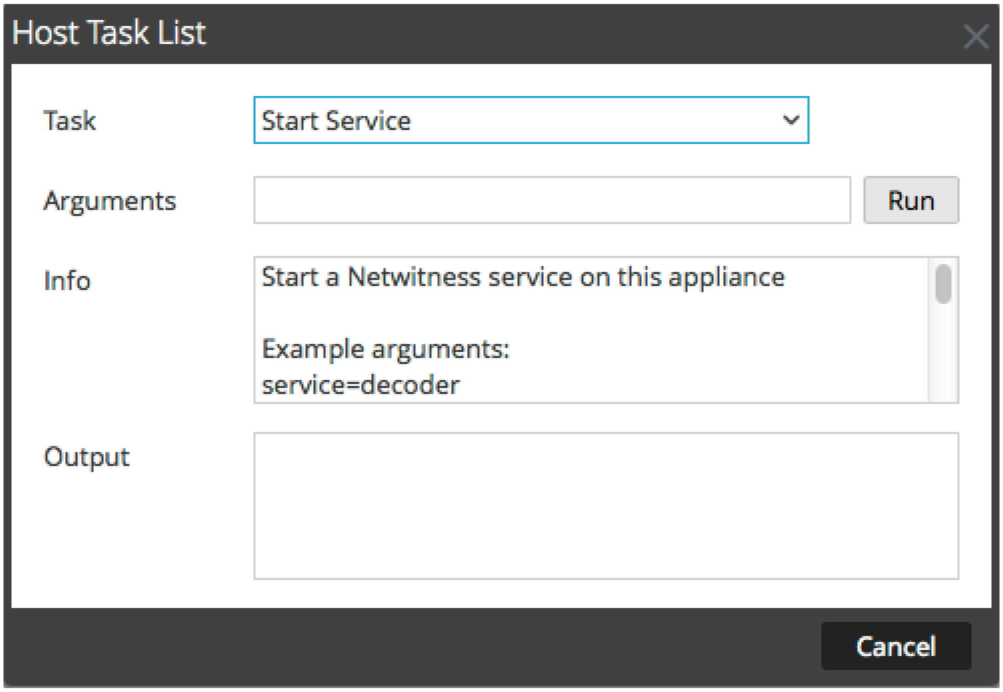
Example arguments:
service=decoder

5. Specify the service (decoder, concentrator, broker, logdecoder, logcollector) to stop in the **Arguments** field; for example,
   service=decoder

6. To execute the task, click **Run**.
   The service stops and the status is displayed in the **Output** area. All processes of the service are stopped and users connecting to the service are disconnected. Unless there is a problem with the service, it restarts automatically.

Start a Service on a Host

1. In the **Host Task List**, click **Start Service**.
   The task is displayed in the **Task** field, and information about the task is displayed in the **info** area.



Task: Start Service

Arguments:

Info: Start a Netwitness service on this appliance

Example arguments:
service=decoder

Output:

2. Specify the service (decoder, concentrator, broker, logdecoder, logcollector) to start in the **Arguments** field; for example,
   service=decoder

3. To execute the task, click **Run**.
   The service starts and the status is displayed on the **Output** area.

Service Procedures

The following procedures describe how to:

- Assign access and permissions to a service.
- Start and stop a service.
- Review the operating status of a service.

Topics

- Add, Replicate or Delete a Service User
- Add a Service User Role
- Change a Service User Password
- Create and Manage Service Groups
- Duplicate or Replicate a Service Role
- Edit Core Service Configuration Files
- Edit or Delete a Service
- Explore and Edit Service Property Tree
- Kill a Connection to a Service
- Search for Services
- Start, Stop or Restart a Service
- View Service Details

Add, Replicate or Delete a Service User

You must add a user to a service for:

- Aggregation
- Accessing the service with the:
  - Thick client
  - REST API

Note: This topic does not apply to users who access services through the user interface on Security Analytics server. You must add those users to the system, not a service. For details, see the **Set Up a User** topic in *System Security and User Management*.

For each service user, you can:

- Configure user authentication and query handling properties for the service
- Make the user a member of a role, which has a set of permissions the user receives
- Replicate the user account to other services
- Change the service user password on selected services

Change a Service User Password provides instructions for changing the service user password across services.

Replication and Migration Considerations

When replicating a user from a Security Analytics 10.5 or later service to a Security Analytics 10.4 service, Query Timeout migrates to Query Level based on the closest level. For example, if a user has a Query Timeout of 15 minutes, the user gets a Query Level of 3 after the migration. If a user has a Query Timeout of 35 minutes, the user gets a Query Level of 2 after the migration. If a user has a Query Timeout of 45 minutes, the user gets a Query Level of 2 after the migration.

When migrating or replicating a user from a Security Analytics 10.4 service to a Security Analytics 10.5 or later service, Query Level migrates to Query Timeout based on the following definitions:

- Query Level 1 = 60 minutes
- Query Level 2 = 40 minutes
- Query Level 3 = 20 minutes

Procedures

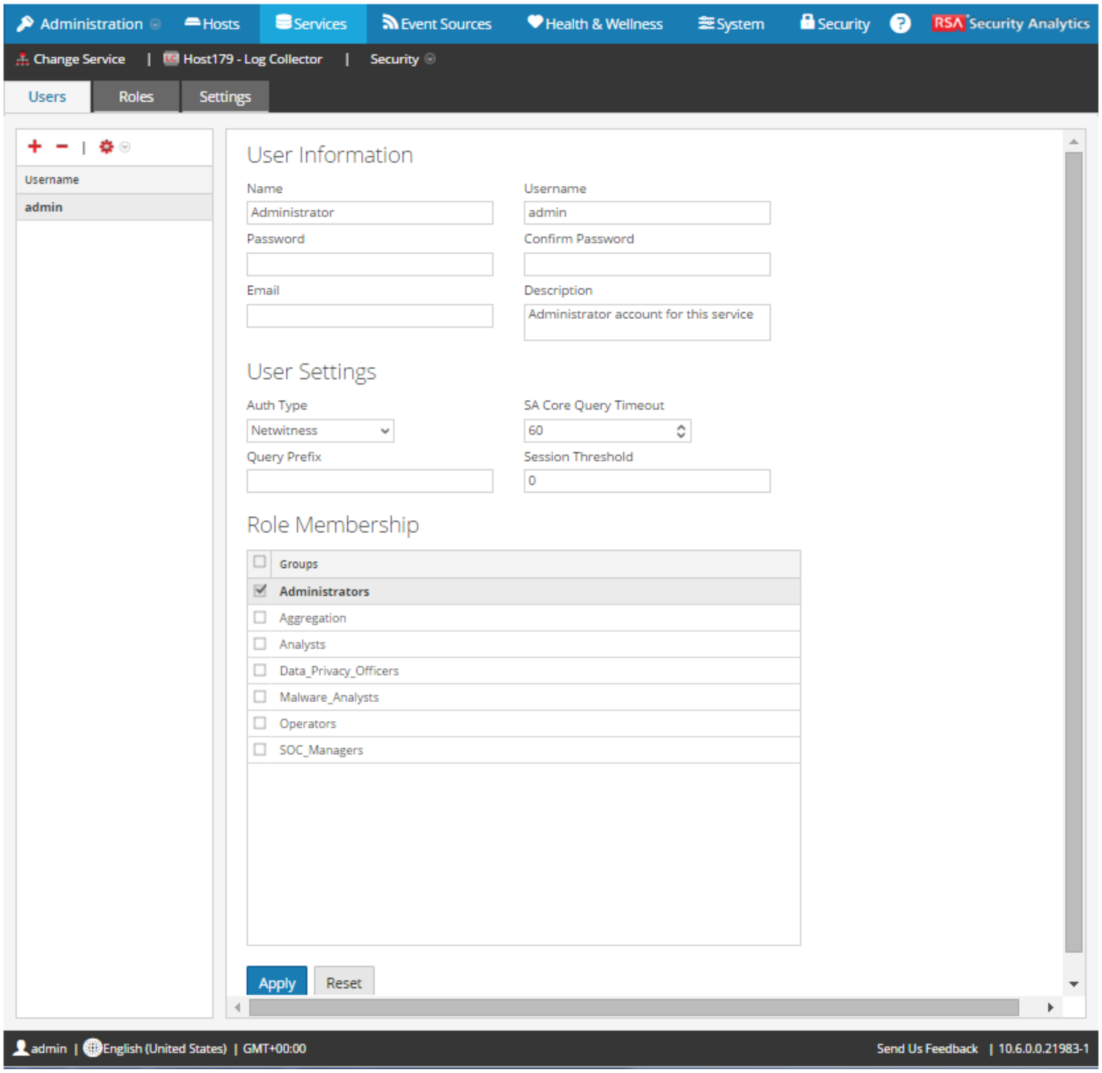
Access the Security View

Each of the following procedures starts in the Services Security view.

To navigate to the Services Security view:

1. In the Security Analytics menu, select **Administration** > **Services**.
2. Select a service, then ⚙ > **View** > **Security**.

   The Security view for the selected service is displayed with the Users tab open.



User Information

Name: Administrator
Username: admin
Password:
Confirm Password:
Email:
Description: Administrator account for this service

User Settings

Auth Type: Netwitness
SA Core Query Timeout: 60
Query Prefix:
Session Threshold: 0

Role Membership

☐	Groups
☑	Administrators
☐	Aggregation
☐	Analysts
☐	Data_Privacy_Officers
☐	Malware_Analysts
☐	Operators
☐	SOC_Managers

Note: For Security Analytics 10.4 and earlier service versions, in the User Settings section, the **Query Level** field is displayed instead of **SA Core Query timeout**.

Add a Service User

1. On the **Users** tab, click ✚.
2. Type the Username to access the service, then press **Enter**.
   The User Information section displays the Username and the rest of the fields are available for editing.
3. Type the password for logging on to the service in the **Password** and **Confirm Password** fields.
4. (Optional) Provide additional information:
   - **Name** for logging on to Security Analytics
   - **Email** address
   - **Description** of the user
5. In the User Settings section, select the following information:
   - **Authentication Type**
     - If Security Analytics authenticates the user, select Netwitness.
     - If Active Directory or PAM is configured on Security Analytics Server to authenticate the user, select External.

   Note: In 10.4 and later, trusted connections make it unnecessary to configure external user accounts on the service. All external configuration is centralized on Security Analytics Server.

   - **SA Core Query Timeout** is the maximum number of minutes a user can run a query on the service. This field applies to Security Analytics 10.5 and later service versions and does not appear for 10.4 and earlier versions.
   - **Query Level** is the maximum number of minutes allowed for a user to perform a query on a service. There are three query levels: 1, 2, and 3. This field applies to Security Analytics 10.4 and earlier service versions and does not appear for 10.5 and later service versions.
6. (Optional) Specify additional query criteria:
   - **Query Prefix** filters queries. Type a prefix to restrict results the user sees.

- **Session Threshold** controls how the service scans meta values to determine session counts. Any meta value with a session count that is above the threshold stops its determination of the true session count.

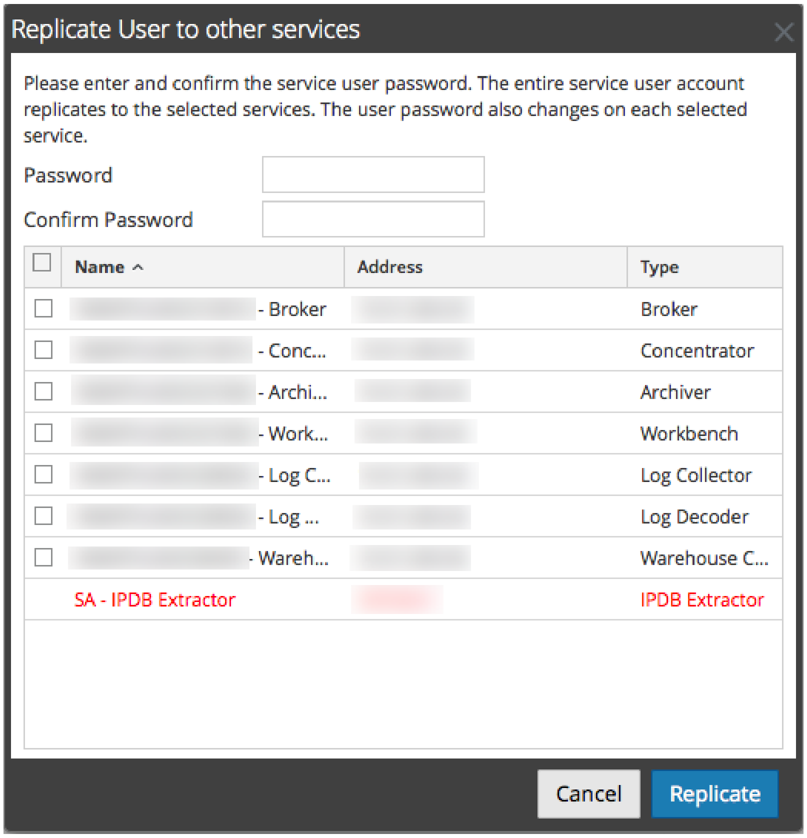
7. In the **Role Membership** section, select each role to assign to the user. When a user is a member of a role on a service, the user has the permissions assigned to the role.
8. To activate the new service user, click **Apply**.

The user is added to the service immediately.

Replicate a User to Other Services

1. In the Users tab, select a user and ⚙ ⌄ > **Replicate**.

   The Replicate Users to Other Services dialog is displayed.



Replicate User to other services

Please enter and confirm the service user password. The entire service user account replicates to the selected services. The user password also changes on each selected service.

Password

Confirm Password

☐	Name ^	Address	Type
☐	[redacted] - Broker	[redacted]	Broker
☐	[redacted] - Conc...	[redacted]	Concentrator
☐	[redacted] - Archi...	[redacted]	Archiver
☐	[redacted] - Work...	[redacted]	Workbench
☐	[redacted] - Log C...	[redacted]	Log Collector
☐	[redacted] - Log ...	[redacted]	Log Decoder
☐	[redacted] - Wareh...	[redacted]	Warehouse C...
	SA - IPDB Extractor	[redacted]	IPDB Extractor

2. Enter the user's **password** and confirm the password.
3. Select each service to which you are replicating the user.
4. Click **Replicate**.

The user account is added to each selected service.

Delete a Service User

1. On the **Users** tab, select the **Username** and click −.

   Security Analytics requests confirmation that you want to delete the selected user.

2. To confirm, click **Yes**.

The user is deleted from the service immediately.

Add a Service User Role

There are pre-configured roles in Security Analytics that are installed on the server and on each service. You can also add custom roles. The following table lists the pre-configured system roles and their permissions.

Role	Permission
Administrators	Full system access
Operators	Access to configurations but not to meta and session content
Analysts	Access to meta and session content but not to configurations
SOC_Managers	Same access as Analysts plus additional permission to handle incidents
Malware_Analysts	Access to malware events and to meta and session content
Data_Privacy_Officers	Access to meta and session content as well as configuration options that manage obfuscation and viewing of sensitive data within the system (see Data Privacy Management).

You must add a service role when you have added a:

- **Service** user or users that requires a new set of permissions.
- **Custom role on Security Analytics server** because trusted connections require that the same custom role exists both on the server and on each service the custom role will access. The names must be identical. For example, if you add a JuniorAnalysts role on the server then you must add a JuniorAnalysts role on each service the role will access. For more information, see the **Add a Role and Assign Permissions** topic in *System Security and User Management*.

There is also a pre-configured **Aggregation** service role. Aggregation Role and Service User Roles and Permissions provide additional information.

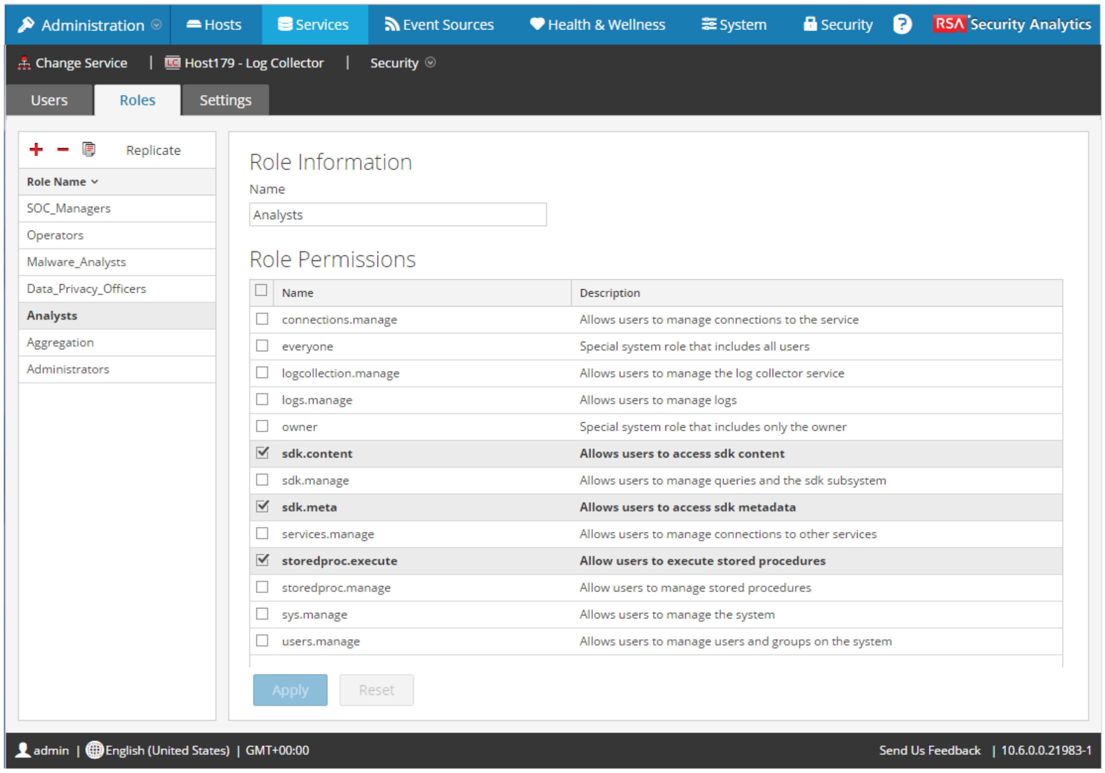
Procedure

To add a service user role and assign permissions to it:

1. In the Security Analytics menu, select **Administration** > **Services**.
2. Select a service, then ⚙ ⌄ > **View** > **Security**.

   The Security view for the selected service is displayed with the Users tab open.
3. Select the **Roles** tab and click **+**.

   The Services Security view is displayed and five pre-configured roles are already listed.



Role Name
SOC_Managers
Operators
Malware_Analysts
Data_Privacy_Officers
Analysts
Aggregation
Administrators

Role Information

Name: Analysts

Role Permissions

□	Name	Description
□	connections.manage	Allows users to manage connections to the service
□	everyone	Special system role that includes all users
□	logcollection.manage	Allows users to manage the log collector service
□	logs.manage	Allows users to manage logs
□	owner	Special system role that includes only the owner
☑	**sdk.content**	**Allows users to access sdk content**
□	sdk.manage	Allows users to manage queries and the sdk subsystem
☑	**sdk.meta**	**Allows users to access sdk metadata**
□	services.manage	Allows users to manage connections to other services
☑	**storedproc.execute**	**Allow users to execute stored procedures**
□	storedproc.manage	Allow users to manage stored procedures
□	sys.manage	Allows users to manage the system
□	users.manage	Allows users to manage users and groups on the system

4. Click **+**, type the **Role Name** and press **Enter**.

   The Role Name is displayed above a list of **Role Permissions**.
5. Select each permission the role will have on the service.
6. Click **Apply**.

The role is added to the service immediately. You can add service users to it in the **Users** tab.

Change a Service User Password

This procedure allows Administrators to change the password of a service user and replicate the new password to all Core services with that user account defined. It replicates only the password change to the Core services selected and does not replicate the entire user account. Administrators can also change the password of the **admin** account on the Core services.

Note: The Change Password option does not apply to external users.

Procedure

To change the password of a service user:

1. In the **Security Analytics** menu, select **Administration** > **Services**.

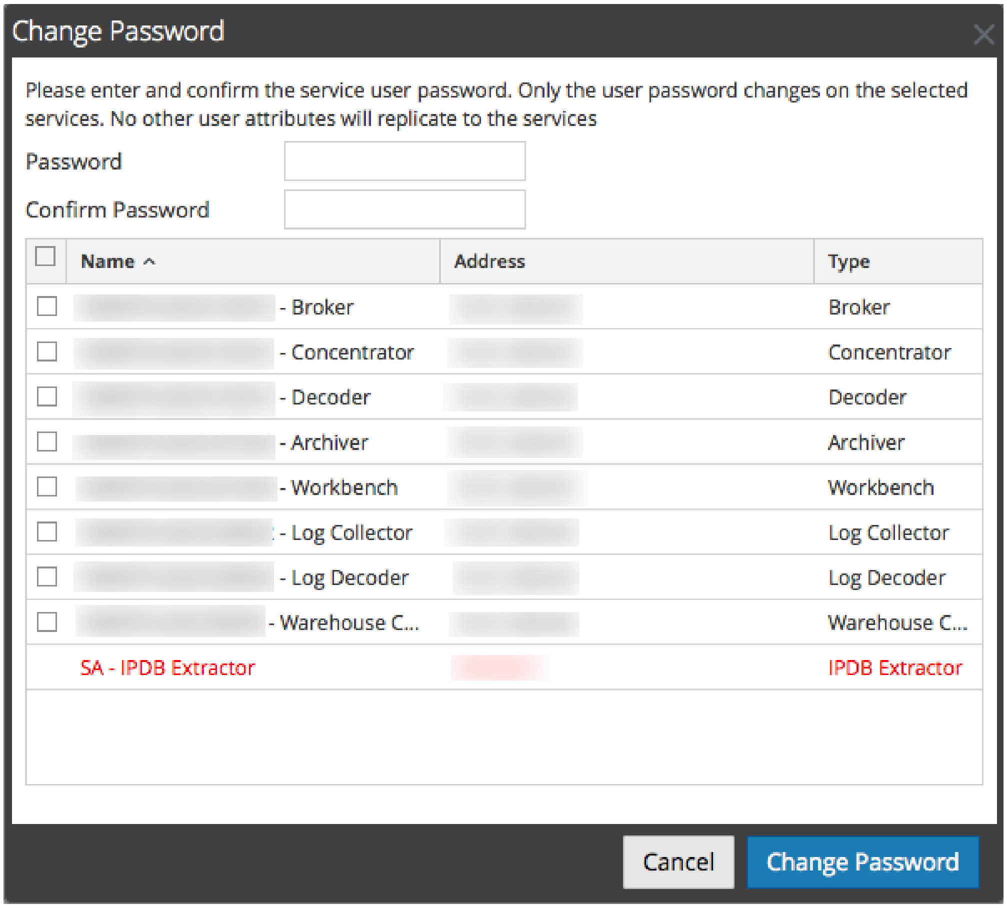
   The Administration Services view is displayed.

2. Select a service, then ⚙ ⌄ > **View** > **Security**.

   The Security view for the selected services is displayed.

3. In the **Users** tab, select a user and ⚙ ⌄ > **Change Password**.

   The **Change Password** dialog is displayed.



Change Password

Please enter and confirm the service user password. Only the user password changes on the selected services. No other user attributes will replicate to the services

Password

Confirm Password

□	Name ^	Address	Type
□	[redacted] - Broker	[redacted]	Broker
□	[redacted] - Concentrator	[redacted]	Concentrator
□	[redacted] - Decoder	[redacted]	Decoder
□	[redacted] - Archiver	[redacted]	Archiver
□	[redacted] - Workbench	[redacted]	Workbench
□	[redacted] - Log Collector	[redacted]	Log Collector
□	[redacted] - Log Decoder	[redacted]	Log Decoder
□	[redacted] - Warehouse C...	[redacted]	Warehouse C...
	SA - IPDB Extractor	[redacted]	IPDB Extractor

4. Type a new password for the user and confirm the password.

5. Select the services where you want the user password to change.

6. Click **Change Password**.

   The status of the password change on the selected services is displayed.

Create and Manage Service Groups

The Administration Services view provides options for creating and managing groups of services. The Services panel toolbar includes options for creating, editing, and deleting service groups. Once groups are created, you can drag individual services from the Services panel into a group.

Groups may reflect functional, geographical, project-oriented, or any other organization principle that is useful. A service may belong to more than one group. Here are some examples of possible groupings.

- Group different service types to make it easier to configure and monitor all Brokers, Decoders, or Concentrators.
- Group services that are part of the same data flow; for example, a Broker, and all associated Concentrators and Decoders.
- Group services according to their geographic region and location within the region. If a major power outage occurs in a location, potentially affected services are easily identifiable.

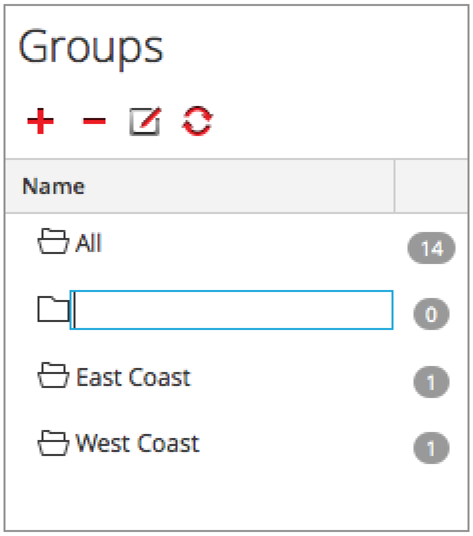
Create a Group

1. In the **Security Analytics menu**, select **Administration** > **Services**.

   The Administration Services view is displayed.

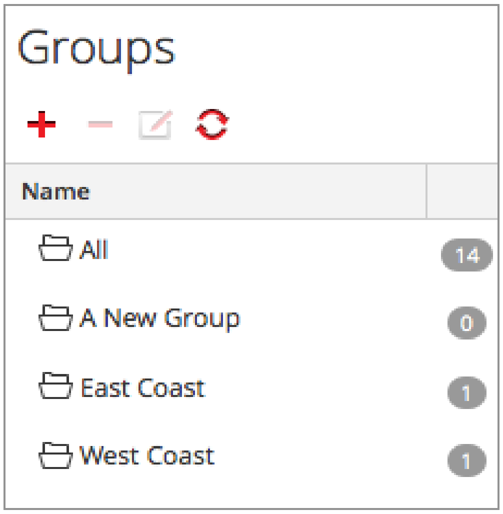
2. In the **Groups** panel toolbar, click +.

   A field for the new group opens with a blinking cursor.



3. Type the name of the new group in the field (for example, **A New Group**) and press **Enter**.

The group is created as a folder in the tree. The number next to the group indicates the number of services in that group.



Groups

Name	
All	14
A New Group	0
East Coast	1
West Coast	1

Change the Name of a Group

1. In the Services view **Groups panel**, double-click the group name or select the group and click ☑.

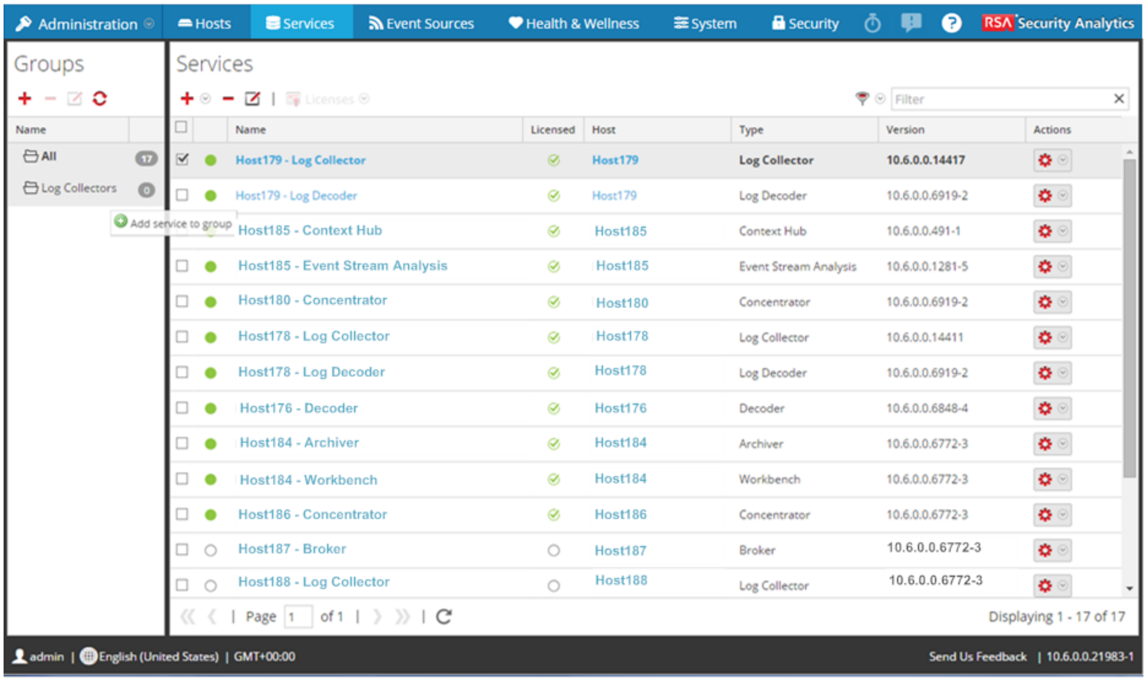
   The name field opens with a blinking cursor.

2. Type the new name of the group and press **Enter**.

   The name field closes and the new group name is displayed in the tree.

Add a Service to a Group

In the Services view **Services panel**, select a service and drag the service to a group folder in the groups panel; for example,**Log Collectors**.



□		Name	Licensed	Host	Type	Version	Actions
☑	●	Host179 - Log Collector	✓	Host179	Log Collector	10.6.0.0.14417	⚙
□	●	Host179 - Log Decoder	✓	Host179	Log Decoder	10.6.0.0.6919-2	⚙
	●	Host185 - Context Hub	✓	Host185	Context Hub	10.6.0.0.491-1	⚙
□	●	Host185 - Event Stream Analysis	✓	Host185	Event Stream Analysis	10.6.0.0.1281-5	⚙
□	●	Host180 - Concentrator	✓	Host180	Concentrator	10.6.0.0.6919-2	⚙
□	●	Host178 - Log Collector	✓	Host178	Log Collector	10.6.0.0.14411	⚙
□	●	Host178 - Log Decoder	✓	Host178	Log Decoder	10.6.0.0.6919-2	⚙
□	●	Host176 - Decoder	✓	Host176	Decoder	10.6.0.0.6848-4	⚙
□	●	Host184 - Archiver	✓	Host184	Archiver	10.6.0.0.6772-3	⚙
□	●	Host184 - Workbench	✓	Host184	Workbench	10.6.0.0.6772-3	⚙
□	●	Host186 - Concentrator	✓	Host186	Concentrator	10.6.0.0.6772-3	⚙
□	○	Host187 - Broker	○	Host187	Broker	10.6.0.0.6772-3	⚙
□	○	Host188 - Log Collector	○	Host188	Log Collector	10.6.0.0.6772-3	⚙

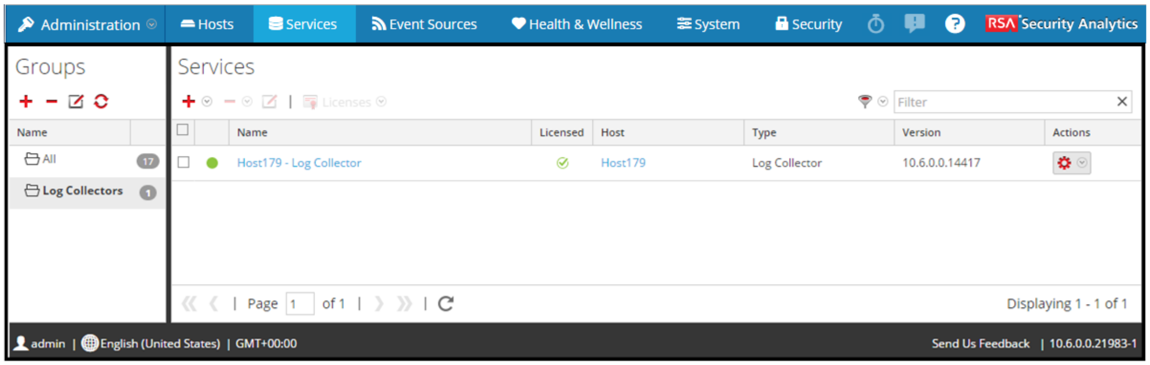
Page 1 of 1 — Displaying 1 - 17 of 17

The service is added to the group.

View the Services in a Group

To view the services in a group, click the group in the **Groups** panel.

The **Services** panel lists the services in that group.



□		Name	Licensed	Host	Type	Version	Actions
□	●	Host179 - Log Collector	✓	Host179	Log Collector	10.6.0.0.14417	⚙

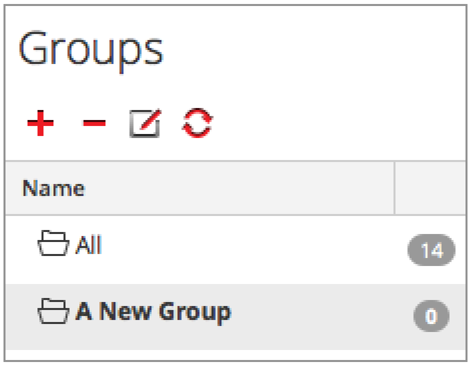
Page 1 of 1 — Displaying 1 - 1 of 1

Remove a Service from a Group

1. In the Services view **Groups panel**, select the group that contains the service that you want to remove. The services in that group appear in the Services panel.
2. In the **Services panel**, select one or more services that you want to remove from the group, and in the toolbar, select − ⌄ > **Remove from Group**.

The selected services are removed from the group, but are not removed from the Security Analytics user interface. The number of services in the group, which is listed near the group name, decreases by the number of services removed from the group. The **All** group contains the services that were removed from the group.

In the following example, the service group called **A New Group** does not contain any services, since the service in that group was removed.



Delete a Group

1. In the Services view **Groups panel**, select the group that you want to delete.
2. Click −.

   The selected group is removed from the Groups panel. The services that were in the group are not removed from the Security Analytics user interface. The **All** group contains the services from the deleted group.

Duplicate or Replicate a Service Role

An efficient way to add a new service role is to duplicate a similar role, save it with a new name and revise the permissions that are already assigned. For example, you could duplicate the Analysts role. Then, save it as JuniorAnalysts and modify the permissions.

The quick way to add an existing role to other services is to replicate the role. For example, you could replicate the JuniorAnalysts role that exists on a broker to a concentrator and log decoder.

Each of the following procedures starts in the Services Security view.

To navigate to the Services Security view:

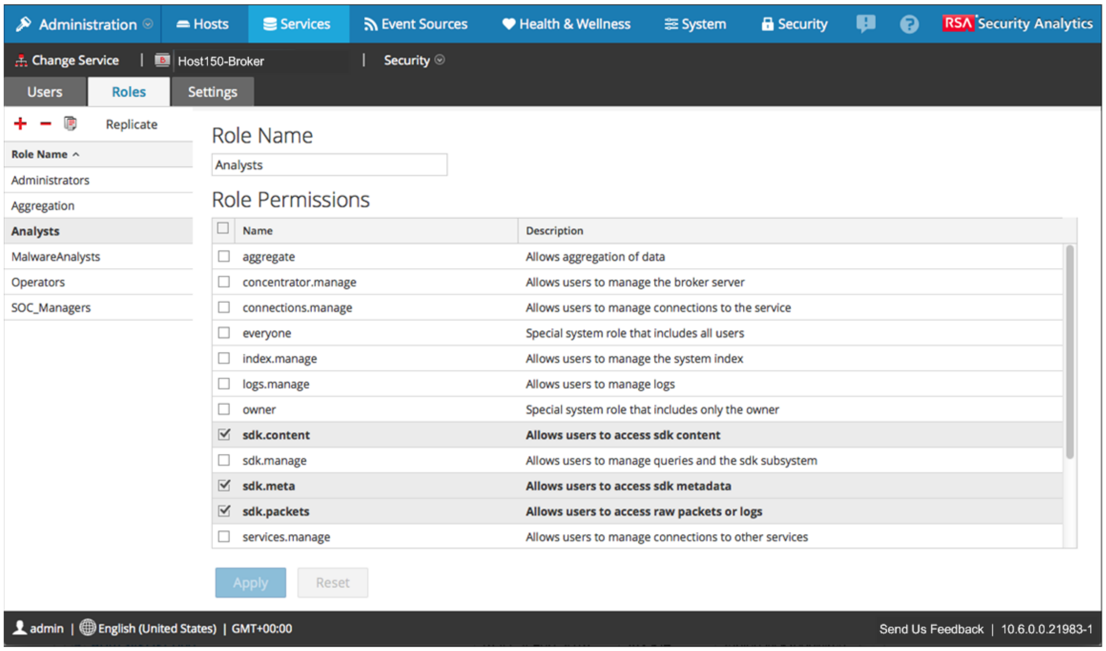
1. In the Security Analytics menu, select **Administration** > **Services**.
2. Select a service, then > **View** > **Security**.

   The Security view for the selected service is displayed with the Users tab open.
3. Select the **Roles** tab.

Procedures

Duplicate a Service Role

1. In the Roles tab, select the role you want to duplicate.



Role Name

Analysts

Role Permissions

□	Name	Description
□	aggregate	Allows aggregation of data
□	concentrator.manage	Allows users to manage the broker server
□	connections.manage	Allows users to manage connections to the service
□	everyone	Special system role that includes all users
□	index.manage	Allows users to manage the system index
□	logs.manage	Allows users to manage logs
□	owner	Special system role that includes only the owner
☑	sdk.content	Allows users to access sdk content
□	sdk.manage	Allows users to manage queries and the sdk subsystem
☑	sdk.meta	Allows users to access sdk metadata
☑	sdk.packets	Allows users to access raw packets or logs
□	services.manage	Allows users to manage connections to other services

2. Click **Duplicate Role.**

3. Type a new name and click **Save**.
4. Select the new role.
5. In the **Role Permissions** section, select or deselect permissions to modify what the new role can do.

The duplicated role is added to the service immediately.

Replicate a Role

1. In the Roles tab, select the role you want to replicate and click **Replicate**.
2. In the **Replicate Role to Other Services** dialog, select each service on which to add the role.
3. Click **Replicate**.

The replicated role is added to each selected service immediately.

Edit Core Service Configuration Files

The service configuration files--for Decoder, Log Decoder, Broker, Concentrator, Archiver, and Workbench services-- are editable as text files. In the Service Config view > Files tab, you can:

- View and edit a service configuration file that the Security Analytics system is currently using.
- Retrieve and restore the latest backup of the file you are editing.
- Push the open file to other services.
- Save changes made to a file.

The files available to edit vary depending upon the type of service being configured. The files that are common to all Core services are:

- The service index file.
- The netwitness file.
- The crash reporter file.
- The scheduler file.

In addition the Decoder has files that configure parsers, feed definitions, and a wireless LAN adapter.

> **Note:** The default values in these configuration files are generally good for the most common situations; however, some editing is necessary for optional services, such as the crash reporter or scheduler. Only administrators with a good understanding of the networks and the factors that affect the way services collect and parse data should make changes to these files in the Files tab.

For more detail on service configuration parameters, see Service Configuration Settings.

Edit a Service Configuration File

To edit a file:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the Services grid, select a service.
3. Select ⚙ ⌄ > **View** > **Config**.

   The Service Config view is displayed with the General tab open.

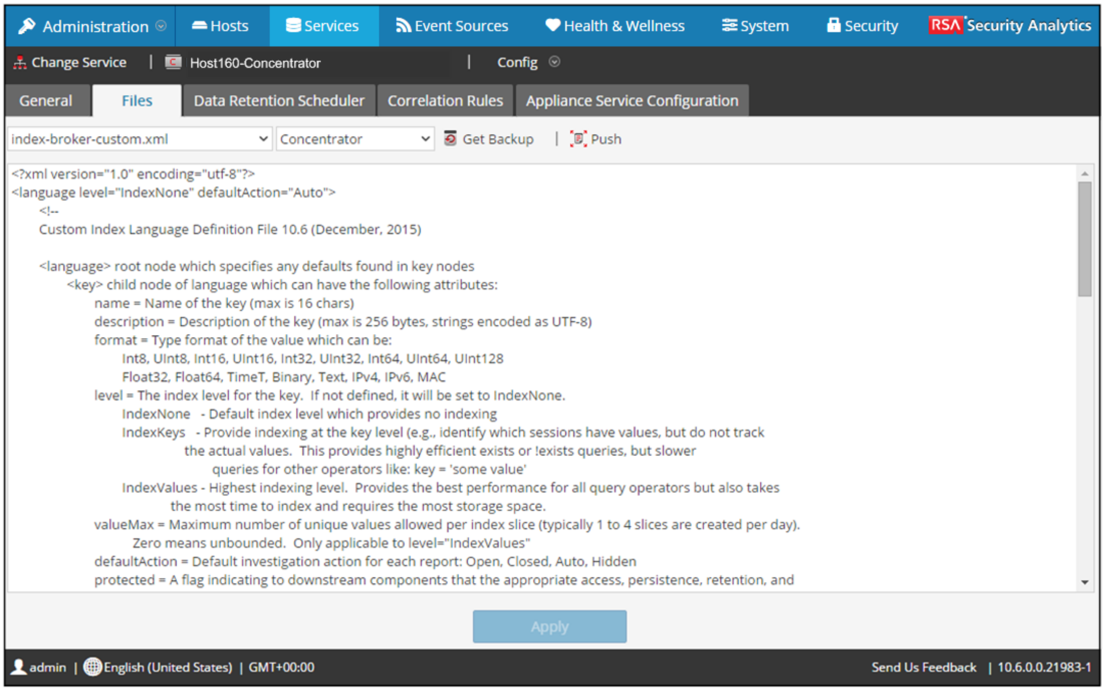
4. Click the **Files** tab.

   The selected service, such as Concentrator, appears in the drop-down list on the right.

5. (Optional) To edit a file for the host instead of the service, select **Host** in the drop-down list.

6. Choose a file from the **Please Select A File To Edit** drop-down list.

   The file content is displayed in edit mode.



```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto">
    <!--
    Custom Index Language Definition File 10.6 (December, 2015)

    <language> root node which specifies any defaults found in key nodes
        <key> child node of language which can have the following attributes:
            name = Name of the key (max is 16 chars)
            description = Description of the key (max is 256 bytes, strings encoded as UTF-8)
            format = Type format of the value which can be:
                Int8, UInt8, Int16, UInt16, Int32, UInt32, Int64, UInt64, UInt128
                Float32, Float64, TimeT, Binary, Text, IPv4, IPv6, MAC
            level = The index level for the key.  If not defined, it will be set to IndexNone.
                IndexNone   - Default index level which provides no indexing
                IndexKeys   - Provide indexing at the key level (e.g., identify which sessions have values, but do not track
                          the actual values.  This provides highly efficient exists or !exists queries, but slower
                              queries for other operators like: key = 'some value'
                IndexValues - Highest indexing level.  Provides the best performance for all query operators but also takes
                        the most time to index and requires the most storage space.
            valueMax = Maximum number of unique values allowed per index slice (typically 1 to 4 slices are created per day).
                 Zero means unbounded.  Only applicable to level="IndexValues"
            defaultAction = Default investigation action for each report: Open, Closed, Auto, Hidden
            protected = A flag indicating to downstream components that the appropriate access, persistence, retention, and
```

7. Edit the file and click **Save**.

The current file is overwritten and a backup file is created. The changes go into effect after the service is restarted.

Revert to a Backup Version of a Service Configuration File

After you make changes to a configuration file, save the file, and restart the service, a backup file is available. To revert to a backup of a configuration file:

1. To select a configuration file, follow steps 1-6 of the previous procedure.

2. Click Get Backup.

   The backup file opens in the text editor.

3. To revert to the backup version, click **Save**.

The changes go into effect after the service is restarted.

Push a Configuration File to Other Services

Once you have edited a service configuration file, you can push the same configuration to other services of the same type.

1. To select a configuration file, follow steps 1-6 in the first procedure.
2. Click Push. The Select Services dialog is displayed.
3. Select each service to push the configuration file on it.

   Each service must be the same type as the one you selected in the Services view.

   > **Caution:** If you decide not to push the configuration file, click **Cancel**.

4. To push the configuration file to all selected services, click **OK**.

The configuration file is pushed to all selected services.

Topics

- Configure the Task Scheduler
- Edit a Service Index File
- Enable Crash Reporter Service
- Maintain the Table Map Files

Configure the Task Scheduler

The scheduler File

One of the files available for editing in the Service Config view > Files tab is **scheduler.** This file configures the built-in task scheduler for a service. The task scheduler can automatically send messages at predefined intervals or specific times of the day.

Scheduler Task Syntax

A task line in the scheduler file consists of the following syntax, where **<Value>** has no spaces:

```
<ParamName>=<Value>
```

if **<Value>** has any spaces, this is the syntax:

```
<ParamName>="<Value>"
```

In each task line, these guidelines apply:

- Parameter **time** or one of the interval parameters (**seconds**, **minutes** or **hours**) is required.
- Escape special characters with a \ (backslash).

Task Line Parameters

The following task line parameters are accepted by the scheduler.

Syntax	Description
daysOfWeek: <string, optional, {enum-any-:sun|mon|tue|wed|thu|fri|sat|all}>	The days of week to execute a task. The default value is **all**.
deleteOnFinish: <bool, optional>	Delete the task when it has successfully finished.
hours: <uint32, optional, {range:1 to 8760}>	The number of hours between executions.
logOutput: <string, optional>	Output the response to log using the specified module name.

Syntax	Description
minutes: <uint32, optional, {range:1 to 525948}>	The number of minutes between executions.
msg: <string>	The message to send the node.
params: <string, optional>	The parameters for the message.
pathname: <string>	The path of the node that receives the message.
seconds: <uint32, optional, {range:1 to 31556926}>	The number of seconds between executions.
time: <string>	The time of execution in HH::MM:SS format (local time of this server).
timesToRun: <uint32, optional>	How many times to run since service start, **0** = means unlimited (default).

Messages

The following are the message strings to use in the Task Scheduler **msg** parameter.

Message	Description
addInter	Add a task to run at a defined interval. For example, this message runs the **/index save** command every 6 hours: addInter hours=6 pathname=/index msg=save
addMil	Add a task to run at a specific time of day or even day(s) of the week. For example, this message runs the **/index save** command at 1AM every business day: addMil time= 01:00:00 pathname=/index msg=save daysOfWeek=mon,tue,wed,thu,fri

Message	Description
delSched	Deletes an existing scheduled task. The **id** parameter of the task must be retrieved from the print message.
print	Prints all scheduled tasks.
replace	Assign all scheduled tasks in one message, deleting any existing tasks.
save	Tell a node to save

Sample Task Line

The following example task line in the scheduler file downloads the feeds package file (**feeds.zip**) to the selected Decoder every 120 minutes from the feeds host server:

```
minutes=120 pathname=/parsers msg=feed params="type\=wget
file\=http://feedshost/nwlive/feeds.zip"
```

Edit a Service Index File

This topic provides important information and guidelines for configuring service custom index files, which are editable in the Service Config view > Files tab.

The index file, along with other configuration files, controls operation of each core service. Accessing the index file through the Service Config view in Security Analytics opens the file in a text editor, where you can edit the file.

> **Note:** Only Administrators with a thorough and comprehensive understanding of Core service configuration are qualified to make changes to an Index file, which is one of the central configuration files for the appliance service. Changes made should be consistent across all Core services. Invalid entries or a misconfigured file can prevent the system from starting and can require the assistance of RSA Support to bring the system back into a working state.

These are the index files:

- **index-broker.xml**, **index-broker -custom.xml**
- **index-concentrator.xml**, **index-concentrator -custom.xml**
- **index-decoder.xml**, **index-decoder -custom.xml**
- **index-logdecoder.xml**, **index-logdecoder--custom.xml**
- **index-archiver.xml**, **index-archiver -custom.xml**
- **index-workbench.xml**, and **index-workbench -custom.xml**

Index and Custom Index Files

All customer-specific index changes are made in **index-<service>-custom.xml**. This file overrides any settings in **index-<service>.xml**, which is solely controlled by RSA.

> **Note:** Customers using Security Analytics versions prior to 10.1 had to customize index files by editing and saving the index file, and this method relied on Security Analytics creating a backup of the current index file upon restart of the service. Using this process, the current file is overwritten and a backup file is created. The toolbar option provides a way to revert to a backup version of the index file.
>
> During software upgrades, **index-<service>.xml** is not preserved, as it is overwritten by any changes made by the RSA content team. However, a backup is made in the same directory and named **index-<service>.xml.rpm_pre_save**. The **index-<service>.xml.rpm_pre_save** file can be referenced if needed to create the customer-specific **index-<service>-custom.xml** file, which needs to be done only once. Going forward, the new system allows RSA to make index changes without modifying existing customer specific changes.

The custom index file, **index-<service>--custom.xml,** allows creation of custom definitions or overrides of your own language keys that are not overwritten during the upgrade process.

- Keys that are defined in **index-<service>--custom.xml** replace the definitions found in **index-<service>.xml**.
- Keys that are added to **index-<service>--custom.xml** and not found in **index - <service>.xml** are added to the language as a new key.

Some common applications for editing the index file are:

- To add new custom meta keys to add new fields to the Security Analytics user interface.
- To configure protected meta keys as part of a data privacy solution as described in the *Data Privacy Management* guide.
- To adjust the Security Analytics Core database query performance as described in the *Security Analytics Core Database Tuning Guide*.

Note: For Security Analytics 10.1 and above, there is no need to edit the Broker custom index file, except for data privacy deployment scenarios and system roles. The Broker automatically merges the keys of all aggregate services to create a comprehensive language. The fallback language defined in **index--broker.xml** and **index--broker-custom.xml** is used if there are no services or if all services are offline.

Caution: Never set the index level to IndexKeys or IndexValues on a Decoder if you have a Concentrator or Archiver aggregating from the Decoder. The index partition size is too small to support any indexing beyond the default `time` meta key.

Enable Crash Reporter Service

The Crash Reporter is an optional service for Security Analytics services. When activated for any of the core services, the Crash Reporter automatically generates a package of information to be used for diagnosing and solving the problem that resulted in the service failure. The package is automatically sent to RSA for analysis. The results are forwarded to RSA support for any further action.

The information package sent to RSA does not contain captured data. This information package consists of the following information:

- Stack trace
- Logs
- Configuration settings
- Software version
- CPU information
- Installed RPMs
- Disk geometry

The Crash Reporter crash analysis can be activated for any Core product.

The crashreporter.cfg File

One of the files available for editing in the Service Config view > Files tab is **crashreporter.cfg**, the Crash Reporter Client Server configuration file.

This file is used by the script that checks, updates, and builds crash reports on the host. The list of products to monitor can include Decoders, Concentrators, hosts, and Brokers.

This table lists the settings for the **crashreporter.cfg** file.

Setting	Description
applicationlist=decoder, concentrator, host	Define the list of products to monitor.
sitedir=/var/crashreporter	Location of the site directory for the report.
webdir=/usr/share/crashreporter/Web	Location of the web directory.

Setting	Description
devdir=/var/crashreporter/Dev	Location of the development directory.
datadir=/var/crashreporter/data	Location of the directory storing data files.
perldir=/usr/share/crashreporter/perl	Location of the perl files.
bindir=/usr/share/crashreporter/bin	Location of the binary executables.
libdir=/usr/share/crashreporter/lib	Location of the binary libraries.
cfgdir=/etc/crashreporter	Location of the configuration files.
logdir=/var/log/crashreporter	Location of the log files.
scriptdir=/usr/share/crashreporter/scripts	Location of the directory containing scripts.
workdir=/var/crashreporter/work	Location of the process work directory.
sqldir=/var/crashreporter/sql	Location where created sql files are placed.
reportdir=/var/crashreporter/reports	Location where temporary reports are created.
packagedir=/var/crashreporter/packages	Location of the created package files.
gdbconfig=/etc/crashreporter/crashreporter.gdb	Location of the gdb configuration file.

Setting	Description
corewaittime=30	Define the number of seconds to wait after finding a core in order to determine if the core is still being written.
cyclewaittime=10	Define the number of minutes to wait between search cycles
deletecores=1	Specify if the core files should be deleted after report. 0 = No 1 = Yes **NOTE:** Until the core file is deleted, it is reported each time crashreporter is restarted.
deletereportdir=1	Specify if the report directory should be deleted after the report. Useful in order to view core reports on box. 0 = No 1 = Yes **NOTE:** If not deleted, the directory will be included in each subsequent package.

Setting	Description
debug=1	Specify whether debugging messages are turned on or off in the **crashreporter** logging output. 0 = No 1 = Yes
posturl=https://www.net-witnesslive.com/crash...ter/submit.php	Define the webserver post url.
postpackages=0	Specify if the packages should be posted to the webserver. 0 = No 1 = Yes
deletepackages=1	Specify if packages should be deleted after they are posted to webserver. 0 = No 1 = Yes

Configure the Crash Reporter Service

To configure the Crash Reporter service:

1. In the Services view, select a service then click ⚙ > **View** > **Config**.
2. Select the **Files** tab.
3. Edit **crashreporter.cfg**.
4. Click **Save**.
5. To display the Service System view, select **Config** > **System**.

6. To restart the service. click ⏻ Shutdown Service.

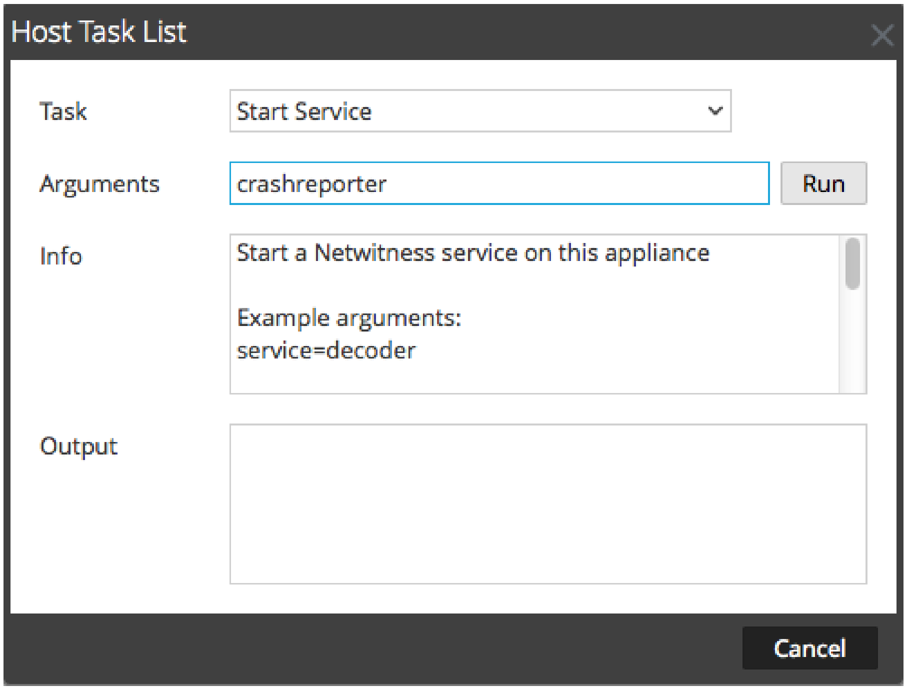
   The service shuts down and restarts.

Start and Stop the Crash Reporter Service

To start the Crash Reporter Service:

1. In the Services view, select the service then click ⚙ > **View** > **System**.
2. In the toolbar, click Host Tasks.

   The Host Task List is displayed.
3. In the Task drop-down list, select **Start Service**.
4. In the Arguments field, type **crashreporter**, then click **Run**.



Host Task List

Task	Start Service
Arguments	crashreporter
Info	Start a Netwitness service on this appliance Example arguments: service=decoder
Output	

The Crash Reporter service is activated and remains active until you stop it.

To stop the Crash Reporter service, select **Stop Service** from the Task drop-down list.

Maintain the Table Map Files

The table mapping file provided by RSA, **table-map.xml**, is a very significant part of the Log Decoder. It is a meta definition file which also maps the keys used in a log parser to the keys in the metadb.

Do not edit the **table-map.xml** file. If you want to make changes to the table-map, make them in the **table-map-custom.xml** file. The latest table-map.xml file is available on Live and RSA updates it as required. If you make changes to the table-map.xml file, they can be overwritten during an upgrade of service or content.

In the **table-map.xml**, some meta keys are set to `Transient` and some are set to `None`. To store and index a specific meta key, the key must be set to `None`. To make changes to the mapping, you need to create a copy of the file named table-map-custom.xml on the Log Decoder and set the meta keys to `None`.

For meta key indexing:

- When a key is marked as `None` in the **table-map.xml** file in the Log Decoder, it is indexed.
- When a key is marked as `Transient` in the **table-map.xml** file in the Log Decoder, it is not indexed. To index the key, copy the entry to the **table-map-custom.xml** file and change the keyword `flags="Transient"` to `flags="None"`.
- If a key does not exist in the **table-map.xml** file, add an entry to the **table-map-custom.xml** file in the Log Decoder.

Caution: Do not update the **table-map.xml** file since an upgrade can overwrite it. Add all of the changes that you want to make to the **table-map-custom.xml** file.

Prerequisites

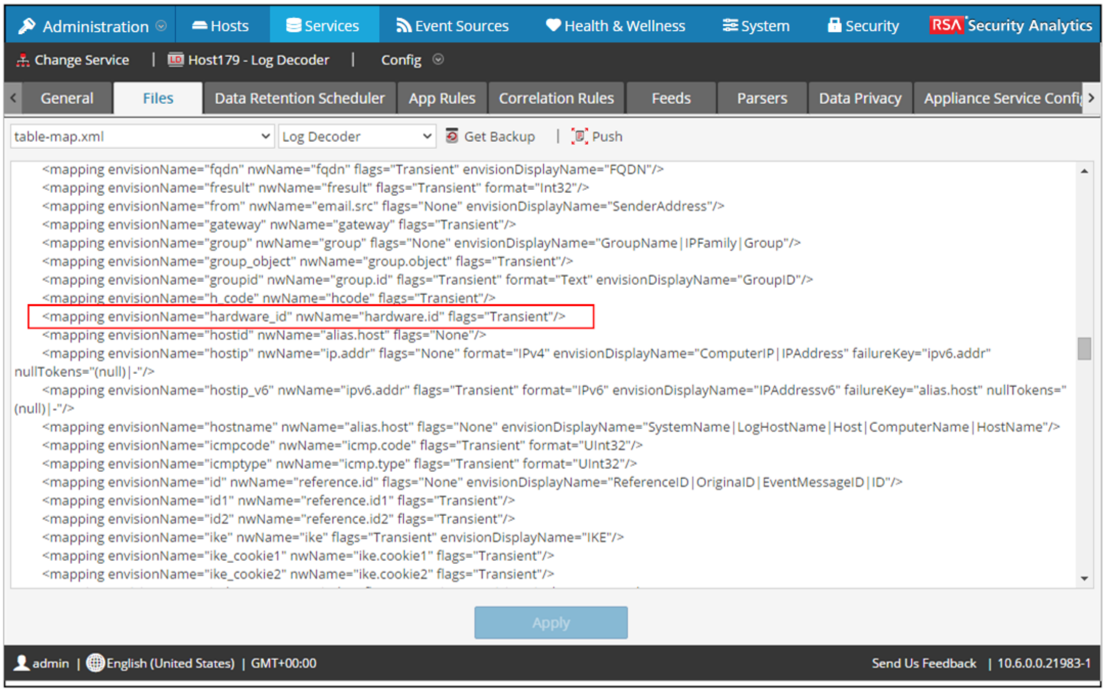
If you do not have a **table-map-custom.xml** file on the Log Decoder, create a copy of **table-map.xml** and rename it to **table-map-custom.xml**.

Procedure

To verify and update the table mapping file:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder and ⚙ > **View** > **Config**.

3. Click the **Files** tab and select the **table-map.xml** file.



```
    <mapping envisionName="fqdn" nwName="fqdn" flags="Transient" envisionDisplayName="FQDN"/>
    <mapping envisionName="fresult" nwName="fresult" flags="Transient" format="Int32"/>
    <mapping envisionName="from" nwName="email.src" flags="None" envisionDisplayName="SenderAddress"/>
    <mapping envisionName="gateway" nwName="gateway" flags="Transient"/>
    <mapping envisionName="group" nwName="group" flags="None" envisionDisplayName="GroupName|IPFamily|Group"/>
    <mapping envisionName="group_object" nwName="group.object" flags="Transient"/>
    <mapping envisionName="groupid" nwName="group.id" flags="Transient" format="Text" envisionDisplayName="GroupID"/>
    <mapping envisionName="h_code" nwName="hcode" flags="Transient"/>
    <mapping envisionName="hardware_id" nwName="hardware.id" flags="Transient"/>
    <mapping envisionName="hostid" nwName="alias.host" flags="None"/>
    <mapping envisionName="hostip" nwName="ip.addr" flags="None" format="IPv4" envisionDisplayName="ComputerIP|IPAddress" failureKey="ipv6.addr"
nullTokens="(null)|-"/>
    <mapping envisionName="hostip_v6" nwName="ipv6.addr" flags="Transient" format="IPv6" envisionDisplayName="IPAddressv6" failureKey="alias.host" nullTokens="
(null)|-"/>
    <mapping envisionName="hostname" nwName="alias.host" flags="None" envisionDisplayName="SystemName|LogHostName|Host|ComputerName|HostName"/>
    <mapping envisionName="icmpcode" nwName="icmp.code" flags="Transient" format="UInt32"/>
    <mapping envisionName="icmptype" nwName="icmp.type" flags="Transient" format="UInt32"/>
    <mapping envisionName="id" nwName="reference.id" flags="None" envisionDisplayName="ReferenceID|OriginalD|EventMessageID|ID"/>
    <mapping envisionName="id1" nwName="reference.id1" flags="Transient"/>
    <mapping envisionName="id2" nwName="reference.id2" flags="Transient"/>
    <mapping envisionName="ike" nwName="ike" flags="Transient" envisionDisplayName="IKE"/>
    <mapping envisionName="ike_cookie1" nwName="ike.cookie1" flags="Transient"/>
    <mapping envisionName="ike_cookie2" nwName="ike.cookie2" flags="Transient"/>
```

4. Verify that the flags keywords are set correctly to either `Transient` or `None`.

5. If you need to change an entry, do not change the **table-map.xml** file since an upgrade can overwrite it. Instead, copy the entry, select the **table-map-custom.xml** file and change the flags keyword from `Transient` to `None`.

   For example, the following entry for the hardware.id meta key in the **table-map.xml** file is not indexed and the flags keyword shows as `Transient`:

   ```
   <mapping envisionName="hardware_id" nwName="hardware.id"
   flags="Transient"/>
   ```

   To index the hardware.id meta key, change the flags keyword from `Transient` to `None` in the **table-map-custom.xml**:

   ```
   <mapping envisionName="hardware_id" nwName="hardware.id"
   flags="None"/>
   ```

6. If an entry does not exist in the table-map.xml file, add an entry to the **table-map-custom.xml** file.

7. After making your changes to the **table-map-custom.xml** file, click **Apply**.

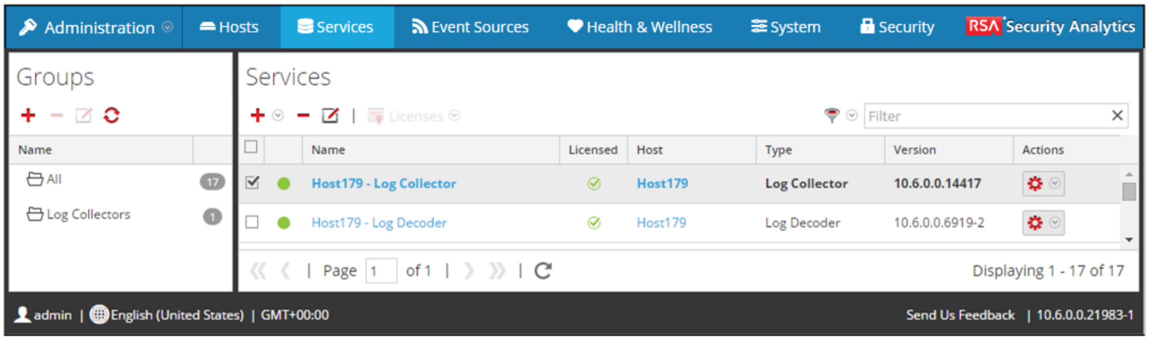
> **Caution:** Before changing the table mapping files, carefully consider the effect of changing the index from `Transient` to `None` since it can impact the available storage and performance of the Log Decoder. For this reason, only certain meta keys are indexed out of the box. Use the **table-map-custom.xml** file for different use cases.

Edit or Delete a Service

You can edit service settings, such as changing the host name or port number, or delete a service that you no longer need.

Each of the following procedures starts in the Services view.

To navigate to the Services view, in the Security Analytics menu select **Administration** > **Services**.



Name	
All	17
Log Collectors	1

☐		Name	Licensed	Host	Type	Version	Actions
☑	●	Host179 - Log Collector	✓	Host179	Log Collector	10.6.0.0.14417	⚙
☐	●	Host179 - Log Decoder	✓	Host179	Log Decoder	10.6.0.0.6919-2	⚙

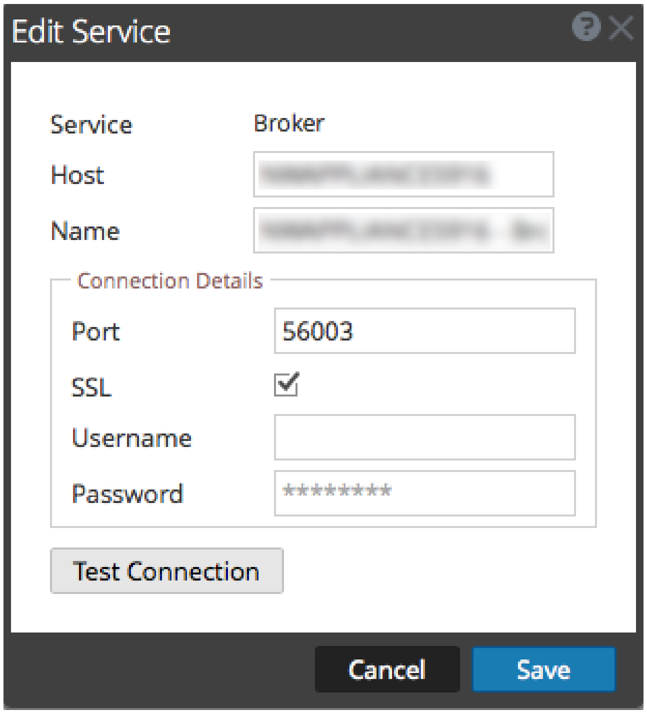
Displaying 1 - 17 of 17

Procedures

Edit a Service

1. In the Services view, select a service and click ✎ or ⚙ > **Edit**.

   The **Edit Service** dialog is displayed. It shows only the fields that apply to the selected service.



Service: Broker

Host: [redacted]

Name: [redacted]

Port: 56003

SSL: ☑

Username:

Password: *********

2. Edit the service details by changing any of the following fields:
   - **Name**
   - **Port** - Each core service has two ports, SSL and non-SSL. For trusted connections, you must use the SSL port.
   - **SSL** - For trusted connections, you must use SSL.
   - **Username** and **Password** - Use these credentials to test the connection to a service.
     a. If you use a trusted connection, delete the username.
        If you do not use a trusted connection, type a username and password.
     b. Click **Test Connection**.
3. (Optional) If the service requires a license select Entitle Service. This option is displayed only for services that require a license.
4. Click **Save**.

The changes take effect immediately.

Delete a Service

1. In the Services view, select one or more services and click − or ⚙ > **Delete**.
2. A dialog requests confirmation. To delete the service, click **Yes**.

The deleted service is no longer available to Security Analytics modules.

Explore and Edit Service Property Tree

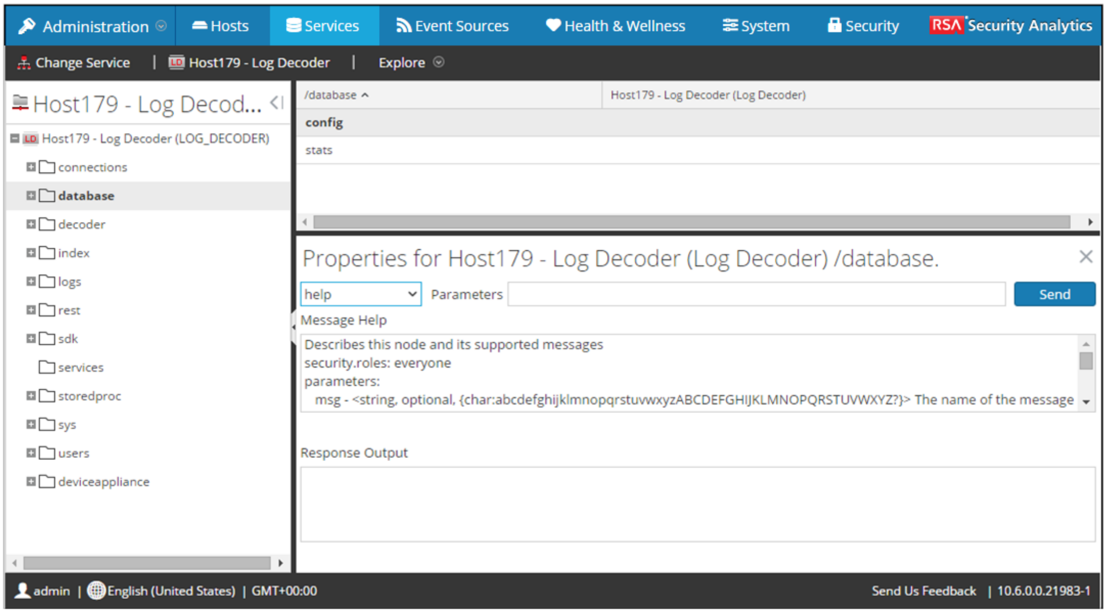
You have advanced access and control of service functionality in the Services Explore view, which consists of two parts. The Node list displays service functionality in a tree structure of folders. The Monitor panel displays properties of the folder or file selected in the Nodes list.

Each of the following procedures starts in the Explore view.

To navigate to the Explore view:

1. In the Security Analytics menu, select **Administration** > **Services**.
2. Select a service, then ⚙ > **View** > **Explore**.

   The Explore view is displayed. The Node list is on the left and the Monitor panel is on the right.



Properties for Host179 - Log Decoder (Log Decoder) /database.

```
Describes this node and its supported messages
security.roles: everyone
parameters:
  msg - <string, optional, {char:abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ?}> The name of the message
```

Procedures

Display or Edit a Service Property

To display a service property:

1. Right-click a file in the Node list or Monitor panel.
2. Click **Properties**.

To edit the value of a service property:

1. In the **Monitor panel**, select an editable property value.
2. Type a new value.

Send a Message to a Node

1. In the Properties Dialog select a **message type**. Options vary according to the file selected in the Node list.

   A description of the selected message type is displayed in the the **Message Help** field.
2. (Optional) If the message requires them, type the **Parameters**.
3. Click **Send**.

   The value or format is displayed in the **Response Output** field.

Kill a Connection to a Service

You can view sessions that are running on a service in the Service System view. From within the list of sessions, you can end the session and end active queries in a session.

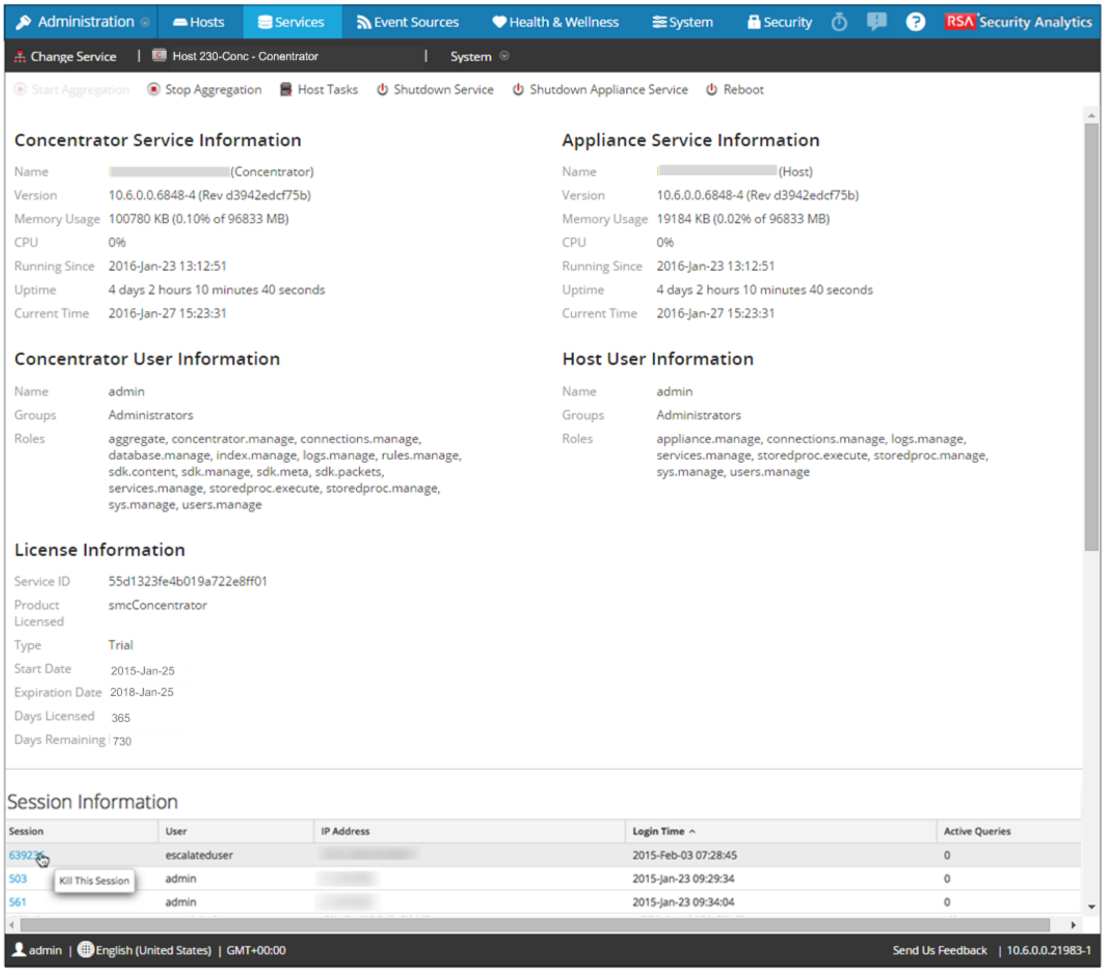
End a Session on a Service

1. In the **Security Analytics menu**, select **Administration > Services**.

   The Administration Services view is displayed.

2. Select a service, and select ⚙ ⌄ > **View > System**.

   The Service System view is displayed.



Concentrator Service Information

Name	[redacted] (Concentrator)
Version	10.6.0.0.6848-4 (Rev d3942edcf75b)
Memory Usage	100780 KB (0.10% of 96833 MB)
CPU	0%
Running Since	2016-Jan-23 13:12:51
Uptime	4 days 2 hours 10 minutes 40 seconds
Current Time	2016-Jan-27 15:23:31

Appliance Service Information

Name	[redacted] (Host)
Version	10.6.0.0.6848-4 (Rev d3942edcf75b)
Memory Usage	19184 KB (0.02% of 96833 MB)
CPU	0%
Running Since	2016-Jan-23 13:12:51
Uptime	4 days 2 hours 10 minutes 40 seconds
Current Time	2016-Jan-27 15:23:31

Concentrator User Information

Name	admin
Groups	Administrators
Roles	aggregate, concentrator.manage, connections.manage, database.manage, index.manage, logs.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Host User Information

Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

License Information

Service ID	55d1323fe4b019a722e8ff01
Product Licensed	smcConcentrator
Type	Trial
Start Date	2015-Jan-25
Expiration Date	2018-Jan-25
Days Licensed	365
Days Remaining	730

Session Information

Session	User	IP Address	Login Time ^	Active Queries
639236	escalateduser	[redacted]	2015-Feb-03 07:28:45	0
503	admin	[redacted]	2015-Jan-23 09:29:34	0
561	admin	[redacted]	2015-Jan-23 09:34:04	0

Kill This Session
admin | English (United States) | GMT+00:00
Send Us Feedback | 10.6.0.0.21983-1

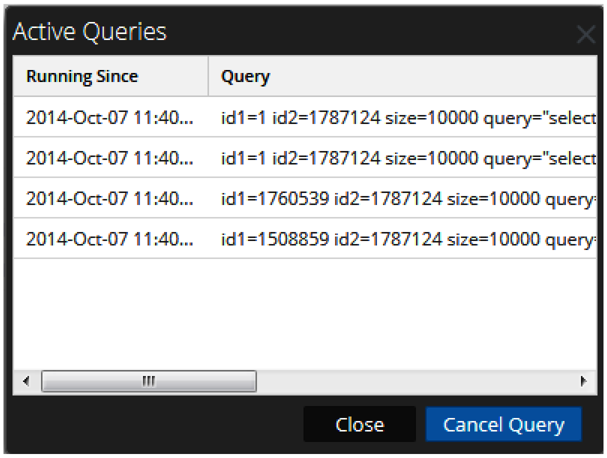
3. In the **Sessions** grid at the bottom, click a **session number > Kill This Session**.

The session ends and is removed from the grid.

End an Active Query in a Session

1. Scroll down to the **Sessions** grid.
2. In the **Active Queries** column, click a non-zero count of active queries for a session. You cannot click on it if there are 0 active queries.

   The Active Queries dialog is displayed.

   Active Queries

Running Since	Query
2014-Oct-07 11:40...	id1=1 id2=1787124 size=10000 query="select
2014-Oct-07 11:40...	id1=1 id2=1787124 size=10000 query="select
2014-Oct-07 11:40...	id1=1760539 id2=1787124 size=10000 query
2014-Oct-07 11:40...	id1=1508859 id2=1787124 size=10000 query

3. Select a query and click **Cancel Query**.

   The query stops and the Active Queries column is updated.

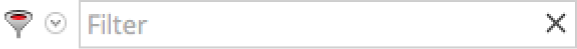
Search for Services

You can search for services from the list of services in the Administration Services view. The Services view enables you quickly filter the list of services by Name, Host, and Service Type. You can use the Filter drop-down menu and the Filter field separately or at the same time to filter the Services view.

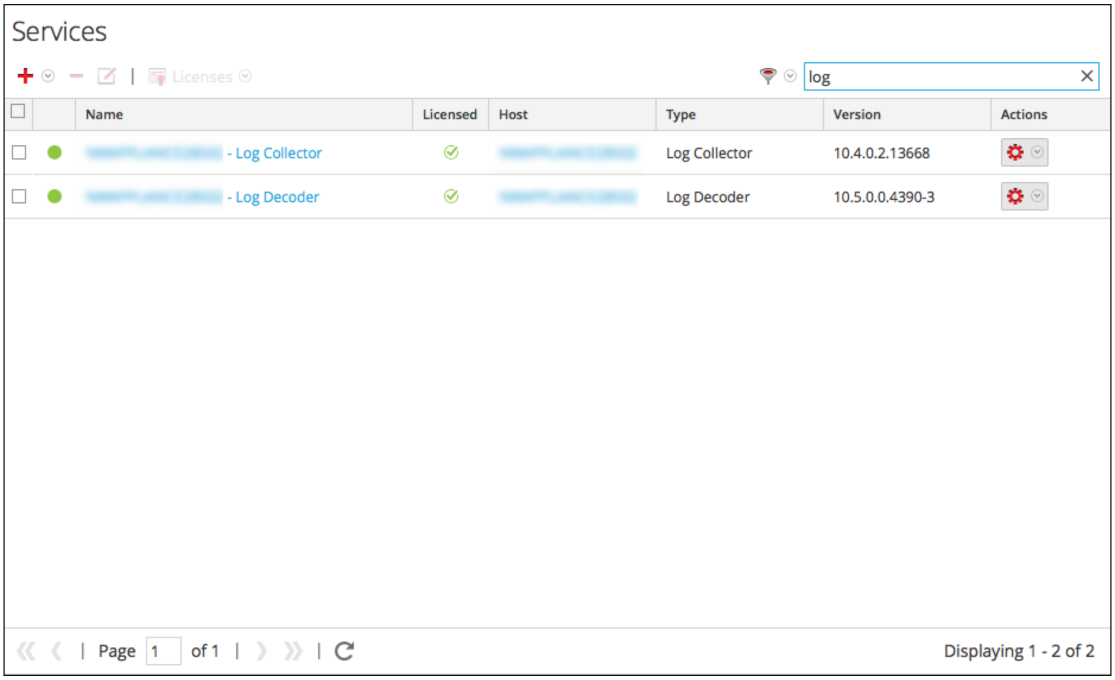
In addition to being able to locate the services for a host in the Services view, you can also quickly find the services that run on a host in the Hosts view.

Search for a Service

1. In the Security Analytics menu, select **Adminstration** > **Services**.
2. In the **Services panel** toolbar, type a service **Name** or **Host** in the **Filter** field.



The Services panel lists the services that match the names entered in the Filter field. The following example shows the search results after starting to type **log** in the filter field.

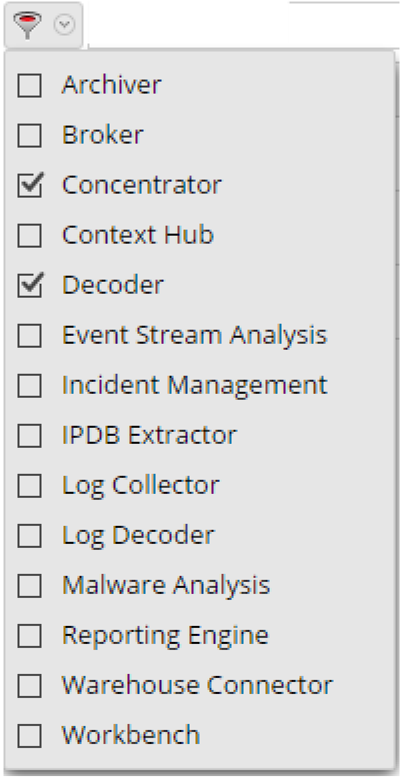


☐		Name	Licensed	Host	Type	Version	Actions
☐	●	[redacted] - Log Collector	✓	[redacted]	Log Collector	10.4.0.2.13668	
☐	●	[redacted] - Log Decoder	✓	[redacted]	Log Decoder	10.5.0.0.4390-3	

Filter Services by Type

1. In the Security Analytics menu, select **Adminstration** > **Services**.

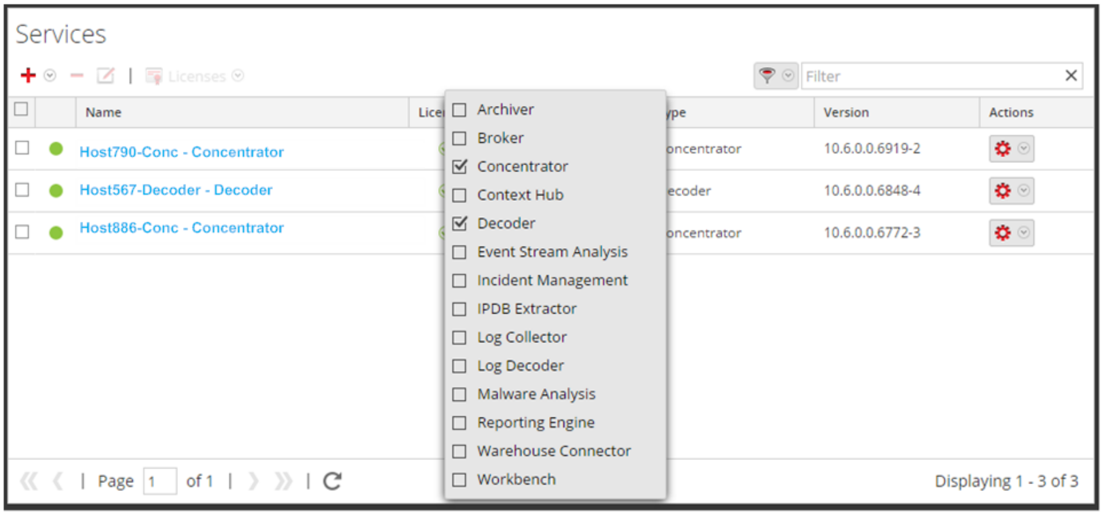
2. In the Services view, click and select the service types that you would like to appear in the Services view.



☐ Archiver
☐ Broker
☑ Concentrator
☐ Context Hub
☑ Decoder
☐ Event Stream Analysis
☐ Incident Management
☐ IPDB Extractor
☐ Log Collector
☐ Log Decoder
☐ Malware Analysis
☐ Reporting Engine
☐ Warehouse Connector
☐ Workbench

The selected service types appear in the Services view. The following example shows the

Services view filtered for Concentrator and Decoder.



Services

□		Name	Lice	ype	Version	Actions
□	●	Host790-Conc - Concentrator		oncentrator	10.6.0.0.6919-2	
□	●	Host567-Decoder - Decoder		ecoder	10.6.0.0.6848-4	
□	●	Host886-Conc - Concentrator		oncentrator	10.6.0.0.6772-3	

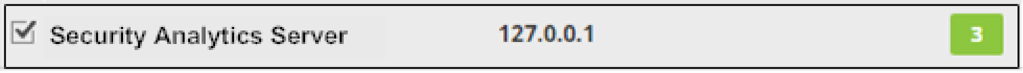
- □ Archiver
- □ Broker
- ☑ Concentrator
- □ Context Hub
- ☑ Decoder
- □ Event Stream Analysis
- □ Incident Management
- □ IPDB Extractor
- □ Log Collector
- □ Log Decoder
- □ Malware Analysis
- □ Reporting Engine
- □ Warehouse Connector
- □ Workbench

Find the Services on a Host

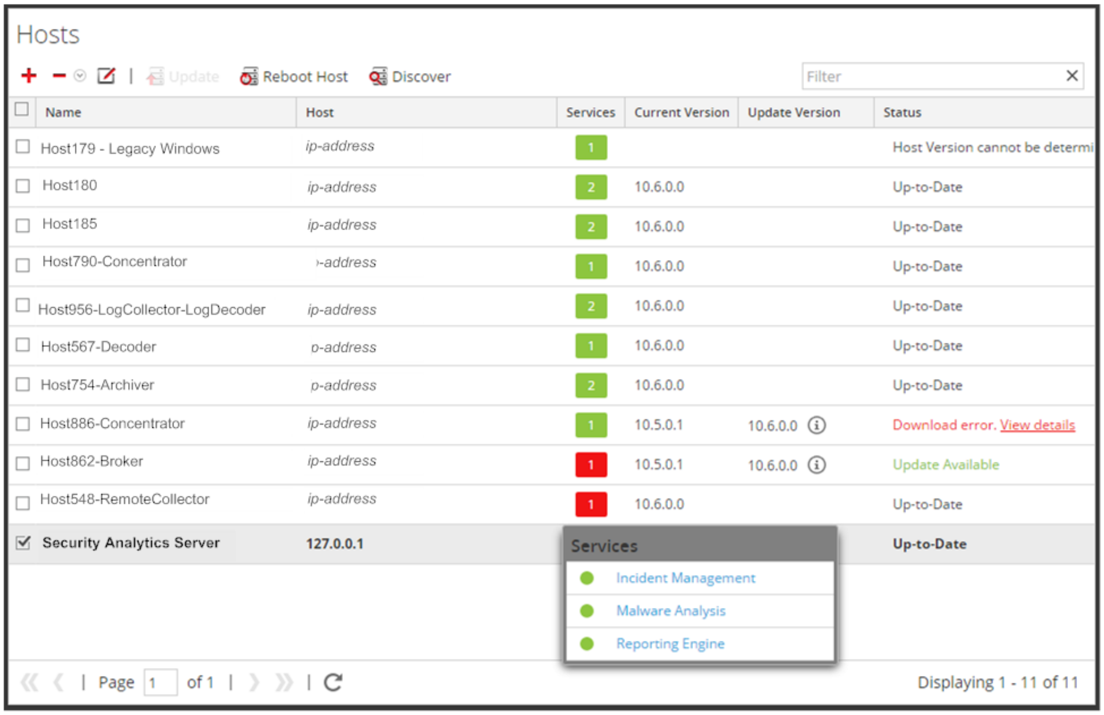
In addition to being able to locate the services for a host in the Services view, you can also quickly find the services that run on a host in the Hosts view.

1. In the Security Analytics menu, select **Adminstration** > **Hosts**.
2. In the Hosts view, select a host and click the box that contains a number (the number of services) in the **Services** column. A list of the services on the selected host is displayed.

   In the following example, a list of three services on the selected host are listed after clicking the box containing the number 3.



☑ Security Analytics Server 127.0.0.1 3



☐	Name	Host	Services	Current Version	Update Version	Status
☐	Host179 - Legacy Windows	ip-address	1			Host Version cannot be determi
☐	Host180	ip-address	2	10.6.0.0		Up-to-Date
☐	Host185	ip-address	2	10.6.0.0		Up-to-Date
☐	Host790-Concentrator	›-address	1	10.6.0.0		Up-to-Date
☐	Host956-LogCollector-LogDecoder	ip-address	2	10.6.0.0		Up-to-Date
☐	Host567-Decoder	p-address	1	10.6.0.0		Up-to-Date
☐	Host754-Archiver	p-address	2	10.6.0.0		Up-to-Date
☐	Host886-Concentrator	ip-address	1	10.5.0.1	10.6.0.0 ⓘ	Download error. View details
☐	Host862-Broker	ip-address	1	10.5.0.1	10.6.0.0 ⓘ	Update Available
☐	Host548-RemoteCollector	ip-address	1	10.6.0.0		Up-to-Date
☑	**Security Analytics Server**	**127.0.0.1**				**Up-to-Date**

Services
- ● Incident Management
- ● Malware Analysis
- ● Reporting Engine

You can click the service links to view the services in the Services view.

Start, Stop or Restart a Service

These procedures apply to core services only.

Each of the following procedures starts in the Services view. In the Security Analytics menu, select **Administration** > **Services**.

Start a Service

Select a service and click ⚙ ⌄ > **Start**.

Stop a Service

When you stop a service, all of its processes stop and active users are disconnected from it.

To stop a service:

1. Select a service and click ⚙ ⌄ > **Stop**.
2. A dialog requests confirmation. To stop the service, click **Yes**.

Restart a Service

Occasionally, you have to restart a service for changes to take effect. When you change a parameter that requires a restart, Security Analytics displays a message.

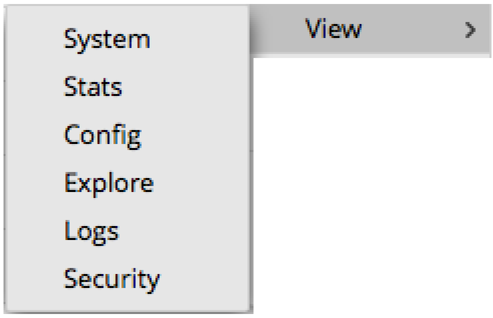
To restart a service:

1. Select a service and click ⚙ ⌄ > **Restart**.
2. A dialog requests confirmation. To stop the service, click **Yes**.

The service stops, then restarts automatically.

View Service Details

You can view and edit information about services using options in the View menu for a service.



Purpose of Each Service View

Each view displays a functional piece of a service and is described in detail in its own section:

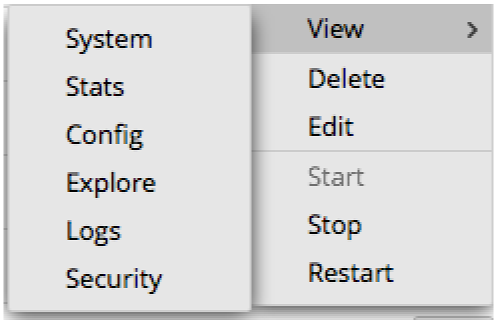
- Services System View shows a summary of service, appliance service, host user, license, and session information.
- Services Stats View provides a way to monitor service operations and status.
- Services Config View is for configuring all aspects of a service.
- Services Explore View is for viewing and editing host and service configurations.
- Services Logs View shows service logs that you can search.
- Services Security View is a way to add Security Analytics Core user accounts for aggregation, thick client users, and REST API users.

Access a Service View

To access a view for a service:

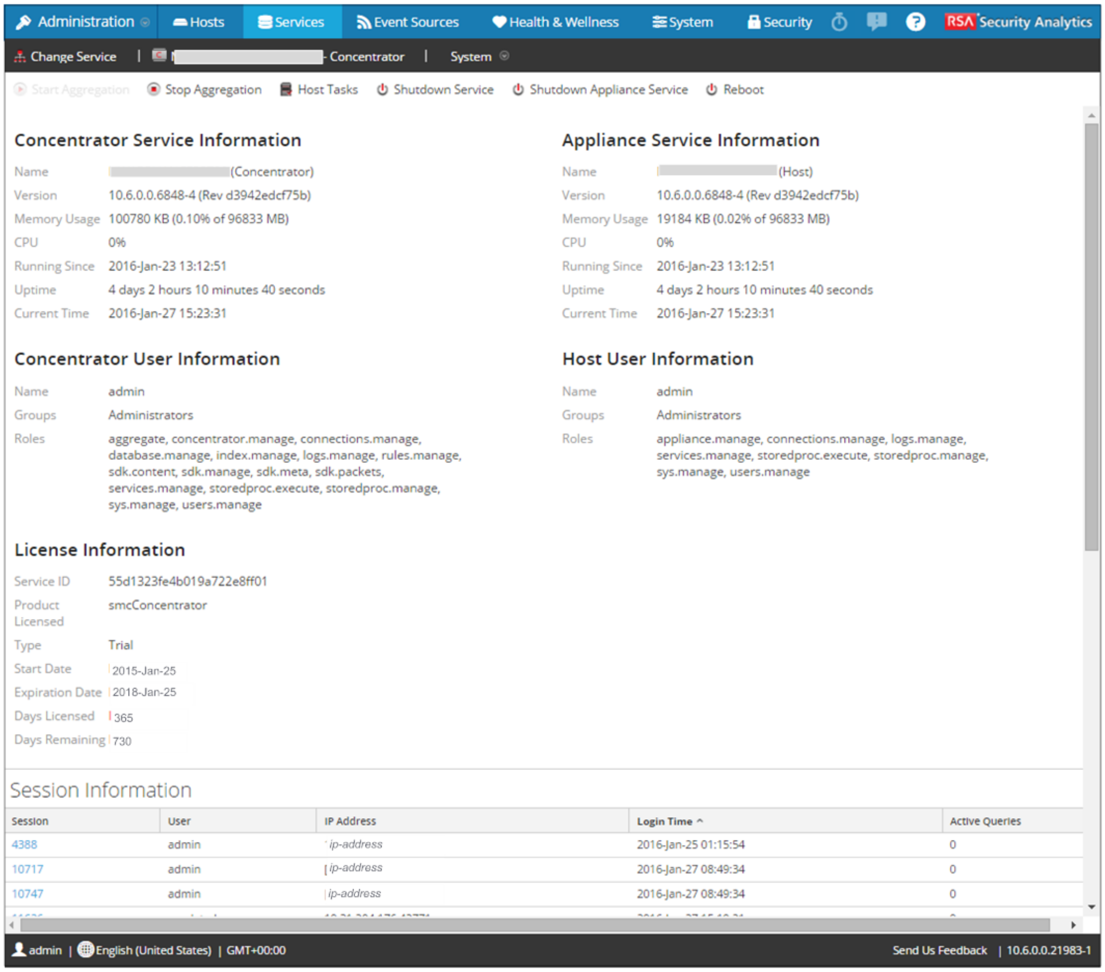
1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. Select a service and click ⚙ ⌄ > **View**.

   The View menu is displayed.



3. From the options on the left, select a view.

   This is a System view for a Concentrator.



Concentrator Service Information

Name	[redacted] (Concentrator)
Version	10.6.0.0.6848-4 (Rev d3942edcf75b)
Memory Usage	100780 KB (0.10% of 96833 MB)
CPU	0%
Running Since	2016-Jan-23 13:12:51
Uptime	4 days 2 hours 10 minutes 40 seconds
Current Time	2016-Jan-27 15:23:31

Appliance Service Information

Name	[redacted] (Host)
Version	10.6.0.0.6848-4 (Rev d3942edcf75b)
Memory Usage	19184 KB (0.02% of 96833 MB)
CPU	0%
Running Since	2016-Jan-23 13:12:51
Uptime	4 days 2 hours 10 minutes 40 seconds
Current Time	2016-Jan-27 15:23:31

Concentrator User Information

Name	admin
Groups	Administrators
Roles	aggregate, concentrator.manage, connections.manage, database.manage, index.manage, logs.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Host User Information

Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, logs.manage, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

License Information

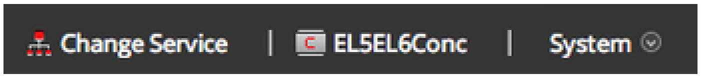
Service ID	55d1323fe4b019a722e8ff01
Product Licensed	smcConcentrator
Type	Trial
Start Date	2015-Jan-25
Expiration Date	2018-Jan-25
Days Licensed	365
Days Remaining	730

Session Information

Session	User	IP Address	Login Time ^	Active Queries
4388	admin	ip-address	2016-Jan-25 01:15:54	0
10717	admin	ip-address	2016-Jan-27 08:49:34	0
10747	admin	ip-address	2016-Jan-27 08:49:34	0

admin | English (United States) | GMT+00:00
Send Us Feedback | 10.6.0.0.21983-1

4. Use the toolbar to navigate:



- Click **Change Service** to select another service.
- Click the **name of the current service**, EL5EL6Conc in the example, to see the service configuration for it.
  The letter in the icon to the left of the name indicates the type of service:
  - **B** for Broker
  - **C** for Concentrator
  - **D** for Decoder and Log Decoder.
- Click ⌄ to the right of the **current view**, which is System in the example, to select a different view.

References

This topic is a reference for features in the Security Analytics Administration user interface.

This topic describes features available in the Security Analytics Administration user interface. The Administration module pulls Security Analytics administration activities into a single view to monitor and manage hosts (appliances), services, tasks, and security.

Topics

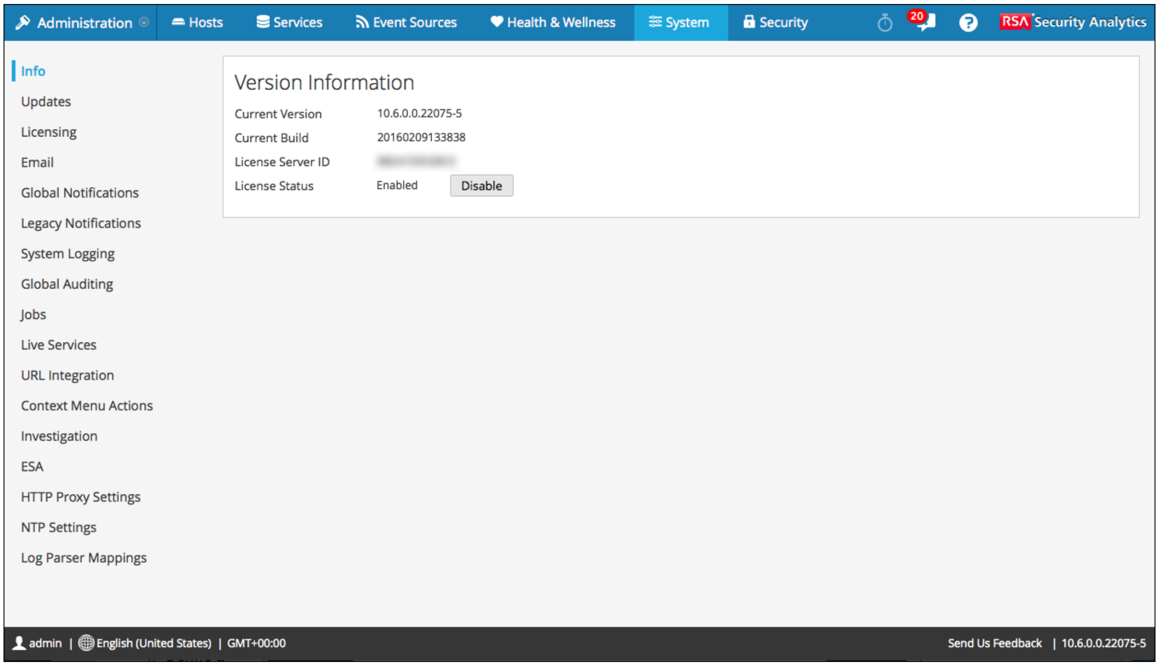
- Administration System View
- Service Configuration Settings
- Hosts View
- Services View
- Services Config View
- Services Explore View
- Services Logs View
- Services Security View
- Services Stats View
- Services Stats View - Malware Analysis
- Services System View

Administration System View

This topic introduces the features of Security Analytics Administration System view.

The Administration System view consolidates configuration of Security Analytics global auditing, email, system logging, jobs, connection to RSA Live Services, URL integration, Investigation, Event Stream Analysis (ESA), and advanced performance settings. In addition, you can manage Security Analytics versions, update the Security Analytics version, and configure the local licensing server.

To access the System view, in the **Security Analytics** menu, select **Administration** > **System**.



Version Information

Current Version	10.6.0.0.22075-5
Current Build	20160209133838
License Server ID	[redacted]
License Status	Enabled

Features

On the left panel of the Administration System view is an options panel listing all system nodes available for configuration. When you select a node, the associated content is displayed in the right panel.

Topics

- System Logging Panel
- URL Integration Panel

System Logging Panel

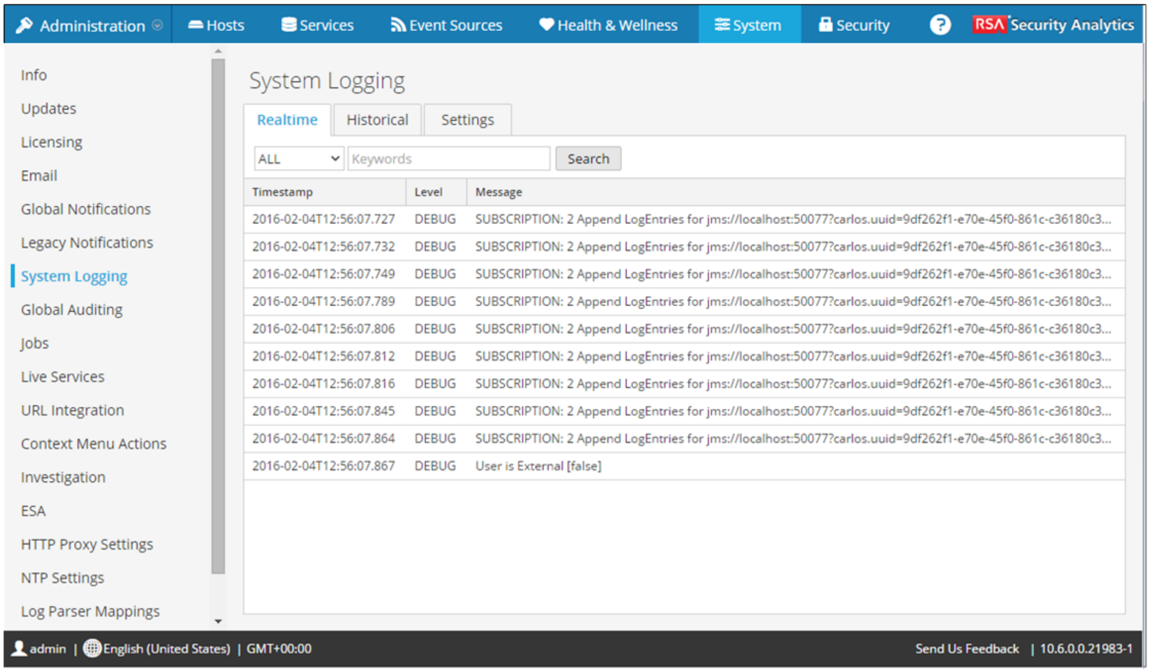
This topic introduces the features of Security Analytics System Logging panel.

The System Logs view provides the ability to view and search Security Analytics system logs. The System Logs view is similar to the Services Logs view with two exceptions:

- The Services Logs view has an additional filter to select messages for the service or host.
- The System Logging panel has additional tabs for Settings and Auditing.

To access the Security Analytics System Logs view:

1. In the **Security Analytics** menu, select **Administration** > **System.**
2. In the options panel, select **System Logging**.



Timestamp	Level	Message
2016-02-04T12:56:07.727	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.732	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.749	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.789	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.806	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.812	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.816	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.845	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.864	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.867	DEBUG	User is External [false]

Features

The System Logging panel has three tabs: Realtime, Historical, and Settings.

Feature	Description
Realtime tab	This is the monitor mode of the Security Analytics log. See Realtime Tab for more information.

Feature	Description
Historical tab	This is a searchable view of the Security Analytics log. See Historical Tab for more information.
Settings tab	This tab allows you to modify the basic logging configuration for Security Analytics as well as the packages to be logged. See Settings Tab for more information.

Topics

- Historical Tab
- Realtime Tab
- Settings Tab

Historical Tab

This topic describes the features of the System Service Logging > Historical tab and the Services Logs view > Historical tab.

The Historical tab provides a searchable view of the Security Analytics log or the service log in a paged format. When initially loaded, the grid shows the last page of the log entries for the system or the system.

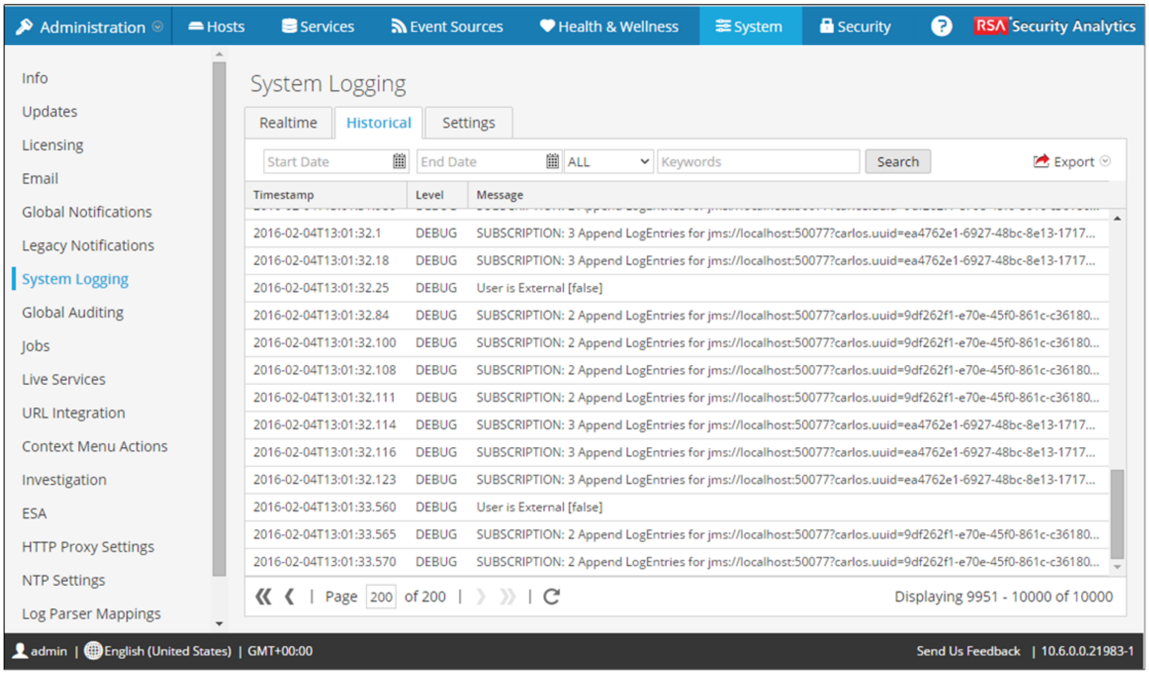
To access the Historical tab:

1. In the **Security Analytics** menu, select **Administration > System.**
2. In the options panel, select **System Logging**.

   The System Logging panel opens to the **Realtime** tab by default.
3. Click the **Historical** tab.

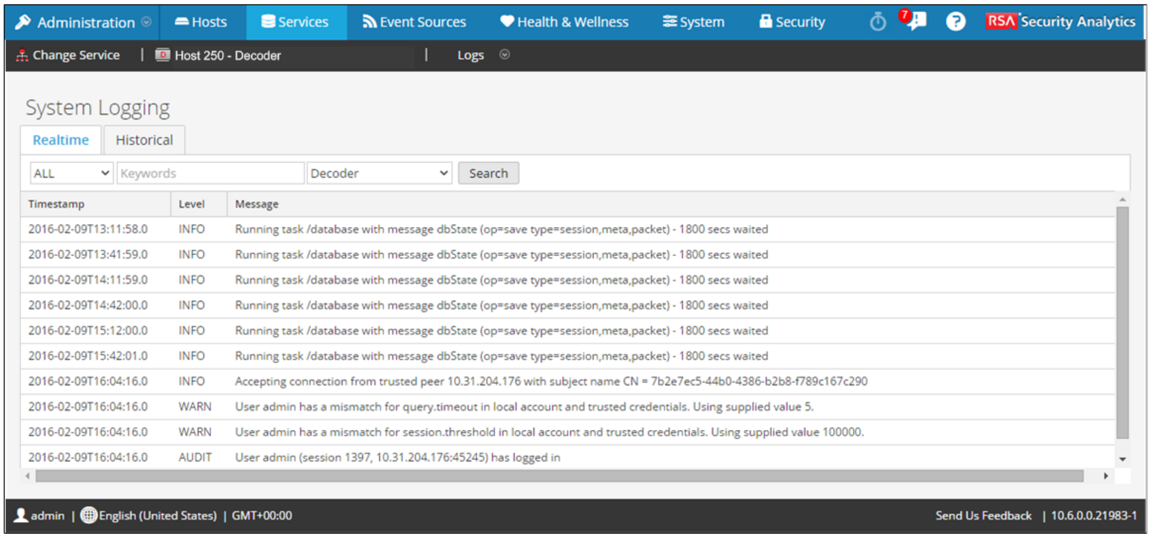
For information about accessing service logs, see Services Logs View.

The following is an example of the **Historical** tab in the System Logging panel. It shows the Security Analytics logs.



Timestamp	Level	Message
2016-02-04T13:01:32.1	DEBUG	SUBSCRIPTION: 3 Append LogEntries for jms://localhost:50077?carlos.uuid=ea4762e1-6927-48bc-8e13-1717...
2016-02-04T13:01:32.18	DEBUG	SUBSCRIPTION: 3 Append LogEntries for jms://localhost:50077?carlos.uuid=ea4762e1-6927-48bc-8e13-1717...
2016-02-04T13:01:32.25	DEBUG	User is External [false]
2016-02-04T13:01:32.84	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180...
2016-02-04T13:01:32.100	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180...
2016-02-04T13:01:32.108	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180...
2016-02-04T13:01:32.111	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180...
2016-02-04T13:01:32.114	DEBUG	SUBSCRIPTION: 3 Append LogEntries for jms://localhost:50077?carlos.uuid=ea4762e1-6927-48bc-8e13-1717...
2016-02-04T13:01:32.116	DEBUG	SUBSCRIPTION: 3 Append LogEntries for jms://localhost:50077?carlos.uuid=ea4762e1-6927-48bc-8e13-1717...
2016-02-04T13:01:32.123	DEBUG	SUBSCRIPTION: 3 Append LogEntries for jms://localhost:50077?carlos.uuid=ea4762e1-6927-48bc-8e13-1717...
2016-02-04T13:01:33.560	DEBUG	User is External [false]
2016-02-04T13:01:33.565	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180...
2016-02-04T13:01:33.570	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180...

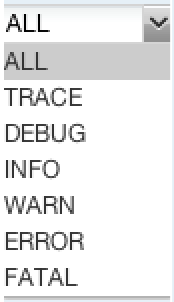
The following is an example of the **Historical** tab in the Services Logs view. It shows the services logs.



Timestamp	Level	Message
2016-02-09T13:11:58.0	INFO	Running task /database with message dbState (op=save type=session,meta,packet) - 1800 secs waited
2016-02-09T13:41:59.0	INFO	Running task /database with message dbState (op=save type=session,meta,packet) - 1800 secs waited
2016-02-09T14:11:59.0	INFO	Running task /database with message dbState (op=save type=session,meta,packet) - 1800 secs waited
2016-02-09T14:42:00.0	INFO	Running task /database with message dbState (op=save type=session,meta,packet) - 1800 secs waited
2016-02-09T15:12:00.0	INFO	Running task /database with message dbState (op=save type=session,meta,packet) - 1800 secs waited
2016-02-09T15:42:01.0	INFO	Running task /database with message dbState (op=save type=session,meta,packet) - 1800 secs waited
2016-02-09T16:04:16.0	INFO	Accepting connection from trusted peer 10.31.204.176 with subject name CN = 7b2e7ec5-44b0-4386-b2b8-f789c167c290
2016-02-09T16:04:16.0	WARN	User admin has a mismatch for query.timeout in local account and trusted credentials. Using supplied value 5.
2016-02-09T16:04:16.0	WARN	User admin has a mismatch for session.threshold in local account and trusted credentials. Using supplied value 100000.
2016-02-09T16:04:16.0	AUDIT	User admin (session 1397, 10.31.204.176:45245) has logged in

Features

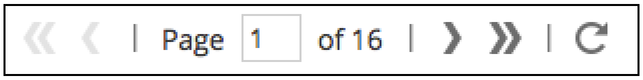
The **Historical** tab has a toolbar with input fields to allow filtering of the entries, a grid containing the log entries, and paging tools.

Feature	Description
Start Date and **End Date**	The **Start Date** and **End Date** range search options limit the log entries to a point in time. When used, you must provide both a start and end date. The times are optional. The date range is validated to assure that the end date is not before the start date.
Log Level drop-down  ALL ALL TRACE DEBUG INFO WARN ERROR FATAL	Selects the log level for entries to display in the grid. The **Log Level** drop-down shows the available log levels for the system or the service. • System logs have seven log levels. • Service logs have only six log levels because they do not include the **TRACE** level. • The default is **ALL** log entries.

Feature	Description
Keyword field	Specifies a keyword to use when filtering entries. This field is the same for system and service log filtering.
Service field (Service Logs only)	Specifies the service type to use when filtering service log entries. Possible values are the host or the service.
Search button	Click to activate a search based on the start and end date, log level, keyword, and service selections.
Export	Click to export the currently viewed grid entries to a text file. You can select either comma-separated or tab-separated format for the entries in the file.

Column	Description
Timestamp	This is the timestamp for the entry.
Level	This is the log level for the message.
Message	This is the text of the log entry.

The paging tools below the grid provide a way to navigate through the pages of log entries.



Tool	Description
«	First page
‹	Previous page
Page 1 of 16	Page number
›	Next page

Tool	Description
»	Last page
↻	Refresh

Search Log Entries

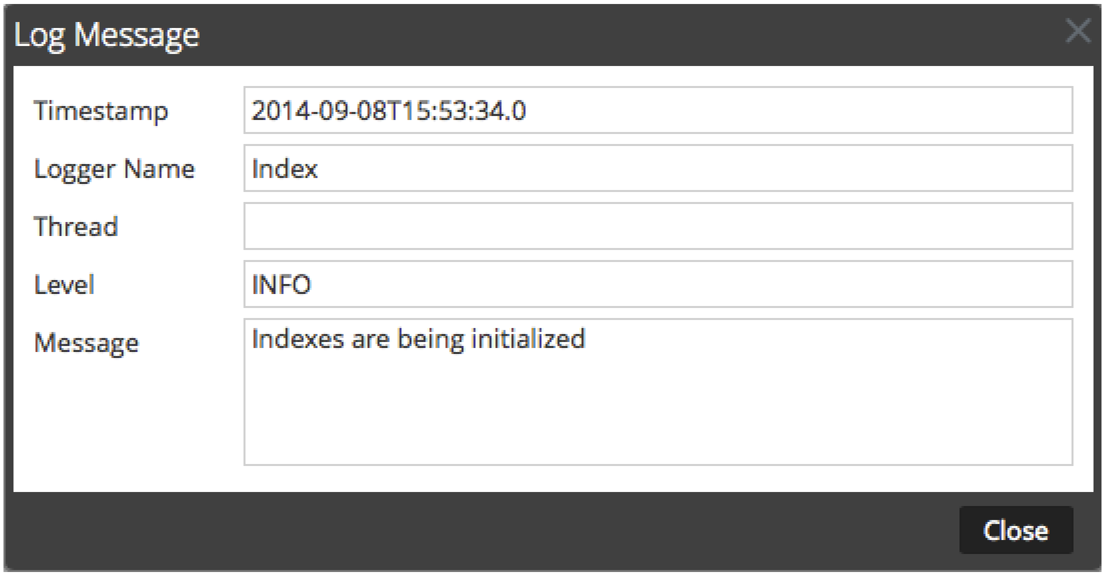
To search the results shown in the **Historical** tab:

1. (Optional) Select a **Start Date** and **End Date**. Optionally, select a **Start Time** and **End Time**.
2. (Optional) For system and service logs, select a **Log Level** and a **Keyword**, or both.
3. (Optional) For service logs, select the **Service**: host or service.
4. Click **Search**.
   The view is refreshed with the most recent 10 entries matching your filter. As new matching log entries become available, the view is updated to show those entries.

Show Details of a Log Entry

Each row of the **Historical** tab Log grid provides the summary information of a log entry. To view complete details:

1. Double-click a log entry.
   The Log Message dialog, which contains the Timestamp, Logger Name, Thread, Level and Message, is displayed.



Timestamp: 2014-09-08T15:53:34.0

Logger Name: Index

Thread:

Level: INFO

Message: Indexes are being initialized

2. When finished viewing, click **Close**.

Page Through the Entries

To view the different pages of the grid, use the paging controls on the bottom of the grid as follows:

- Use the navigation buttons
- Manually enter the page you want to view, and press **ENTER**.

Export

To export the logs in the current view:

Click **Export**, and select one of the drop-down options, **CSV Format** or **Tab Delimited**. The file is downloaded with a filename that identifies the log type and the field delimiter. For example, a Security Analytics system log exported with comma-separated values is named **UAP_log_export_CSV.txt**, and an appliance log exported with tab-separated values is named **APPLIANCE_log_export_TAB.txt**.

Realtime Tab

This topic describes the features of the System Logging > Realtime tab and the Services Logs view > Realtime tab.

The **Realtime** tab is a view of the Security Analytics log or a service log. When it is initially loaded, the view contains the last 10 log entries. As new entries become available, the view is updated with those entries.

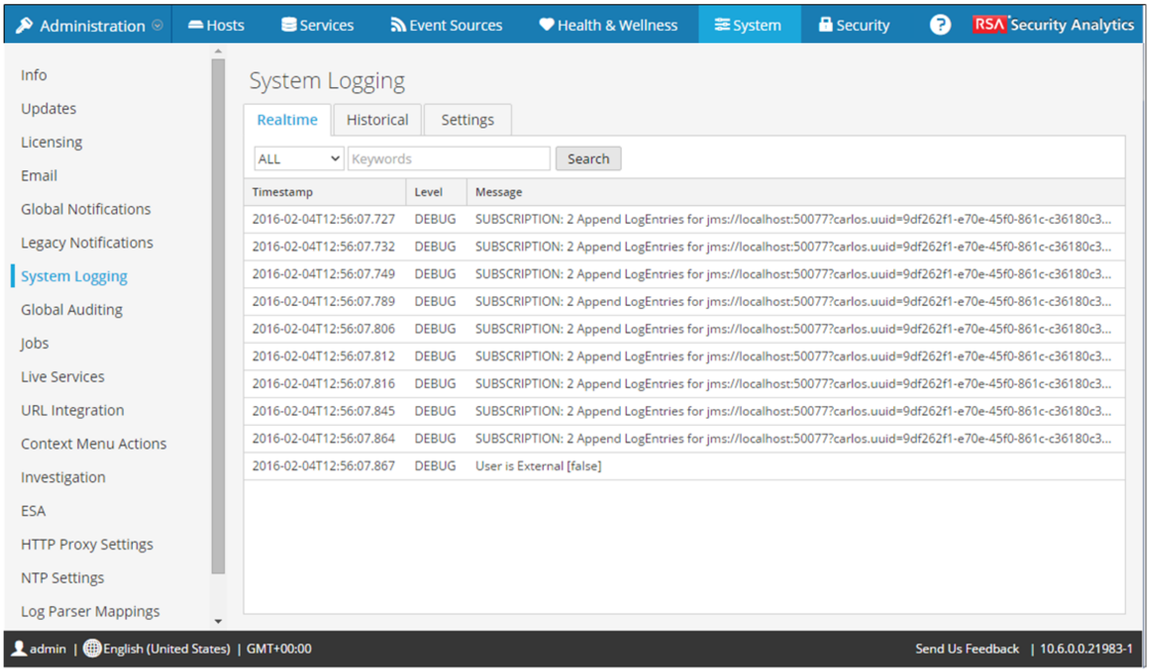
To access the Realtime tab:

1. In the **Security Analytics** menu, select **Administration > System.**
2. In the options panel, select **System Logging**.

   The System Logging panel opens to the **Realtime** tab by default.

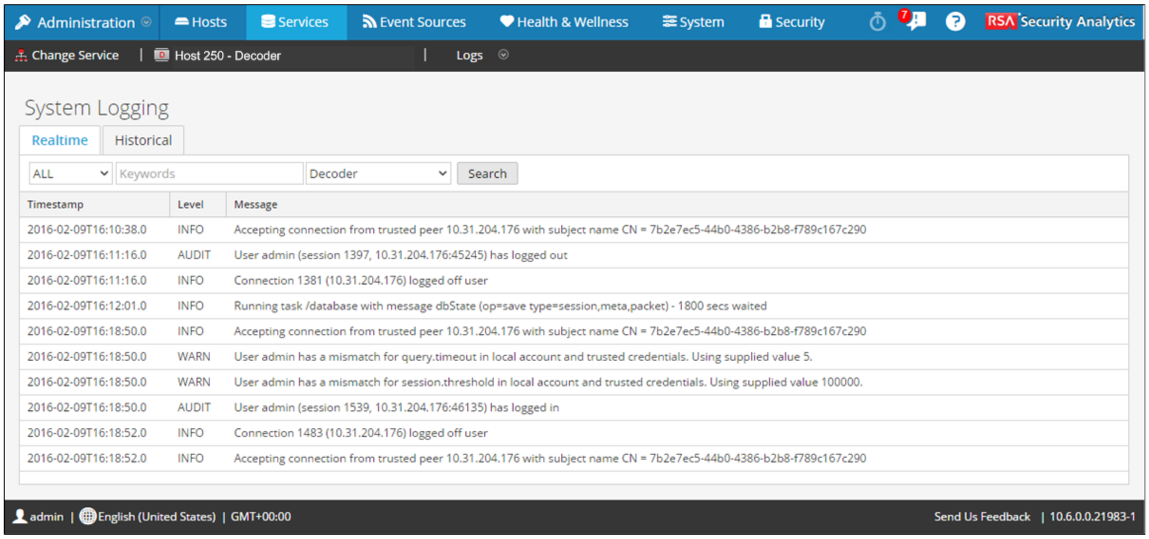
For information about accessing service logs, see Services Logs View.

The following is an example of the **Realtime** tab in the System Logging panel.



Timestamp	Level	Message
2016-02-04T12:56:07.727	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.732	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.749	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.789	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.806	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.812	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.816	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.845	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.864	DEBUG	SUBSCRIPTION: 2 Append LogEntries for jms://localhost:50077?carlos.uuid=9df262f1-e70e-45f0-861c-c36180c3...
2016-02-04T12:56:07.867	DEBUG	User is External [false]

The following is an example of the **Realtime** tab in the Services Logs view, which is similar.



Timestamp	Level	Message
2016-02-09T16:10:38.0	INFO	Accepting connection from trusted peer 10.31.204.176 with subject name CN = 7b2e7ec5-44b0-4386-b2b8-f789c167c290
2016-02-09T16:11:16.0	AUDIT	User admin (session 1397, 10.31.204.176:45245) has logged out
2016-02-09T16:11:16.0	INFO	Connection 1381 (10.31.204.176) logged off user
2016-02-09T16:12:01.0	INFO	Running task /database with message dbState (op=save type=session,meta,packet) - 1800 secs waited
2016-02-09T16:18:50.0	INFO	Accepting connection from trusted peer 10.31.204.176 with subject name CN = 7b2e7ec5-44b0-4386-b2b8-f789c167c290
2016-02-09T16:18:50.0	WARN	User admin has a mismatch for query.timeout in local account and trusted credentials. Using supplied value 5.
2016-02-09T16:18:50.0	WARN	User admin has a mismatch for session.threshold in local account and trusted credentials. Using supplied value 100000.
2016-02-09T16:18:50.0	AUDIT	User admin (session 1539, 10.31.204.176:46135) has logged in
2016-02-09T16:18:52.0	INFO	Connection 1483 (10.31.204.176) logged off user
2016-02-09T16:18:52.0	INFO	Accepting connection from trusted peer 10.31.204.176 with subject name CN = 7b2e7ec5-44b0-4386-b2b8-f789c167c290

Features

The **Realtime** tab has a toolbar with input fields to allow filtering of the entries, and below the toolbar is a grid containing the log entries.

Toolbar

Feature	Description
Log Level drop-down ALL ALL TRACE DEBUG INFO WARN ERROR FATAL	Selects the log level for entries to display in the grid. The **Log Level** drop-down shows the available log levels for the system or the service. • System logs have seven log levels. • Service logs have only six log levels because they do not include the **TRACE** level. • The default is **ALL** log entries.
Keywords field	Specifies a keyword to use when filtering entries. This field is the same for system and service log filtering.

Feature	Description
Service field (Service Logs only)	Specifies the service type to use when filtering service log entries. Possible values are the host or the service.
Filter button	Click to activate filtering based on the log level, keyword, and service selections.

Log Grid Columns

Column	Description
Timestamp	This is the timestamp for the entry.
Level	This is the log level for the message.
Message	This is the text of the log entry.

Settings Tab

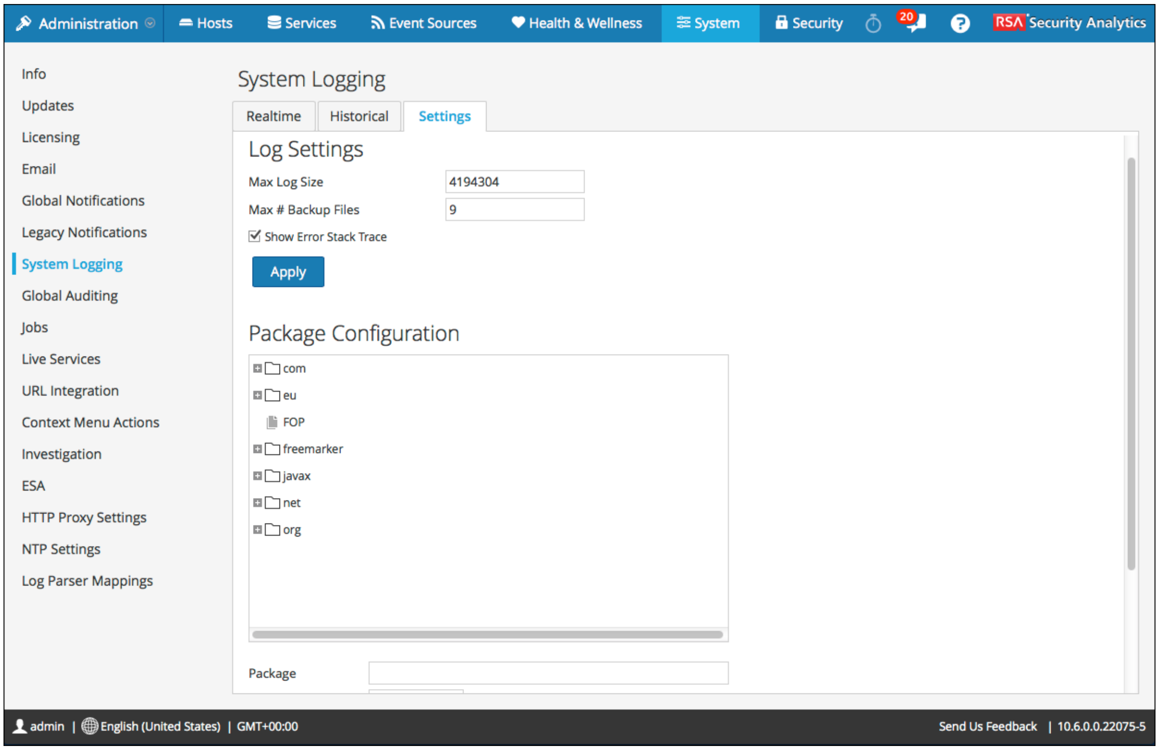
This topic introduces the features of the System Logging > Settings tab.

The RSA Security Analytics Settings tab in the System Logging panel configures the size of the log files, the number of backup log files maintained, as well as the default logging levels for the packages within Security Analytics. The **Configure Log File Settings** topic in the *System Configuration Guide* provides detailed procedures.

To access the Settings tab:

1. In the **Security Analytics** menu, select **Administration > System.**
2. In the options panel, select **System Logging**.

   The System Logging panel opens to the Realtime tab by default.
3. Click the **Settings** tab.



System Logging

Log Settings

Max Log Size 4194304

Max # Backup Files 9

☑ Show Error Stack Trace

Package Configuration

Package

Features

The **Settings** tab has two sections: Log Settings and Package Configuration.

Log Settings

The Log Settings section configures the size of the Security Analytics log files and the number of backup logs that Security Analytics maintains.

Feature	Description
Max Log Size	Configures the maximum size in bytes of each log file. The minimum value for this setting is **4096**.
Max # Backup Files	Specifies how many backup log files are maintained. The minimum value for this setting is **0**. When the maximum number of log files is attained, and a new backup file is made, the oldest backup is discarded.
□ Show Error Stack Trace	Select checkbox to display ERROR, STACK, and TRACE log messages.
Apply	Puts the settings into effect immediately for all future logs.

Package Configuration

The Package Configuration section shows the Security Analytics packages in a tree structure.

Feature	Description
Package tree	The tree contains all the packages used within Security Analytics. You can drill down into the tree to view the log levels of each package. The **root** logging level represents the default log level for all packages that are not explicitly set. The root level is set to **INFO**
Package field	This field is populated with the name of the selected package when you select a package in the **Package** tree.
Log Level	If the selected package has a log level explicitly set, the value is displayed in the **Log Level** field.

Feature	Description
□ Reset recursively	Select checkbox to reset the log recursively.
Apply	This button puts the settings into effect immediately for all future logs.
Reset	This button resets the selected package to the log level of **root**.

URL Integration Panel

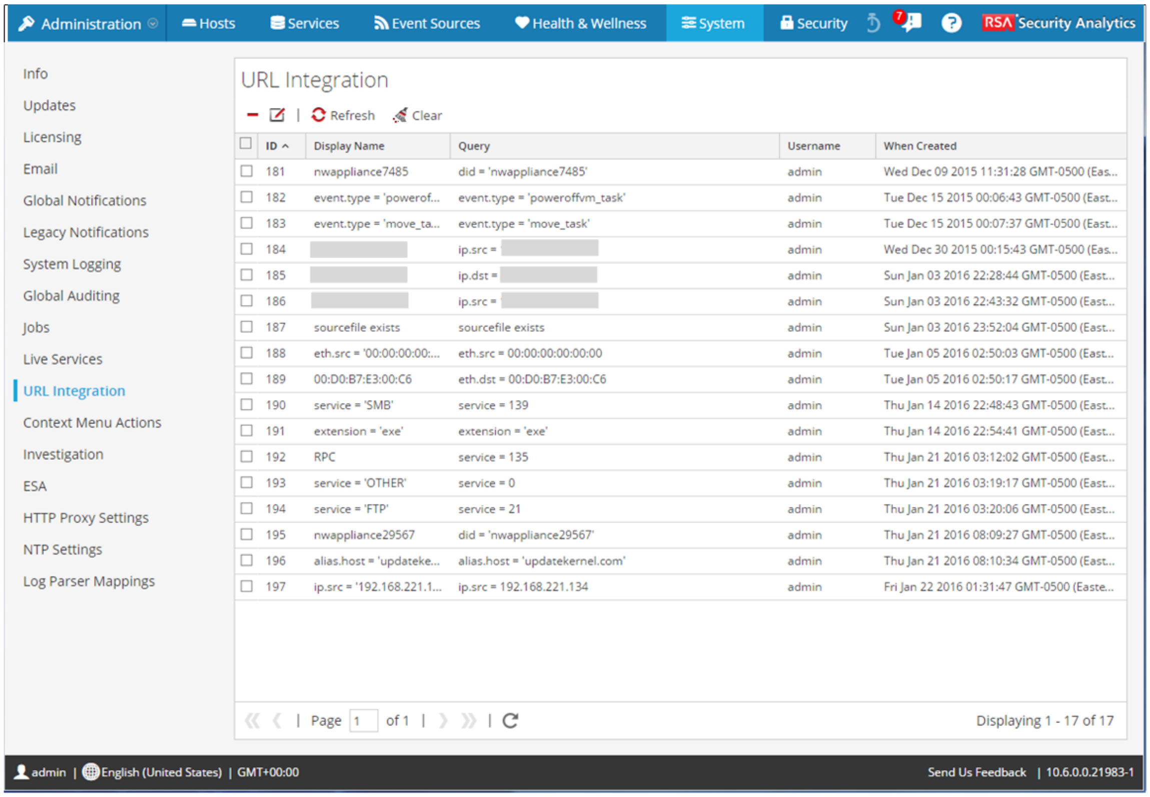
This topic introduces the features of the URL Integration panel.

URL integration provides a way to represent the breadcrumbs, or query paths, a user takes when actively investigating a service in the Navigation view. The need to view and modify these objects rarely occurs.

Caution: After a query has been removed from the system, any Investigation URLs that included the ID of that query will no longer function.

To access this view:

1. In the **Security Analytics** menu, click **Administration** > **System**.
2. In the options panel, select **URL Integration**.



□	ID ^	Display Name	Query	Username	When Created
□	181	nwappliance7485	did = 'nwappliance7485'	admin	Wed Dec 09 2015 11:31:28 GMT-0500 (Eas...
□	182	event.type = 'powerof...	event.type = 'poweroffvm_task'	admin	Tue Dec 15 2015 00:06:43 GMT-0500 (East...
□	183	event.type = 'move_ta...	event.type = 'move_task'	admin	Tue Dec 15 2015 00:07:37 GMT-0500 (East...
□	184	[redacted]	ip.src = [redacted]	admin	Wed Dec 30 2015 00:15:43 GMT-0500 (Eas...
□	185	[redacted]	ip.dst = [redacted]	admin	Sun Jan 03 2016 22:28:44 GMT-0500 (East...
□	186	[redacted]	ip.src = [redacted]	admin	Sun Jan 03 2016 22:43:32 GMT-0500 (East...
□	187	sourcefile exists	sourcefile exists	admin	Sun Jan 03 2016 23:52:04 GMT-0500 (East...
□	188	eth.src = '00:00:00:00:...	eth.src = 00:00:00:00:00:00	admin	Tue Jan 05 2016 02:50:03 GMT-0500 (East...
□	189	00:D0:B7:E3:00:C6	eth.dst = 00:D0:B7:E3:00:C6	admin	Tue Jan 05 2016 02:50:17 GMT-0500 (East...
□	190	service = 'SMB'	service = 139	admin	Thu Jan 14 2016 22:48:43 GMT-0500 (East...
□	191	extension = 'exe'	extension = 'exe'	admin	Thu Jan 14 2016 22:54:41 GMT-0500 (East...
□	192	RPC	service = 135	admin	Thu Jan 21 2016 03:12:02 GMT-0500 (East...
□	193	service = 'OTHER'	service = 0	admin	Thu Jan 21 2016 03:19:17 GMT-0500 (East...
□	194	service = 'FTP'	service = 21	admin	Thu Jan 21 2016 03:20:06 GMT-0500 (East...
□	195	nwappliance29567	did = 'nwappliance29567'	admin	Thu Jan 21 2016 08:09:27 GMT-0500 (East...
□	196	alias.host = 'updateke...	alias.host = 'updatekernel.com'	admin	Thu Jan 21 2016 08:10:34 GMT-0500 (East...
□	197	ip.src = '192.168.221.1...	ip.src = 192.168.221.134	admin	Fri Jan 22 2016 01:31:47 GMT-0500 (Easte...

Components

The URL Integration panel has a grid and a toolbar. This table describes the information in the grid.

Column	Description
ID	This is a unique ID that is used to look up the query in the Security Analytics data store.
Display Name	This is the string that is displayed in the breadcrumb trail.
Query	This is the underlying query snippet.
Username	This is the name of the user who made the query.
When Created	This is the date and time that the query was made.

The toolbar has these options.

Option	Description
−	Deletes the selected queries. Security Analytics requests confirmation that you want to delete the queries. You can respond **Yes** or **No**.
✎	Displays the Edit Query dialog.
⟳	Refreshes the list.
Clear	Clears the entire list of queries. Security Analytics requests confirmation that you want to clear the list. You can respond **Yes** or **No**.

Service Configuration Settings

This topic introduces the available service configuration settings for RSA Security Analytics Core services.

RSA Security Analytics Core services include Brokers, Concentrators, Decoders, Log Decoders, Archivers, and the Appliance service. The service configuration parameters listed in these tables constitute all viewable and configurable parameters. Some parameters are configurable in various parts of the Security Analytics user interface and others are viewable or configurable only on the Services Explore view.

Topics

- Appliance Service Configuration
- Archiver Service Configuration
- Broker Service Configuration
- Aggregation Configuration Nodes
- Concentrator Service Configuration
- Core Service Logging Configuration
- Core Service-to-Service Configuration
- Core Service System Configuration
- Decoder Service Configuration
- Decoder and Log Decoder Common Configuration
- Log Decoder Service Configuration
- REST Interface Configuration
- Security Analytics Core Service system.roles Modes

Appliance Service Configuration

This topic lists and describes the available the configuration parameters for the RSA Security Analytics Core Appliance service.

The RSA Security Analytics Core Appliance service provides hardware monitoring on legacy NetWitness hardware.

Settings

This table describes the Appliance Configuration settings.

Appliance Setting Field	Description
Logs	/logs/config, see Core Service Logging Configuration
REST	/rest/config, see REST Interface Configuration
Services	/services/<service name>/config, see Core Service-to-Service Configuration
System	/sys/config, see Core Service System Configuration

Archiver Service Configuration

This topic lists and describes the available configuration settings for RSA Security Analytics Archivers.

Archiver Configuration Settings

This table lists and describes the Archiver configuration settings.

Archiver Setting Field	Description
Archiver	/archiver/config refer to Aggregation Configuration Nodes
Database	/database/config refer to the **Database Configuration Nodes** topic in the *Security Analytics Core Database Tuning Guide*
Index	/index/config refer to the **Index Configuration Nodes** topic in the *Security Analytics Core Database Tuning Guide*
Logs	/logs/config refer to Core Service Logging Configuration
REST	/rest/config refer to REST Interface Configuration
SDK	/sdk/config refer to the **SDK Configuration Nodes** topic in the *Security Analytics Core Database Tuning Guide* and Security Analytics Core Service system.roles Modes
Services	/services/<service name>/config refer to Core Service-to-Service Configuration
System	/sys/config refer to Core Service System Configuration

Broker Service Configuration

This topic lists and describes the configuration settings for RSA Security Analytics Brokers.

Broker Configuration Settings

This table lists and describes the Broker configuration settings.

Broker Setting Field	Description
Broker	/broker/config refer to Aggregation Configuration Nodes
aggregate.interval.behind	Minimum number of milliseconds before another round of aggregation is requested when the broker is behind. Change takes effect immediately.
Database	/database/config refer to the **Database Configuration Nodes** topic in the *Security Analytics Core Services Database Tuning Guide*
Index	/index/config
index.dir	The directory where the broker device mapping files are stored. Change takes effect on service restart.
language.filename	The index language specification (XML) that is loaded on startup. Change requires service restart.
Logs	/logs/config refer to Core Service Logging Configuration
REST	/rest/config refer to REST Interface Configuration
SDK	/sdk/config refer to the **SDK Configuration Nodes** topic in the *Security Analytics Core Services Database Tuning Guide* and Security Analytics Core Service system.roles Modes
Services	/services/<service name>/config refer to Core Service-to-Service Configuration
System	/sys/config refer to Core Service System Configuration

Aggregation Configuration Nodes

This topic lists and describes the available configuration settings that are common to services that perform aggregation, such as RSA Security Analytics Concentrators and Archivers.

Aggregation Configuration Settings

This table lists and describes the settings that control aggregation on an aggregating service.

Configuration Path	/concentrator/config or /archiver/config
aggregate.autostart	Automatically restarts aggregation after a service restart, if enabled. Change takes effect immediately.
aggregate.buffer.size	Displays the size of the buffer (default unit is KB) used per round of aggregation. Larger buffers may improve aggregation performance but could impact query performance. Change takes effect after aggregation restart.
aggregate.crc	If enabled, all aggregation streams will be CRC validated. Change takes effect immediately.
aggregate.hours	Displays the maximum number of hours behind a service will be allowed to start aggregation. Change takes effect immediately.
aggregate.interval	Lists the minimum number of milliseconds before another round of aggregation is requested. Change takes effect immediately.
aggregate.meta.page.factor	Lists the allocated number meta pages per session used for aggregation. Change takes effect on service restart.
aggregate.meta.perpage	Lists the allocated number of meta stored on one page of data. Change takes effect on service restart.

Configuration Path	/concentrator/config or /archiver/config
aggregate.precache	Determines if the concentrator will precache the next round of aggregation for upstream services. Can improve aggregation performance but could impact query performance. Change takes effect immediately.
aggregate.sessions.max	Lists the number of sessions to aggregate on each round. Change takes effect after aggregation restart.
aggregate.sessions.perpage	Lists the number of sessions stored on one page of data. Change takes effect on service restart.
aggregate.time.window	Displays the maximum +/- time window, in seconds, that all services must be inside before another round of aggregation is requested. Zero turns off time window. Change takes effect immediately.
consume.mode	Determines if the concentrator can only aggregate locally or over a network, based on licensing restrictions. Change takes effect on service restart.
export.enabled	Allows export of session data, if enabled. Change takes effect on service restart.
export.expire.minutes	Lists the number of minutes before export cache files are expired and flushed. Change takes effect immediately.
export.format	Determines the file format used during data export. Change takes effect on service restart.
export.local.path	Displays the local location to cache exported data. Optional assigned max size (=#unit), units are: t for TB; g for GB, m for MB. Change takes effect on service restart.

Configuration Path	/concentrator/config or /archiver/config
export.meta.fields	Determines which meta fields are exported. Comma list of fields. Star means all fields. Star plus field list means all fields BUT listed fields. Just field list says just include those fields. Change takes effect immediately.
export.remote.path	Displays the remote protocol (nfs://) and location to export data. Change takes effect on service restart.
export.rollup	Determines the rollup interval for export files. Change takes effect on service restart.
export.session.max	Displays the maximum sessions per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
export.size.max	Displays the maximum bytes per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
export.usage.max	Displays the maximum percentage of cache space used before stopping aggregation. Zero is no limit. Change takes effect immediately.
heartbeat.error	Lists the number of seconds to wait after a service error before attempting a service reconnect. Change takes effect immediately.
heartbeat.interval	Lists the number of milliseconds between heartbeat service checks. Change takes effect immediately.
heartbeat.next.attempt	Lists the number of seconds to wait before attempting a service reconnect. Change takes effect immediately.
heartbeat.no.response	Lists the number of seconds to wait before taking unresponsive service offline. Change takes effect immediately.

Concentrator Service Configuration

This topic lists and describes the available configuration settings for RSA Security Analytics Concentrators.

Concentrator Configuration Settings

This table lists and describes the Concentrator configuration settings.

Concentrator Setting Field	Description
Concentrator	/concentrator/config refer to Aggregation Configuration Nodes
Database	/database/config refer to the **Database Configuration Nodes** topic in the *Security Analytics Core Database Tuning Guide*
Index	/index/config refer to the **Index Configuration Nodes** topic in the *Security Analytics Core Database Tuning Guide*
Logs	/logs/config refer to Core Service Logging Configuration
REST	/rest/config refer to REST Interface Configuration
SDK	sdk/config refer to the **SDK Configuration Nodes** topic in the *Security Analytics Core Database Tuning Guide*and Security Analytics Core Service system.roles Modes
Services	/services/<service name>/config refer to Core Service-to-Service Configuration
System	/sys/config refer to Core Service System Configuration

Core Service Logging Configuration

This topic lists and describes the logging configuration parameters for all RSA Security Analytics Core services.

Logging configuration is the same on all Security Analytics Core services.

The following table describes the logging configuration settings:

Logs Configuration Folder	/logs/config
log.dir	Displays the directory where the log database is stored. Optional assigned max size (=#) is in MBs. Change takes effect on service restart.
log.levels	Controls what types of log messages are stored (comma separated). Module specific settings are defined like this: <Module>=[debug|info|audit|warning|failure|all|none]. Change takes effect immediately.
log.snmp.agent	Sets a remote SNMP Trap Receiving agent.
snmp.trap.version	Sets the SNMP version to be used for gets and traps (2c or 3).
snmpv3.engine.boots	Displays the SNMPv3 engine boots count. This field auto-increments on startup and should not normally need to be set by the user.

Logs Configuration Folder	/logs/config
snmpv3.engine.id	Sets the SNMPv3 engine ID, which is 10-64 hexadecimal digit number optionally preceded by 0x. You can add suffix values at the end of the engine ID for each of the SA Core services running on the same host. For example, if the generated Engine ID for the SA Core host is 0x1234512345, you can set the Engine ID for the Decoder service as 0x123451234501 and set 0x123451234504 for the Appliance service.
snmpv3.trap.auth.local.key	Sets the SNMPv3 Trap Authentication Local Key, which is a 16 or 20 hexadecimal digit number (depending on which authentication protocol is used) preceded by 0x. For MD5, the key is 16 hexadecimal digits, while SHA uses 20 hexadecimal digits. You can use any desired algorithm to generate the local keys. It is recommended that a generation method involving randomness be used as opposed to selecting key values manually.
snmpv3.trap.auth.protocol	Displays the SNMPv3 Trap Authentication Protocol (none, MD5 or SHA).
snmpv3.trap.priv.local.key	Sets the SNMPv3 Trap Privacy Local Key, which is a 16 hexadecimal digit number preceded by 0x.
snmpv3.trap.priv.protocol	Displays the SNMPv3 Trap Privacy Protocol (none or AES).
snmpv3.trap.security.level	Displays the SNMPv3 Trap Security Level, which indicates whether authentication and privacy are used or not. Possible values are noAuthNoPriv, authNoPriv or authPriv.
snmpv3.trap.security.name	Sets the SNMPv3 Trap Security Name used during SNMPv3 trap authentication.

Logs Configuration Folder	/logs/config
syslog.size.max	Displays the maximum size of a log sent to syslog (some syslog daemons have issues with very large messages). Zero means no limit. Change takes effect immediately.

Core Service-to-Service Configuration

This topic lists and describes the configuration parameters that control how a Core service connects to another Core service. For example, when a Concentrator connects to a decoder, the parameters of that connection are controlled by these settings.

Whenever a Core service establishes a connection to another Core service, the service that acts as the **client** creates a new sub-folder in the /services folder of the configuration tree. The name of the sub-folder corresponds to the name of the service and has the form `host:port`. For example, the service connection folder for a Concentrator connection to a Decoder could be `/services/reston-va-decoder:50004`. Inside each service connection folder, there is a `config` sub-folder that holds configurable parameters.

The following table describes the Service Configuration settings:

Services	/services/host:port/config
allow.nonssl.to.ssl	Allows a non-SSL connection to connect to a SSL service, when set to true. Otherwise, if false, non-secure to secure connections will be denied. Change takes effect immediately.
compression	Displays a config node that determines if data is compressed before sending. A positive value determines the number of bytes that need to be sent before it will be compressed. Zero means no compression.
crc.checksum	Displays a config node that determines if data streams are validated with a CRC checksum. A positive value determines the number of bytes that need to be sent before it will be CRC validated. Zero means no CRC validation.
ssl	Displays a config node that enables or disables SSL encryption on the connection.

Core Service System Configuration

This topic lists and describes the configuration parameters that are common to all RSA Security Analytics Core services.

Settings

The following table lists and describes the System configuration settings:

System Configuration Folder	/sys/config
compression	Displays the minimum amount of bytes before a message is compressed, when set to a positive value. Zero means no compression for any message. Change takes effect on subsequent connections.
crc.checksum	Displays the minimum bytes before a message is sent over the network with a CRC checksum (to be validated by the client), when set to a positive value. Zero means no CRC checksum validation with any message. Change takes effect on subsequent connections.
drives	Displays drives to monitor for usage stats. Change takes effect on service restart.
port	Displays the port this service will listen on. Change takes effect on service restart.
scheduler	Displays the folder for scheduled tasks.
service.name.override	Displays an optional service name used by upstream services for aggregation in lieu of hostname.
ssl	Encrypts all traffic using SSL, if enabled. Change takes effect on service restart.

System Configuration Folder	/sys/config
stat.compression	Compresses stats as they are written to the database, if enabled. Change takes effect on service restart.
stat.dir	Displays the directory where the historical stats database is stored (separate multiple dirs with semicolon). Optional assigned max size (=#unit), units are: t for TB; g for GB, m for MB. Change takes effect on service restart.
stat.exclude	Lists stat pathnames to be excluded from the stat database. The following wildcards are permitted: ? match any single character, * match zero or more characters to delimiter /, ** match zero or more characters including delimiter. Change takes effect immediately.
stat.interval	Determines how often (in milliseconds) statistic nodes are updated in the system. Change takes effect immediately.
threads	Lists the number of threads in the thread pool to handle incoming requests. Change takes effect immediately.

Decoder Service Configuration

This topic lists and describes the available configuration parameters for RSA Security Analytics Decoders.

Decoder Configuration Settings

This table lists and describes the Decoder configuration settings.

Decoder Setting Field	Description
Decoder	/decoder/config refer to Decoder and Log Decoder Common Configuration
Database	/database/config refer to the **Database Configuration Nodes** topic in the *Security Analytics Core Database Tuning Guide*
Index	/index/config refer to the **Index Configuration Nodes** topic in the *Security Analytics Core Database Tuning Guide*
Logs	/logs/config refer to Core Service Logging Configuration
REST	/rest/config refer to REST Interface Configuration
SDK	/sdk/config refer to the **SDK Configuration Nodes** topic in the *Security Analytics Core Database Tuning Guide*and Security Analytics Core Service system.roles Modes
System	/sys/config refer to Core Service System Configuration

Decoder and Log Decoder Common Configuration

This topic lists and describes the configuration parameters that are identical on both packet decoder and log decoder services.

Decoder Configuration Settings

This table lists and describes the Decoder and Log Decoder shared configuration settings.

Decoder Configuration Path	/decoder/config
aggregate.buffer.size	Displays the size of the buffer (default unit is KB) used per round of aggregation. Larger buffers may improve aggregation performance but could impact capture performance. Change takes effect after capture restart.
aggregate.precache	Determines if the decoder will precache the next round of aggregation for upstream services. Can improve aggregation performance but could impact capture performance. Change takes effect immediately.
assembler.pool.ratio	Displays the percentage of pool pages that assembler manages and uses for the assembly process. Change takes effect on service restart.
assembler.session.flush	Flushes sessions when they are complete (1) or flushes sessions when they are parsed (2). Change takes effect on service restart.
assembler.session.pool	Lists the number of entries in the session pool. Change takes effect on service restart.
assembler.size.max	Lists the maximum size that a session will obtain. A setting of 0 removes the session size limit. Change takes effect immediately.

Decoder Configuration Path	/decoder/config
assembler.size.min	Lists the minimum size that a session must be before persisting. Change takes effect immediately.
assembler.timeout.packet	Lists the number of seconds before packets are timed out. Change takes effect immediately.
assembler.timeout.session	Lists the number of seconds before sessions are timed out. Change takes effect immediately.
assembler.voting.weights	Displays the weights used to determine which session stream is marked client and server. Change takes effect immediately.
capture.autostart	Determines if capture begins automatically when the service starts. Change takes effect on service restart.
capture.buffer.size	Displays capture memory buffer allocation size (default unit is MB). Change takes effect on service restart.

Decoder Configuration Path	/decoder/config
capture.device.params	Displays capture service specific parameters. Change takes effect on service restart. The parameters understood by this field are specific to the currently selected capture device. If any of the parameters are not recognized by the current capture device, they are ignored. On Log Decoders, there is only the Log Events capture device. It accepts some optional parameters. • **use-envision-time**: If this is set to 1, the time meta for each event will be imported from the Log Collector stream. If this is 0 or not set, the imported event time will be stored in the event.time meta. • **port**: This parameter can be set to a numeric value to override the default syslog port listener, 514.
capture.selected	Displays current capture service and interface. Change takes effect immediately.
export.expire.minutes	Lists the number of minutes before export cache files are expired and flushed. Change takes effect immediately.
export.packet.enabled	Allows export of packet data, if enabled. Change takes effect on service restart.
export.packet.local.path	Displays the local location to cache packet exported data. Optional assigned max size (=#unit), units are: t for TB; g for GB, m for MB. Change takes effect on service restart.

Decoder Configuration Path	/decoder/config
export.packet.max	Displays the maximum packets per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
export.packet.remote.path	Lists the remote protocol (nfs://) and location to export data. Change takes effect on service restart.
export.packet.size.max	Displays the packet maximum bytes per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
export.rollup	Determines the rollup interval for export files. Change takes effect on service restart.
export.session.enabled	Allows export of session data, if enabled. Change takes effect on service restart.
export.session.format	Determines the file format used during session export. Change takes effect on service restart.
export.session.local.path	Displays the local location to cache session exported data. Optional assigned max size (=#unit), units are: t for TB; g for GB, m for MB. Change takes effect on service restart.
export.session.max	Displays the maximum sessions per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.

Decoder Configuration Path	/decoder/config
export.session.meta.fields	Determines which meta fields are exported. Comma list of fields. Star means all fields. Star plus field list means all fields BUT listed fields. Just field list says just include those fields. Change takes effect immediately.
export.session.remote.path	Displays the remote protocol (nfs://) and location to export data. Change takes effect on service restart.
export.session.size.max	Lists the session maximum bytes per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
export.usage.max	Lists the session maximum bytes per exported file. For export file types that cache this determines cached memory sizes. Zero is no limit. Change takes effect immediately.
parse.threads	Lists the number of parse threads to use for session parsing. Zero means let server decide. Change takes effect on service restart.
pool.packet.page.size	Displays the size of a packet page (default is KB). Change takes effect on service restart.
pool.packet.pages	Lists the number of packet pages decoder will allocate and use. Change takes effect on service restart.
pool.session.page.size	Displays the size of a session page (default is KB). Change takes effect on service restart.
pool.session.pages	Lists the number of session pages decoder will allocate and use. Change takes effect on service restart.

Log Decoder Service Configuration

This topic lists and describes the available configuration parameters for RSA Security Analytics Log Decoders.

Log Decoder Configuration Settings

This table lists and describes the Log Decoder configuration settings.

Log Decoder Setting Field	Description
Database	/database/config refer to the **Database Configuration Nodes** topic in the *Security Analytics Core Database Tuning Guide*
Decoder	/decoder/config refer to Decoder and Log Decoder Common Configuration
Index	/index/config refer to the **Index Configuration Nodes** topic in the *Security Analytics Core Database Tuning Guide*
Logs	/logs/config refer to Core Service Logging Configuration
REST	/rest/config refer to REST Interface Configuration
SDK	/sdk/config refer to the **SDK Configuration Nodes** topic in the *Security Analytics Core Database Tuning Guide*and Security Analytics Core Service system.roles Modes
System	/sys/config refer to Core Service System Configuration

Log Tokenizer Configuration Settings

The log decoder has a set of configuration items that control how the automatic log tokenizer creates meta items from unparsed logs. The log tokenizer is implemented as a set of built-in parsers that each scan for a subset of recognizable tokens. The functionality of each of these native parsers is shown in the table below. These word items form a full-text index when they are fed to the indexing engine on the Concentrator and Archiver. By manipulating the parsers.disabled configuration entry, you can control which Log Tokenizers are enabled.

Parser Name	Description	Configuration Parameters
Log Tokens	Scans for runs of consecutive characters to produce 'word' meta items.	token.device.types, token.char.classes, token.max.length, token.min.length, token.unicode
IPSCAN	Scans for text that appears to be an IPv4 address to produce 'ip.addr' meta items.	token.device.types
IPV6SCAN	Scans for text that appears to be an IPv6 address to produce 'ipv6' meta items.	token.device.types
URLSCAN	Scans for text that appears to be a URI to produce 'alias.host', 'filename', 'username', and 'password' meta items.	token.device.types
DOMAINSCAN	Scans for text that appears to be a domain name to produce 'alias.host', 'tld', 'cctld', and 'sld' meta items.	token.device.types

Parser Name	Description	Configuration Parameters
EMAILSCAN	Scans for text that appears to be an email address to produce 'email' and 'username' meta items.	token.device.types
SYSLOGTIMESTAMPSCAN	Scans for text that appears to be syslog-format timestamps. Syslog is missing the year and time zone. When such text is located, it is normalized into UTC time to create 'event.time' meta items.	token.device.types
INTERNETTIMESTAMPSCAN	Scans for text that appears to be RFC 3339-format timestamps to create 'event.time' meta items.	token.device.types

These are the Log Tokenizer configuration parameters.

Log Decoder Parser Setting Field	Description
token.device.types	The set of device types that will be scanned for raw text tokens. By default, this is set to `unknown`, which means only logs that were not parsed will be scanned for raw text. You can add additional log types here to enrich parsed logs with text token information. If this field is empty, then log tokenization is disabled.

Log Decoder Parser Setting Field	Description
token.char.classes	This field controls the type of tokens that are generated. It can be any combination of the values `alpha`, `digit`, `space`, and `punct`. The default value is `alpha`. • **alpha**: Tokens may contain alphabetic characters • **digit**: Tokens may contain numbers • **space**: Tokens may contain spaces and tabs • **punct**: Tokens may contain punctuation marks
token.max.length	This field puts a limit on the length of the tokens. The default value is 5 characters. The maximum length setting allows the Log Decoder to limit the space needed to store the word metas. Using longer tokens requires more meta database space, but may provide slightly faster raw text searches. Using shorter tokens causes the text query resolver to have to perform more reads from the raw logs during searches, but it has the effect of using much less space in the metadb and index.
token.min.length	This is the minimum length of a searchable text token. The minimum token length will correspond to the minimum number of characters a user may type into the search box in order to locate results. The recommended value is the default, 3.

Log Decoder Parser Setting Field	Description
token.unicode	This Boolean setting controls whether Unicode classification rules are applied when classifying characters according to the token.char.classes setting. If this is set to true, each log is treated as a sequence of UTF-8 encoded code points and then classification is performed after the UTF-8 decoding is performed. If this is set to false, then each log is treated as ASCII characters and only ASCII character classification is done. Unicode character classification requires more CPU resources on the Log Decoder. If you do not need non-English text indexing, you can disable this setting to reduce CPU utilization on the Log Decoder. The default is enabled.

REST Interface Configuration

This topic lists and describes the available configuration settings for the REST interface built in to all RSA Security Analytics Core Services.

Settings

The following table lists and describes the REST configuration settings:

REST Configuration Path	/rest/config
cache.dir	Displays the host directory to use for temporarily creating and storing files. Change takes effect on service restart.
cache.size	Displays the total maximum size (default unit is MB) of all files in the cache directory before the oldest are deleted. Change takes effect on service restart.
enabled	Switches to enable or disable REST services, 1 is on, 0 is off. Change takes effect on service restart.
port	Displays the port the REST service will listen on. Change takes effect on service restart.
ssl	Encrypts all REST traffic using SSL, if enabled. The default 'system' means use setting from /sys/config/ssl. Change takes effect on service restart.

Security Analytics Core Service system.roles Modes

All Security Analytics Core services offer role-based authorization modes. This topic describes the modes that are available, and how they are configured within every service.

system.roles

The configuration node `/sdk/config/system.roles` sets querying and viewing permissions for meta and content on a per key basis. This parameter supports the data privacy management function and when enabled using one of the non-zero values helps a data privacy officer to control access to specific meta keys and content. This parameter is configurable in the Security Analytics user interface (see the **Data Privacy Tab** topic in the *Data Privacy Management* guide for details). When the value is edited, change takes effect immediately.

Zero means that service permissions based on SDK meta keys are disabled.

- 0 - disabled

When one of the non-zero values is specified, the data privacy officer can select a meta key to whitelist or blacklist the display of the associated meta, content, or both, for a specific user role on a service.

- 1 - whitelist meta and content filtered
- 2 - whitelist meta filtered
- 3 - whitelist content filtered
- 4 - blacklist meta and content filtered
- 5 - blacklist meta filtered
- 6 - blacklist content filtered

Hosts View

You manage and configure the hosts and host groups that are available to RSA Security Analytics modules in the Hosts view. Use this view to perform the following tasks.

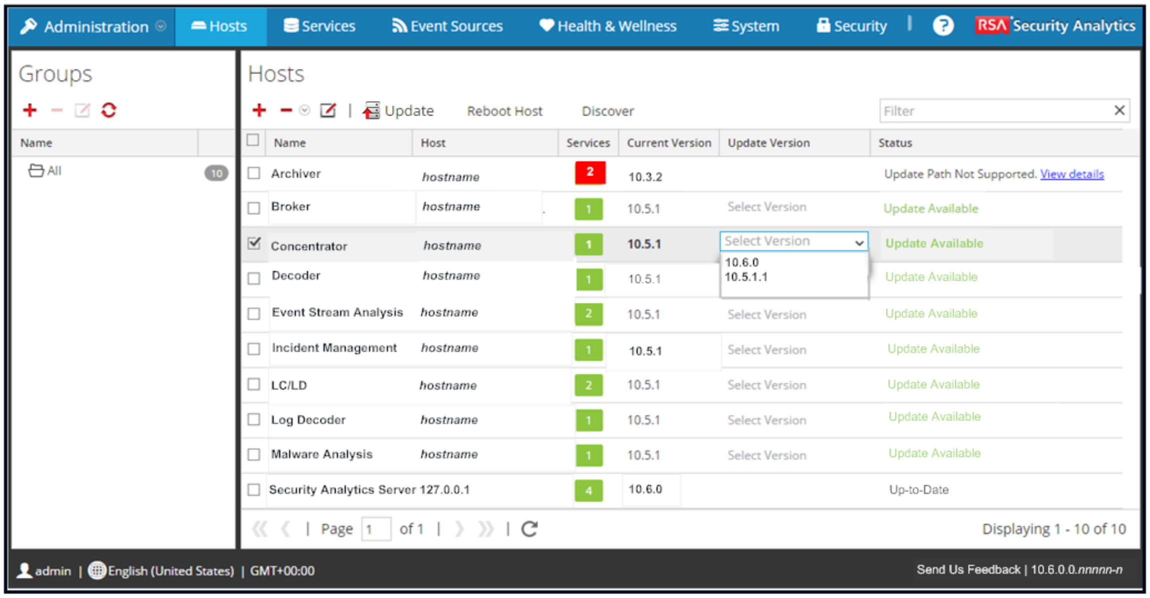
- Quickly search for and locate a specific host or type of host, such as Decoder, Broker, or Concentrator.
- Add, edit, or delete hosts.
- Check for updates on hosts.
- Update a host to a new version.
- Add, edit, or delete host groups.
- Sort hosts by Name and Host.
- Filter hosts by Name and Host.
- Clear provisions on hosts.

Hosts can be physical or virtual and they can map to one or more of the following services.

- Archiver
- Broker
- Concentrator
- Decoder
- Event Stream Analysis
- Incident Management
- IPDB Extractor
- Log Collector
- Log Decoder
- Malware Analysis
- Reporting Engine
- Warehouse Connector
- Workbench

You can access the services on any host by clicking the button in the Services column for that host.

Select **Administration** > **Hosts** in the **Security Analytics** menu to access the Hosts view from any Security Analytics module.



☐	Name	Host	Services	Current Version	Update Version	Status
☐	Archiver	*hostname*	2	10.3.2		Update Path Not Supported. View details
☐	Broker	*hostname*	1	10.5.1	Select Version	Update Available
☑	Concentrator	*hostname*	1	10.5.1	Select Version 10.6.0 10.5.1.1	Update Available
☐	Decoder	*hostname*	1	10.5.1		Update Available
☐	Event Stream Analysis	*hostname*	2	10.5.1	Select Version	Update Available
☐	Incident Management	*hostname*	1	10.5.1	Select Version	Update Available
☐	LC/LD	*hostname*	2	10.5.1	Select Version	Update Available
☐	Log Decoder	*hostname*	1	10.5.1	Select Version	Update Available
☐	Malware Analysis	*hostname*	1	10.5.1	Select Version	Update Available
☐	Security Analytics Server	127.0.0.1	4	10.6.0		Up-to-Date

Features

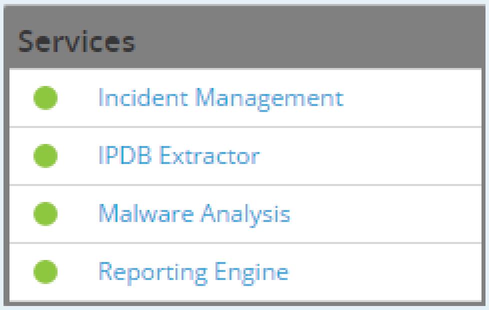
The Hosts view has two panels:

- Hosts panel
- Groups panel

Hosts Panel

In the Hosts panel, you can view information about hosts and perform host operations such as adding, deleting, editing, discovering, updating, and rebooting. You can quickly toggle to the Services view to get detailed information on those services. The Hosts panel contains the list of Security Analytics hosts in your Security Analytics deployment and the Hosts Panel Toolbar.

Column	Description
☐	Select a host or multiple hosts. If you select the checkbox in the column title, it selects all hosts.
Name	The name of the host.
Host	The hostname or IP address of the host.

Column	Description
Services	Displays the number of services connected to the host in the box. The color of the box indicates the status of the services. Green indicates that all of the connected services are started (for example, capturing or aggregating data). Yellow indicates that some of the connected services are started. Red indicates that the connected services are stopped. Click the box under **Services** to show the type of services connected to the host. Security Analytics services are the Archiver, Broker, Concentrator, Context Hub, Decoder, Event Stream Analysis, Incident Management, IPDB Extractor, Log Decoder, Log Collector, Malware Analysis, Reporting Engine, Warehouse Connector, and Workbench. A solid colored green circle indicates that a connected service is started. A blank and white circle indicates that a connected service is stopped.  Services ● Incident Management ● IPDB Extractor ● Malware Analysis ● Reporting Engine You can click the service links to toggle to the Services view for more information about the connected services.
Current Version	Displays the current version of the host.
Update Version	Displays the version or versions to which you can update the host. Select the version to which you want update the host. • When there is only one version is available, Security Analytics displays the `version-number`. Click on it to select it. • When there are multiple versions available, Security Analytics displays `Select Version`. Click `Select Version` and select a version from the drop-down list.

Column	Description
Status	For each host, displays availability of updates and the progress of the update after you initiate it. Refer to **Updating a Host Version** in The Basics for an illustration of the Host view with its update statuses. • Update Available - One or more updates are available, but not applied. • **Update Path Not Supported** - If you have a non-Security Analytics Server host running a version that is earlier than the 10.6.0 update path (for example 10.4.0) and you updated your Security Analytics Server Host to 10.6.0, the non-Security Analytics Server host will display “Update Path Not Supported” in the Status column of the Hosts view and you cannot update it from this view. To update the non-Security Analytics Server host on the unsupported path: 1. Make sure that your Local Update Repository has the minimum supported version (for example 10.4.1.0) rpm zip file (See **Populate Local Update Repository** in the *Security Analytics10.6.0.0 Update Instructions*). 2. SSH to the non-Security Analytics Server host and edit the `/etc/yum/vars/sarelease` file to the version that it intended to update such as ’10.6.0.0’. (baseurl = http/smcupdate.netwitness.com/rsa/updates.10.4.1). 3. Run `yum clean all` Before run `yum update`, verify that it can be updated to that version. 4. Run `yum update` • **Host Version cannot be determined** - Contact Customer Care. • **In Queue for Update** - If you select multiple hosts to update (displays **In Queue for Update** - while it applies the version to each host • **Downloading *n* of *n*** - Tracks progress of the update download by file. • **Running Pre-Update Checks** - checking your your current version configuration to ensure that it has not conflicts. • Update warning. View details - found an issue in your existing configuration that does not prevent you from updating to the new version. Click View details to display the warning message dialog. • Update conflict. View details - found a conflict in your current version that that blocks the update. Click View details to display the conflict message dialog.

Column	Description
	You must resolve this conflict to proceed with the update. See Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors for instructions on how to resolve configuration conflicts. • Download error. View details - could not download version update file from your Local Update Repository. See **Populate Local Update Repository** in the *System Maintenance* guide. • **Initiating Update** - Initiating the update. • **Updating *n* of *n* packages** - Tracks progress of update package by package. • Update error. View details - Encountered an error during the update. Click View details to display the error message dialog. You must resolve this conflict to proceed with the update. See Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors for instructions on how to resolve update errors. • **Reboot Host** - Click **Reboot Host** in the toolbar to reboot the host for updates to take effect.

Groups Panel

The Groups panel provides a way to create logical groups of hosts. Once hosts are grouped, it is easier to perform operations on multiple hosts by interacting with each host in a group rather than individual hosts from an ungrouped list.

> **Note:** In Security Analytics Live, groups can subscribe to resources while individual hosts can not.

The Groups panel consists of a grid populated with a list of defined host groups and the Groups Panel Toolbar.

Column	Description
Name	The name of the host group. Click the group name in the Groups panel to list the hosts in that group on the Hosts panel.
<Blank>	Indicates the number of hosts in the group. Click the number of hosts in the group on Groups panel to list the hosts in that group on the Hosts panel.

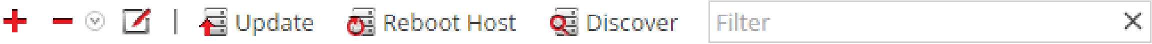
Topics

- Hosts Panel Toolbar
- Groups Panel Toolbar

Hosts Panel Toolbar

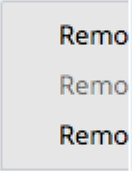
The Host view toolbar contains the tools that you use to maintain the hosts in your Security Analytics deployment.

Select **Administration > Hosts** in the **Security Analytics** menu to access the Hosts view. The Hosts panel toolbar is at the top of the Hosts grid in the Hosts view.



Features

The following table describes the features of the Hosts panel toolbar.

Feature	Description
+	Open the Add Host dialog in which you add a host (see [Step 1. Add or Update a Host](#)). The features of this dialog are: **Name** - The name that you give to the host. **Hostname** - The hostname or IP address of the physical or virtual machine for the host. **Cancel** - Closes the dialog without adding the host. **Save** - Adds the host.
− ⊙ 	Display the following options: • **Remove Host**: Removes a host that is no longer needed from the Security Analytics user interface along with its associated services. If you select this option, you can no longer view the host and its associated services from within Security Analytics. • **Remove From Group**: If the host is part of a host group, you can remove the host from the group. • **Remove and Repurpose Host**: This option is only available on the Primary Application host. Use this option when you want to completely rebuild a host.

Feature	Description
✎	Open the Edit Host dialog in which you edits a host or service identification and basic communication settings. This dialog has the same features as the Add Host dialog. Related procedures: • Step 1. Add or Update a Host • Change the Name and Hostname of a Host. • See the **Change IP Address or Hostname of a Host** topic in the *System Maintenance* guide
Update	Start the update process.
Reboot Host	Restart the host.
Discover	Most of the time, the Discover function completes automatically and it is not necessary to click the Discover button. For a fresh installation, click Discover to access the Provision dialog box so you can complete the provisioning phase. After the provisioning phase, Security Analytics the discovery of services running on the host happens automatically and it is not necessary to click this button.
Filter	Filter hosts by Name or Host.

Groups Panel Toolbar

The Groups panel toolbar provides options for managing groups of hosts. Use the toolbar to create, edit, and delete groups. After you create a group, you can drag individual hosts from the Hosts panel into that group.

Use groups may to organize hosts by function, geography, project, or any other organization principle that is useful. A host may belong to more than one group.

Select **Administration > Hosts** in the **Security Analytics** menu to access the Hosts view. The Groups panel toolbar is at the top of the Groups grid in the Hosts view.

Features

This table describes toolbar features.

Option	Description
+	Displays a new row in the Group grid in which you enter the name of a new group.
−	Asks for confirmation that you want to delete the group or host. You can confirm or cancel the deletion.
✎	Opens the name field in a row of the Group grid so that you can type a new name for an existing group.

Services View

You administer the services and services groups that are available to RSA Security Analytics modules in the Services view. You can run one or more services on a host. Each service maps to a host and performs various ongoing tasks.

You can administer the following Security Analytics services:

- Archiver
- Broker
- Concentrator
- Context Hub
- Decoder
- Event Stream Analysis
- Incident Management
- IPDB Extractor
- Log Collector
- Log Decoder
- Malware Analysis
- Reporting Engine
- Warehouse Connector
- Workbench

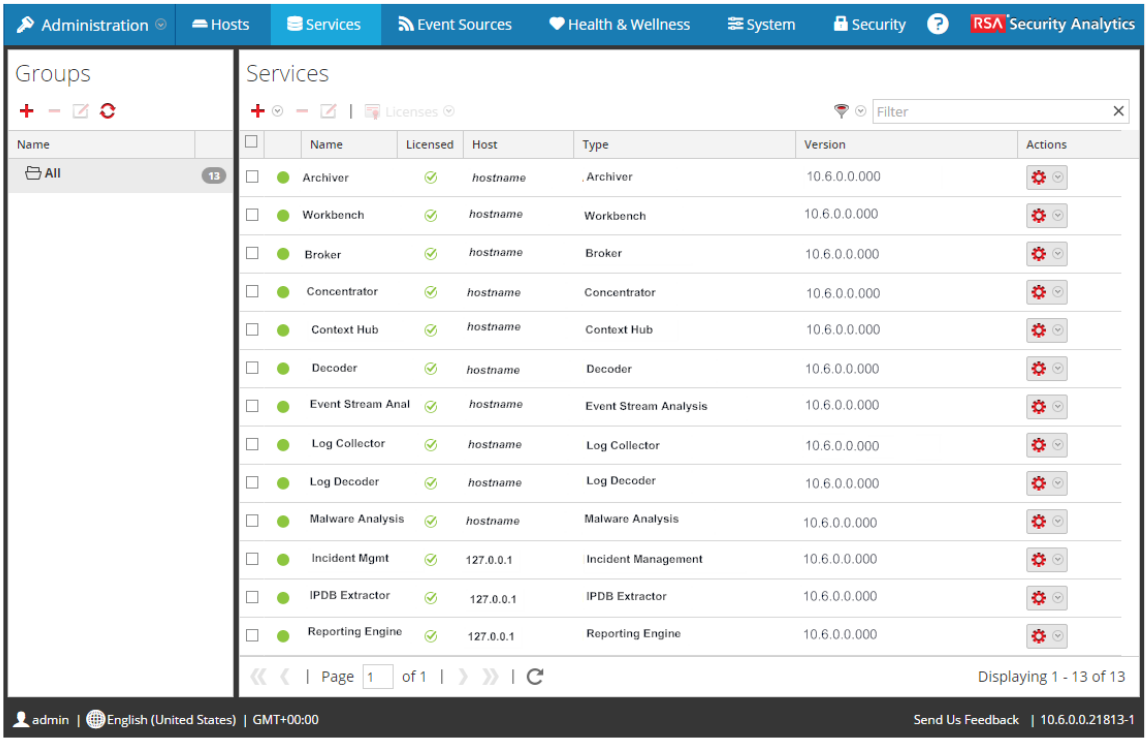
In the Services view, you can:

- Quickly search for and locate a specific service or type of service, such as Log Decoder or Warehouse Connector
- Use shortcuts to get to administration tasks
- Add, edit, and remove services
- Manage licensing and view the license status of a service (licensed or unlicensed)
- Sort Services by Name and Host

- Filter services by Type and by Name and Host
- Start, stop, and restart services

You can access the host where a service is running by clicking the link in the Host column for that service.

To access the Administration Services view, from any Security Analytics module, in the **Security Analytics** menu, select **Administration** > **Services**.



Name	Licensed	Host	Type	Version
Archiver	✓	hostname	Archiver	10.6.0.0.000
Workbench	✓	hostname	Workbench	10.6.0.0.000
Broker	✓	hostname	Broker	10.6.0.0.000
Concentrator	✓	hostname	Concentrator	10.6.0.0.000
Context Hub	✓	hostname	Context Hub	10.6.0.0.000
Decoder	✓	hostname	Decoder	10.6.0.0.000
Event Stream Anal	✓	hostname	Event Stream Analysis	10.6.0.0.000
Log Collector	✓	hostname	Log Collector	10.6.0.0.000
Log Decoder	✓	hostname	Log Decoder	10.6.0.0.000
Malware Analysis	✓	hostname	Malware Analysis	10.6.0.0.000
Incident Mgmt	✓	127.0.0.1	Incident Management	10.6.0.0.000
IPDB Extractor	✓	127.0.0.1	IPDB Extractor	10.6.0.0.000
Reporting Engine	✓	127.0.0.1	Reporting Engine	10.6.0.0.000

You can also view the services from the Default Dashboard in the Available Services section.

Procedures related to services are described in Step 2. Add a Service to a Host, Step 4. Manage Access to a Service, and Service Procedures.

Features

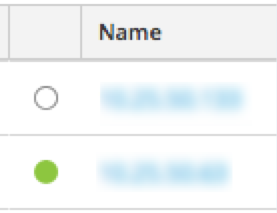
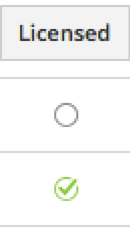
The Services View has two panels:

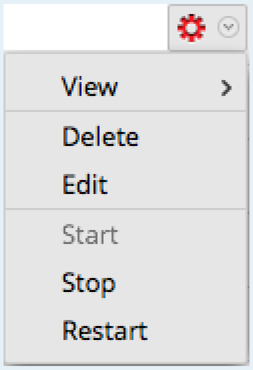
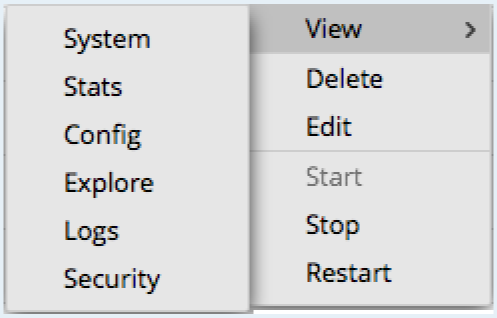
- Services panel
- Groups panel

Services Panel

In the Services panel, you can access different views into a service, and perform service operations such as adding, removing, editing, and administering. The Services panel consists of a grid populated with the list of defined Security Analytics services and the Services Panel Toolbar.

This table describes the columns in the grid.

Column	Description
□	Selects a row for an action in the toolbar. Clicking the checkbox in the column title selects or deselects all rows in the grid.
<Blank>	Indicates whether the service is started (capturing or aggregating data) or stopped. A solid colored green circle indicates that a connected service is started. A blank white circle indicates that a connected service is stopped. 
Name	The name of the service.
Licensed	Indicates whether the service is licensed. A checked circle is licensed and an empty circle is not licensed. 
Host	The name of the host where the service is located.
Type	The type of service. Currently service types are Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Incident Management, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, and Workbench.

Column	Description
Version	The version of software of the service.
Actions	Provides an Actions menu ⚙ for the selected service with actions that can be taken on the service and the associated host. The Actions menu enables you to delete the service, edit the service, and start, stop, and restart the service. A dialog requests confirmation before restarting.  The View submenu from the Actions menu enables you to access the System, Stats, Config, Explore, Logs, and Security views for the selected service.  System Stats Config Explore Logs Security View Delete Edit Start Stop Restart

Groups Panel

The Groups panel provides a way to create logical groups of services. Once services are grouped, it is easier to perform operations on multiple services by interacting with each service in a group rather than individual services from an ungrouped list. In Security Analytics Live, groups can subscribe to resources while individual services can not.

The Groups panel consists of a grid populated with a list of defined services groups and the Groups Panel Toolbar. This table describes the columns in the grid.

Column	Description
Name	The name of the services group. Clicking the group name in the Groups panel lists the services in that group on the Services panel.
<Blank>	Indicates the number of services in the group. Clicking the number of services in the group on Groups panel lists the services in that group on the Services panel.

Topics

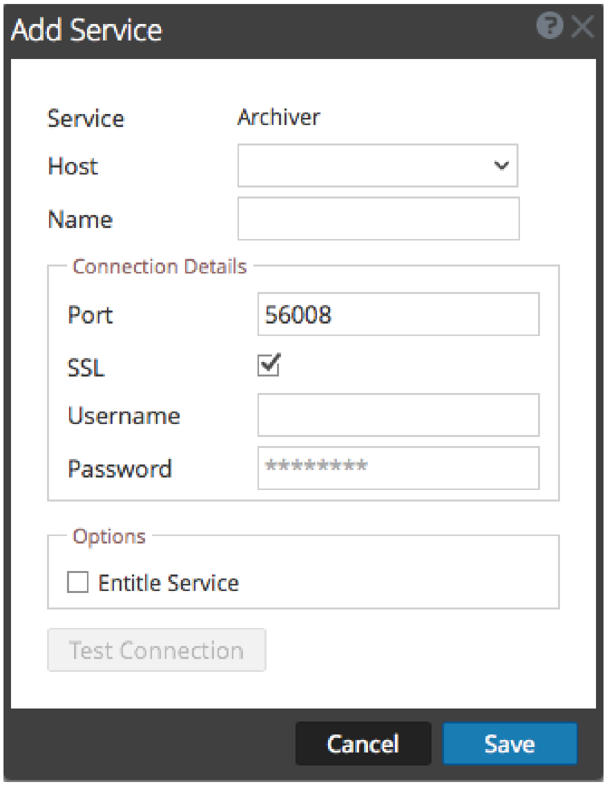
- Add Service or Edit Service Dialog
- Groups Panel Toolbar
- Services Panel Toolbar

Add Service or Edit Service Dialog

This topic introduces the Add Service or Edit Service dialogs accessible from the Administration Services view (Administration > Services).

Security Analytics services are automatically discovered in RSA Security Analytics. You can manually add a service using the Add Service dialog to make services available to Security Analytics modules.

To access the Add Service dialog, navigate to the **Administration Services** view, and select **Add** (+) in the **Services panel** toolbar.



Add Service

Service: Archiver

Host:

Name:

Connection Details

Port: 56008

SSL: ☑

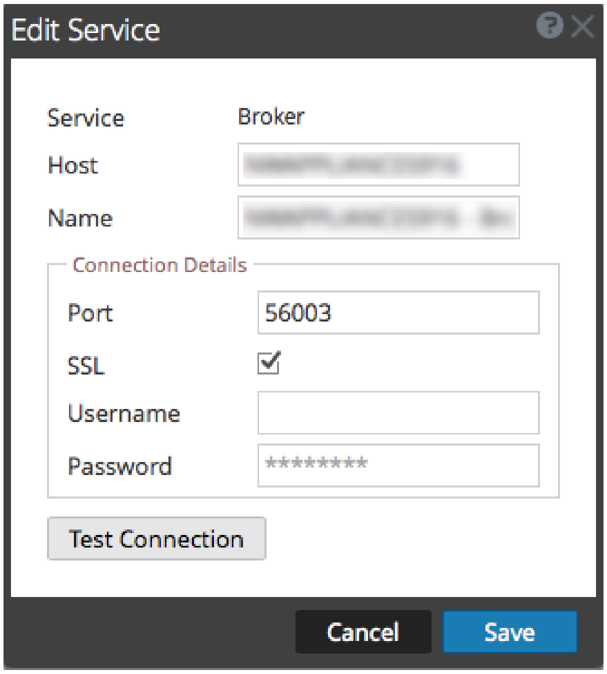
Username:

Password: *********

Options

☐ Entitle Service

You can use the Edit Service dialog to modify services. The Edit Service dialog is similar to the Add Service dialog. To access the Edit Service dialog, navigate to the **Administration Services** view, and select **Edit** (✎) in the **Services panel** toolbar.



Edit Service

Service Broker

Host [redacted]

Name [redacted]

Connection Details

Port 56003

SSL ☑

Username

Password *********

Procedures related to services are described in Step 2. Add a Service to a Host, Step 4. Manage Access to a Service, and Service Procedures.

Features

This table describes the features of the Add Service or Edit Service dialogs.

Field or Option	Description
Service	Displays the service type. You can add the following services: Archiver, Broker, Concentrator, Decoder, Event Stream Analysis, Incident Management, IPDB Extractor, Log Collector, Log Decoder, Malware Analysis, Reporting Engine, Warehouse Connector, and Workbench.
Host	Specifies the host on which the service resides.
Name	Specifies the name used to identify the service; for example, **HQ Broker** or **Broker-10.10.201.99**. An understandable naming convention can make administrative tasks easier. Some administrators find it convenient to use the hostname or IP address (specified in the **Host** field) for the **Name** as well.

Field or Option	Description
Port	Specifies the port used to communicate with this service. The default port based on the selected service type in the **Service** field is autofilled here. If you select **SSL** below, this port becomes an SSL port. If you do not select **SSL**, it becomes a non-SSL port. You can customize this port by opening a firewall for the port that you add. For information on ports, see the **Network Architecture and Ports** topic in the *Deployment Guide*.
SSL	Indicates that Security Analytics uses SSL for communications with this service.
Username	Specifies the user name used to log in to this service. The default username is **admin**.
Password	Specifies the password used to log in to this service. The default password is **netwitness**.
Entitle Service	(Optional) Assigns licenses from the local license server (LLS) to selected services. For more information, see the **View Current Entitlements** topic in the *Licensing Guide*.
Test Connection	Clicking this button tests the connection of a service that you are adding.
Save	Clicking this button saves the new service.
Cancel	Clicking this button closes the Add Service or Edit Service dialog. If you do not save the service before closing the dialog, the service is not added or edited.

Groups Panel Toolbar

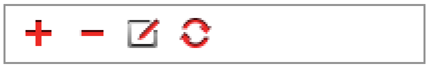
This topic introduces the features and options in Administration Services view > Groups panel toolbar.

The Groups panel toolbar provides options for managing groups of services. The toolbar includes options for creating, editing, and deleting groups. Once groups are created, you can drag individual services from the Services panel into a group.

Groups may reflect functional, geographical, project-oriented, or any other organization principle that is useful. A service may belong to more than one group.

To access the Services view, in the **Security Analytics** menu, select **Administration > Services.** The Groups panel toolbar is at the top of the Groups grid in the Services view.

Features



This table describes toolbar features.

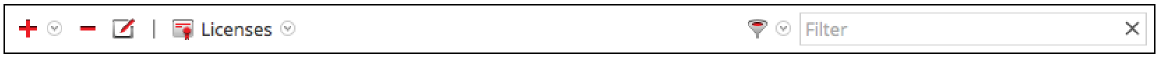
Option	Description
+	Displays a new row in the Group grid in which you enter the name of a new group.
−	Asks for confirmation that you want to delete the group or service. You can confirm or cancel the deletion.
✎	Opens the name field in a row of the Group grid so that you can type a new name for an existing group.
⟳	Refreshes the selected group.

Services Panel Toolbar

This topic introduces the options in Service panel toolbar for adding, removing, editing, and licensing services. You can also filter the services listed in the Services Panel.

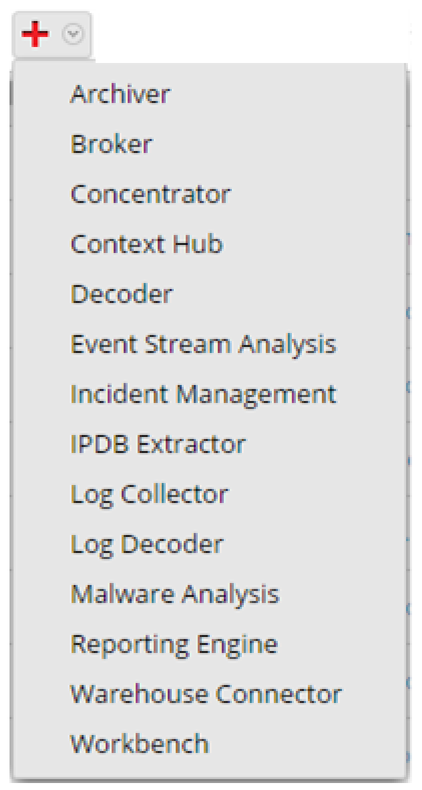
The Services panel toolbar has options for adding, removing, editing, and licensing services. You can filter the listed services based on and one or more service types, service name, and host.

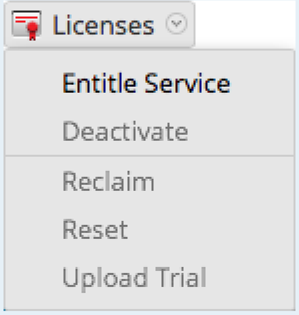
To access the Administration Services view, in the **Security Analytics** menu, select **Administration** > **Services.** The Services panel toolbar is at the top of the Services grid in the Services view.

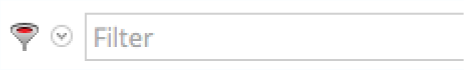
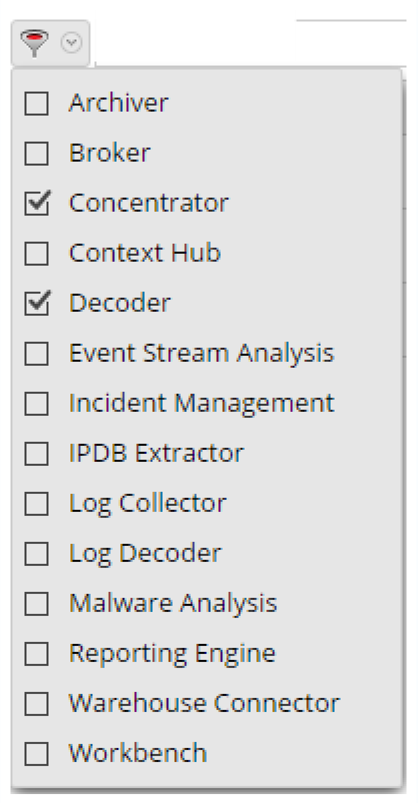


Features

The table describes the features of the Services panel toolbar.

Feature	Description
 Archiver Broker Concentrator Context Hub Decoder Event Stream Analysis Incident Management IPDB Extractor Log Collector Log Decoder Malware Analysis Reporting Engine Warehouse Connector Workbench	Adds a service for this instance of RSA Security Analytics to manage (see Step 2. Add a Service to a Host).

Feature	Description
➖	Deletes a service from this instance of Security Analytics (see Edit or Delete a Service).
✎	Edits service identification and basic communication settings (see Edit or Delete a Service).
 Licenses Entitle Service Deactivate Reclaim Reset Upload Trial	- Entitle Service: Assigns licenses from the local license server (LLS) to selected services (see the **Overview Tab** topic in the *Licensing Guide*). - Deactivate: Not used in Security Analytics 10.6. - Reclaim: Reclaims a deactivated license from LLS for the selected service. - Reset: Not used in Security Analytics 10.6. - Upload Trial: Not used in Security Analytics 10.6.

Feature	Description
  ☐ Archiver ☐ Broker ☑ Concentrator ☐ Context Hub ☑ Decoder ☐ Event Stream Analysis ☐ Incident Management ☐ IPDB Extractor ☐ Log Collector ☐ Log Decoder ☐ Malware Analysis ☐ Reporting Engine ☐ Warehouse Connector ☐ Workbench	Filters the services listed in Services view. In the Filter drop-down menu, you can filter the services by one or more selected service types. In this example, when you select Concentrator and Decoder, only the Concentrator and Decoder services appear in the Services view. In the Filter field, you can filter the services by Name and Host. You can use the Filter drop-down menu and the Filter field at the same time to filter the services listed in the Services view.

Services Config View

This topic introduces the features and functions of the Services Config view.

The Services Config view is one of the views available from the Services View > Actions ( ) menu. It provides a user interface for configuring all aspects of a Core service or Security Analytics service.

The configuration options in the Services Config view are organized as tabs, with each tab providing a view of a set of related parameters. Unlike the Services Explore view, which offers direct access to all configuration files for a service, these tabs present the most commonly modified parameters of service configuration in a user-friendly view.

Due to configuration requirements for different services; each type of service has variations in available tabs and configuration parameters in this view. Individual topics describe configuration parameters that are specific to a host (Brokers and Concentrators, Decoders and Log Decoders) or service (for example, Reporting Engine, IPDB Extractor, Log Collector, and Warehouse Connector).

To access the Services Config view:

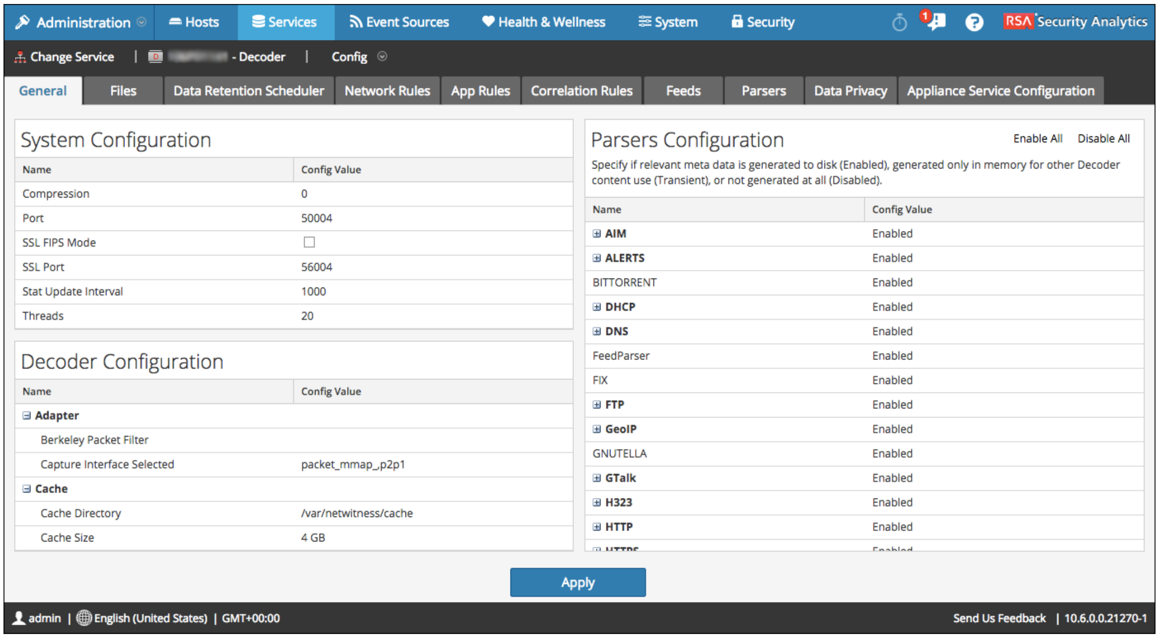
1. In the **Security Analytics** menu, select **Administration > Services**.

   The Administration Services view is displayed.

2. Select a service and select **>View > Config**.

   Services Config view for the selected service is displayed.

This is an example of the Services Config view for a Decoder.



System Configuration

Name	Config Value
Compression	0
Port	50004
SSL FIPS Mode	□
SSL Port	56004
Stat Update Interval	1000
Threads	20

Decoder Configuration

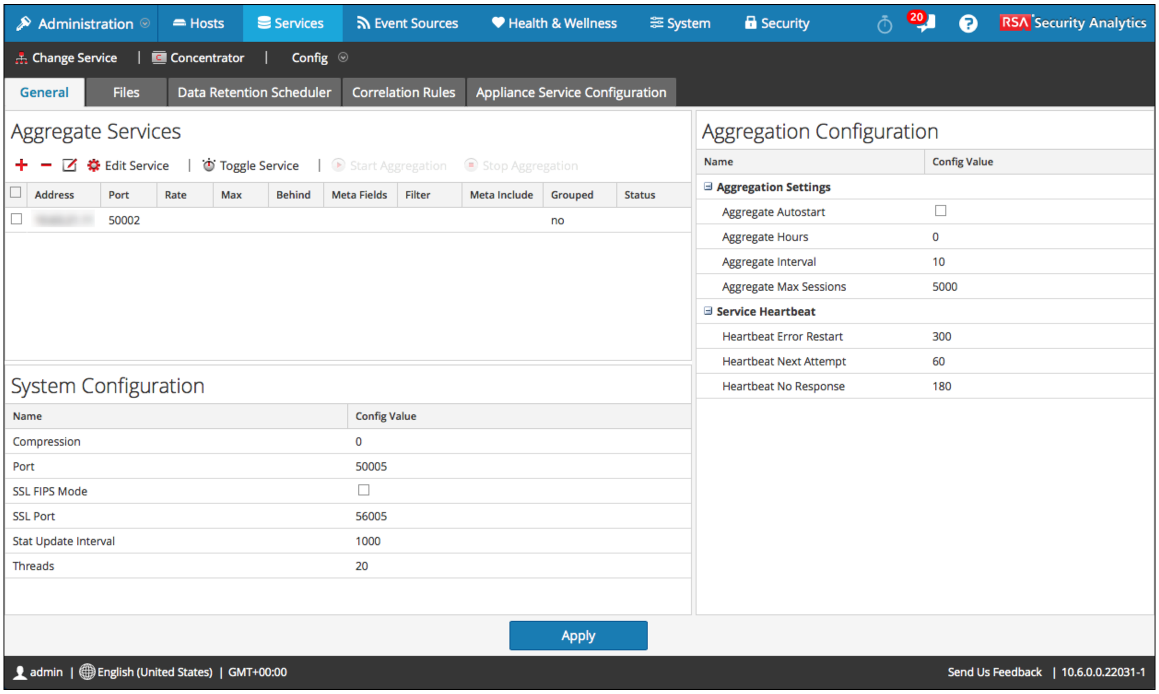
Name	Config Value
⊟ **Adapter**	
Berkeley Packet Filter	
Capture Interface Selected	packet_mmap_,p2p1
⊟ **Cache**	
Cache Directory	/var/netwitness/cache
Cache Size	4 GB

Parsers Configuration

Specify if relevant meta data is generated to disk (Enabled), generated only in memory for other Decoder content use (Transient), or not generated at all (Disabled).

Name	Config Value
⊞ **AIM**	Enabled
⊞ **ALERTS**	Enabled
BITTORRENT	Enabled
⊞ **DHCP**	Enabled
⊞ **DNS**	Enabled
FeedParser	Enabled
FIX	Enabled
⊞ **FTP**	Enabled
⊞ **GeoIP**	Enabled
GNUTELLA	Enabled
⊞ **GTalk**	Enabled
⊞ **H323**	Enabled
⊞ **HTTP**	Enabled

This is an example of the Services Config view for a Concentrator.



Aggregate Services

□	Address	Port	Rate	Max	Behind	Meta Fields	Filter	Meta Include	Grouped	Status
□	[redacted]	50002							no	

System Configuration

Name	Config Value
Compression	0
Port	50005
SSL FIPS Mode	□
SSL Port	56005
Stat Update Interval	1000
Threads	20

Aggregation Configuration

Name	Config Value
⊟ Aggregation Settings	
Aggregate Autostart	□
Aggregate Hours	0
Aggregate Interval	10
Aggregate Max Sessions	5000
⊟ Service Heartbeat	
Heartbeat Error Restart	300
Heartbeat Next Attempt	60
Heartbeat No Response	180

Topics

- Services Config View - Appliance Service Configuration Tab
- Data Retention Scheduler Tab
- Files Tab

Services Config View - Appliance Service Configuration Tab

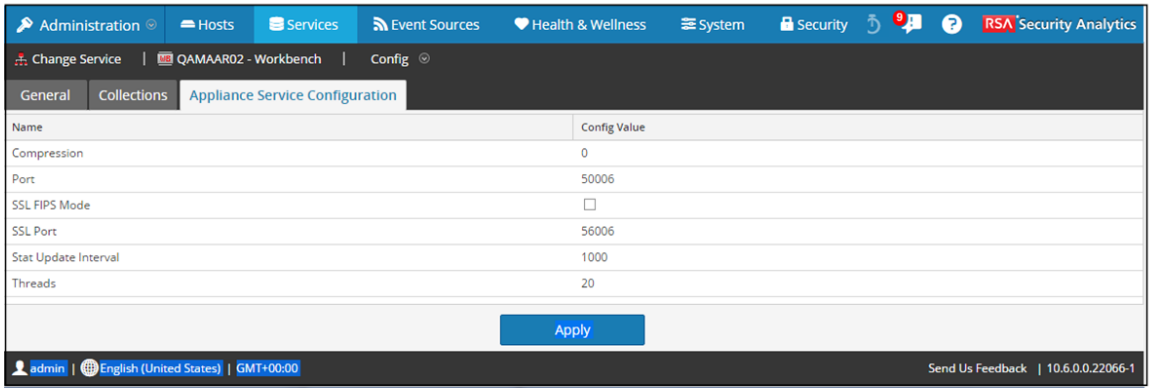
This topic provides a description of the Services Config view > Appliance Service Configuration tab for Security Analytics Workbench.

The Appliance Service Configuration tab for Workbench service allows you to view, add, and remove services. When you have made changes to the configured services, clicking Apply puts the configuration into effect immediately.

To access this view:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. Select a service, and select > **View > Config**.

   The Services Config view is displayed with the Appliance Service Configuration tab open.
3. Select the **Appliance Service Configuration** tab.



Name	Config Value
Compression	0
Port	50006
SSL FIPS Mode	☐
SSL Port	56006
Stat Update Interval	1000
Threads	20

Features

The Appliance Service Configuration tab has a grid that lists relevant information about the workbench configurations.

Grid

The following table describes the features of the grid

Parameter	Description
Compression	When set to a positive value, the minimum amount of bytes before a message is compressed. 0 means no compression for any message. Change takes effect on subsequent connections.
Port	The unencrypted port this service will listen on. 0 means disabled. Change takes effect on service restart.
SSL FIPS Mode	Determines whether the OpenSSL library will enter FIPS mode. Change takes effect on service restart.
SSL Port	The SSL port this service will listen on. 0 means disabled. Change takes effect on service restart.
Stat Update Interval	Determines how often (in milliseconds) statistic nodes are updated in the system. Change takes effect immediately.
Threads	Determines the number of threads in the thread pool to handle incoming requests. Change takes effect immediately.
Config Value	Determines the configuration value of the service. Change takes effect immediately.
Apply	Updates the modified configurations in the grid.

Data Retention Scheduler Tab

This topic describes the configurable options in the Data Retention Scheduler tab for Decoder, Log Decoder, and Concentrator.

In the Data Retention Scheduler tab, you can define the criteria for removing database records from primary storage on Decoder, Log Decoder, and Concentrator services, and schedule the timing for checking the threshold.

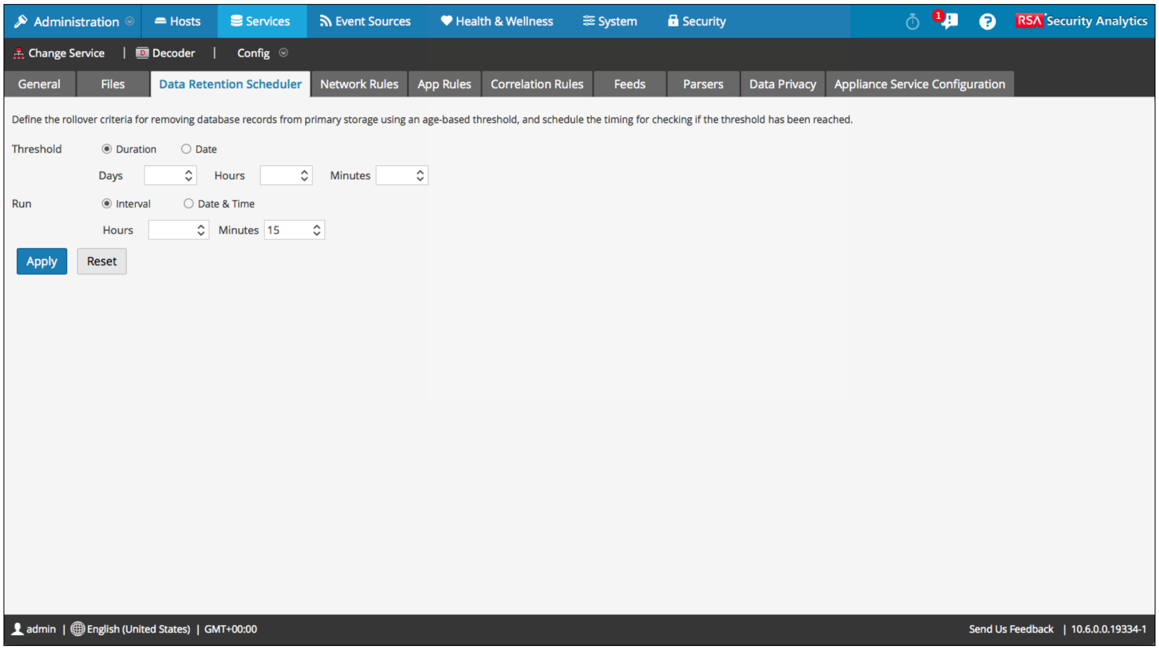
For information on the Data Retention tab for Archiver, see the **Data Retention Tab - Archiver** topic in the *Archiver Configuration Guide*.

> **Note:** If additional customization is necessary, it can be done using the Scheduler under the Files tab in the Services Config view. For example, if more storage is available to save the RAW data versus the meta, it may make more sense to use Capacity as the threshold and to set different thresholds per database (meta versus packet).

To access the Data Retention Scheduler tab:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. Select a Decoder, Log Decoder, or Concentrator, and then select ⚙ > **View** > **Config**.
3. In the **Services Config** view for the service, click the **Data Retention Scheduler** tab.

The following figure illustrates the parameters in the Data Retention Scheduler tab for a Decoder.



Define the rollover criteria for removing database records from primary storage using an age-based threshold, and schedule the timing for checking if the threshold has been reached.

Threshold ● Duration ○ Date

Days ___ Hours ___ Minutes ___

Run ● Interval ○ Date & Time

Hours ___ Minutes 15

Features

The Data Retention Scheduler tab has sections to specify Threshold settings and Run settings. The following table lists the parameters supported for data retention configuration.

Parameter	Description
Threshold	The threshold is based on the age of the data, the amount of time the data has been stored or the date on which the data was stored. The date is from the database file, not from the actual session time. • **Duration**: The duration of time that data can be stored before removal. Specifies the number of days (365 maximum), hours (24 maximum), and minutes (60 maximum) that have elapsed since the time stamp on the data. • **Date**: The removal of data based on the date of the timestamp. Specifies the monthly date and time in the **Calendar** and **Time** fields.
Run	The schedule for running the job that checks rollover criteria. • **Interval**: Schedule the database check to occur at a regular interval. Specifies the **Hours** and **Minutes** between the scheduled checks. • **Date and Time**: Schedule the database check to occur at a regular day and time. Specifies the day from the drop-down list and the system clock time in `hh:mm:ss` format. Possible values for day are **Everyday**, **Weekdays**, **Weekends**, and **Custom**, where **Custom** allows you to select one or more specific days of the week.
Apply	Overwrites any previous schedule for this service and applies the new settings immediately. **Caution:** Once these settings have been applied and the threshold is met, the old data will be deleted from the database and no longer accessible.
Reset	Resets the schedule to the last applied state.

Files Tab

This topic describes the service configuration files that are visible in the Services Config view > Files tab.

The Files tab in the Services Config view is the user interface for editing service configuration files—Decoders, Log Decoders, Brokers, Archivers, and Concentrators—as text files.

The files available to edit vary depending upon the type of service being configured. The files that are common to all Core services are:

- The service index file.
- The netwitness file.
- The crash reporter file.
- The scheduler file.
- The feed definitions file.

In addition, the Decoder has files that configure parsers, feed definitions, and a wireless LAN adapter.

Note: The default values in these configuration files are generally good for the most common situations; however, some editing is necessary for optional services, such as the crash reporter or scheduler. Only administrators with a good understanding of the networks and the factors that affect the way services collect and parse data should make changes to these files in the Files Tab.

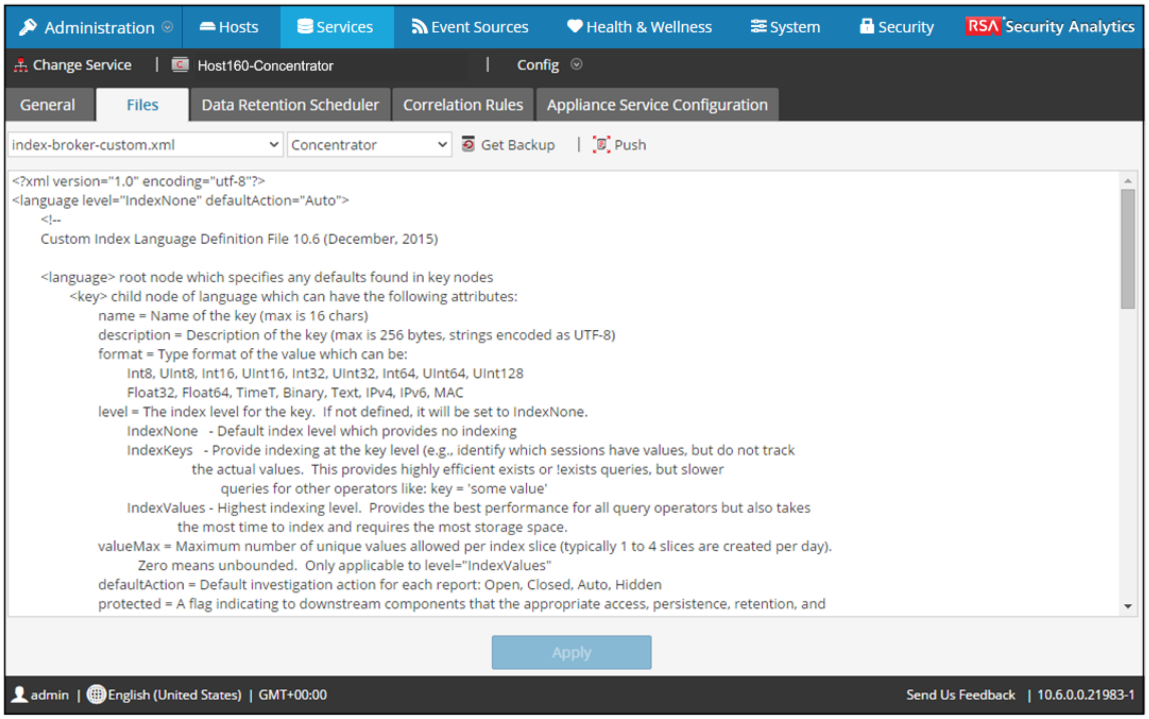
More detail on the service configuration parameters is available in the Service Configuration Settings.

To access the Files tab:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. Select a service and select ⚙ > **View** > **Config**.

   The Services Config view is displayed with the **General** tab open.
3. Click the **Files** tab.

This is an example of the Files tab.

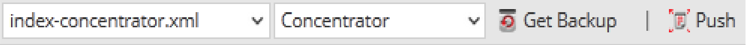


```
<?xml version="1.0" encoding="utf-8"?>
<language level="IndexNone" defaultAction="Auto">
    <!--
    Custom Index Language Definition File 10.6 (December, 2015)

    <language> root node which specifies any defaults found in key nodes
        <key> child node of language which can have the following attributes:
            name = Name of the key (max is 16 chars)
            description = Description of the key (max is 256 bytes, strings encoded as UTF-8)
            format = Type format of the value which can be:
                Int8, UInt8, Int16, UInt16, Int32, UInt32, Int64, UInt64, UInt128
                Float32, Float64, TimeT, Binary, Text, IPv4, IPv6, MAC
            level = The index level for the key.  If not defined, it will be set to IndexNone.
                IndexNone   - Default index level which provides no indexing
                IndexKeys   - Provide indexing at the key level (e.g., identify which sessions have values, but do not track
                          the actual values.  This provides highly efficient exists or !exists queries, but slower
                              queries for other operators like: key = 'some value'
                IndexValues - Highest indexing level.  Provides the best performance for all query operators but also takes
                        the most time to index and requires the most storage space.
            valueMax = Maximum number of unique values allowed per index slice (typically 1 to 4 slices are created per day).
                 Zero means unbounded.  Only applicable to level="IndexValues"
            defaultAction = Default investigation action for each report: Open, Closed, Auto, Hidden
            protected = A flag indicating to downstream components that the appropriate access, persistence, retention, and
```

Files Tab Toolbar

The Files tab has a toolbar and an edit window. This is an example of the toolbar.



These are the features of the Files tab toolbar.

Feature	Description
File drop-down list	Displays a list of files that the system is currently using. When you select a file, the text of the file is displayed in the text edit window. In the text window, you can edit the file and save the changes, or create alternate files to use.
Service / Host drop-down list	Displays the service type and host. You can open a file from either the service or the host for editing.

Feature	Description
	Retrieves the latest backup of the current file, which can prove useful when you have made changes and want to go back to the previous version of the file. The backup does not replace the current file unless you click **Save**.
	Displays a dialog in which you can select services of the same type and push the currently viewed file to the services.
Apply	Overwrites the current file, creates a backup file.

Services Explore View

This topic introduces the features of Security Analytics Services Explore view, a powerful and flexible user interface for viewing and editing host and service configurations.

The Services Explore View offers advanced access and control of all Security Analytics hosts and services. All services expose their functionality through a tree -like series of nodes, similar to the Windows Explorer view of your file system. Here you can:

- View a directory tree showing common files for all selected services.
- Navigate down through the directory to a file.
- Open the same file for each service, and display the contents side by side.
- Select an entry in the file and edit the value.
- Apply a property value from one service to other services.

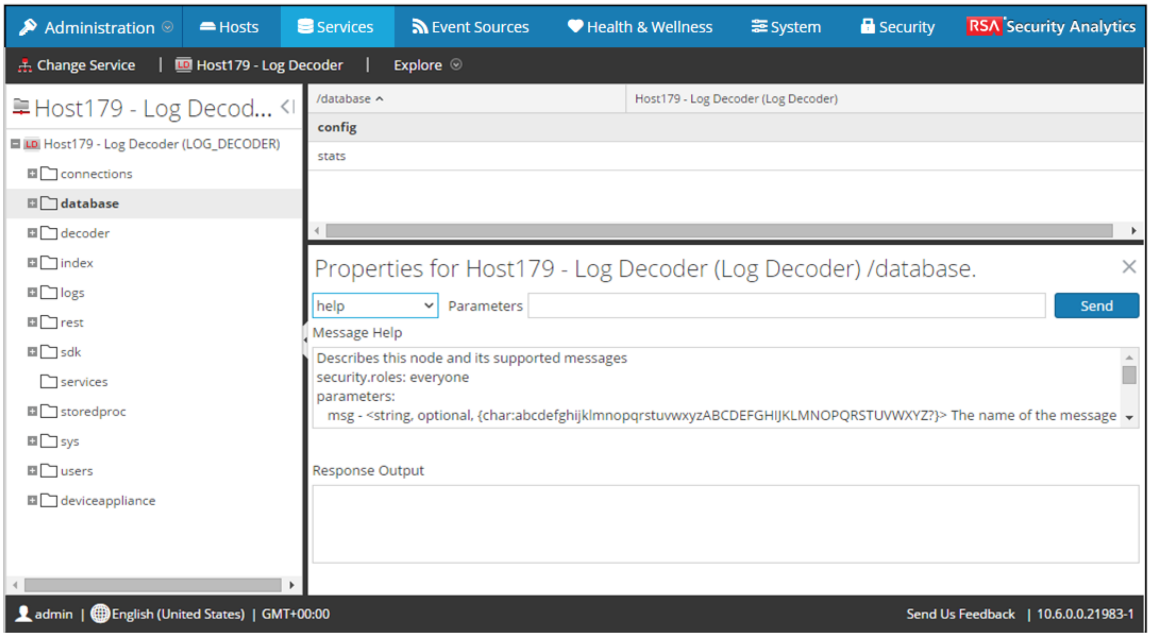
  The Services Explore View can also display a Properties dialog, a simple interface for viewing properties of any node in the system and sending messages to the node, shown in the figure below.

> **Caution:** A good understanding of the nodes and parameters is required when editing in this view. Incorrect settings can cause performance problems.

To access the Services Explore view:

1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. Select a service and select ⚙ > **View** > **Explore**.

This is an example of the Services Explore view.



```
Describes this node and its supported messages
security.roles: everyone
parameters:
  msg - <string, optional, {char:abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ?}> The name of the message
```

Features

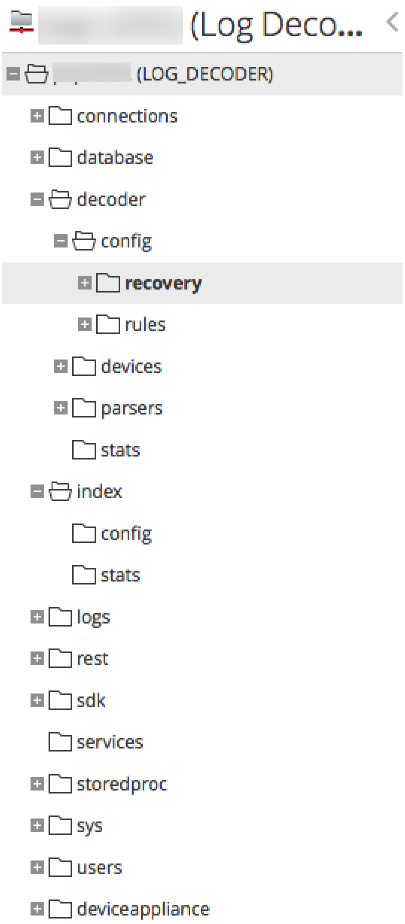
The **Services Explore View** has two main panels:

- The Node list
- The Monitor panel

You can access the Properties of any file by right-clicking the file and selecting Properties.

The Node List

The Node list displays the services as a tree-like series of nodes and folders. The levels in the Node list expand and collapse to display the full hierarchy.



Each root folder is named based on the functionality it exposes. For instance, the **/connections** folder shows all connected IP addresses. Underneath each **IP/Port** are two folders, **sessions** and **stats**.

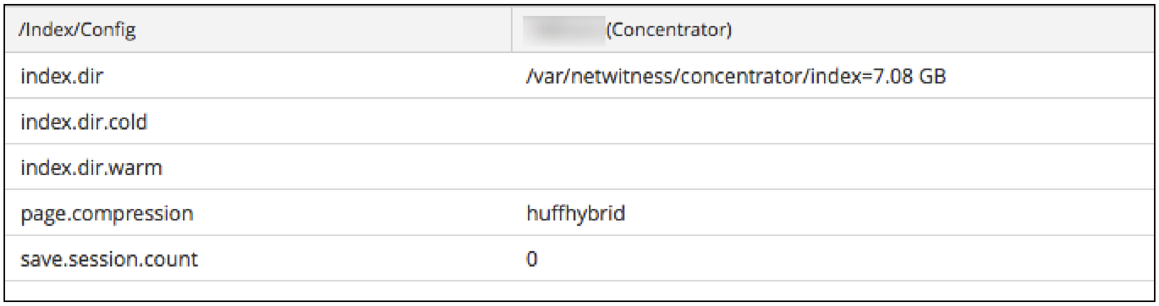
- The **sessions** folder displays all authenticated user sessions originating from the IP/Port.
- The **stats** folder displays values, such as the number of messages sent/received, bytes sent/received, and others, set by the service. These are not editable.

Selecting any folder in the tree view displays its children in the **Monitor** panel. Every node in the tree is actively monitored, so when a statistic or configuration node changes value, it is immediately reflected in the tree and monitor panel.

The Monitor Panel

The **Monitor** panel displays properties and values for a selected node (such as **index**) and a child folder (such as **config**). There are two ways to edit values:

- Clicking the value and typing a new value
- Sending a **set** message in the Properties dialog



/Index/Config	[redacted] (Concentrator)
index.dir	/var/netwitness/concentrator/index=7.08 GB
index.dir.cold	
index.dir.warm	
page.compression	huffhybrid
save.session.count	0

Topics

- Properties Dialog

Properties Dialog

This topic explains how to send messages to a system node in the Services Explore view > Properties dialog.

The Properties dialog opens below the Monitor panel when you select Properties from the context menu. The Properties dialog provides a user-friendly messaging tool for communication with system nodes. This is useful for getting and setting values for a property for multiple services.

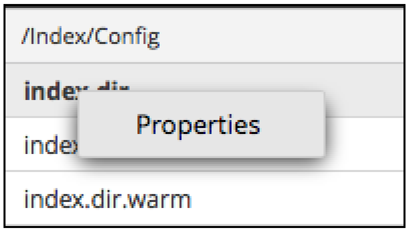
All nodes support the help message, which contains:

- A description of the node.
- The list of supported messages with a corresponding description.
- Security roles needed to access the messages.

The available messages vary according to the service and root folder. Many of these messages are also accessible as options with a Security Analytics dashboard or view.

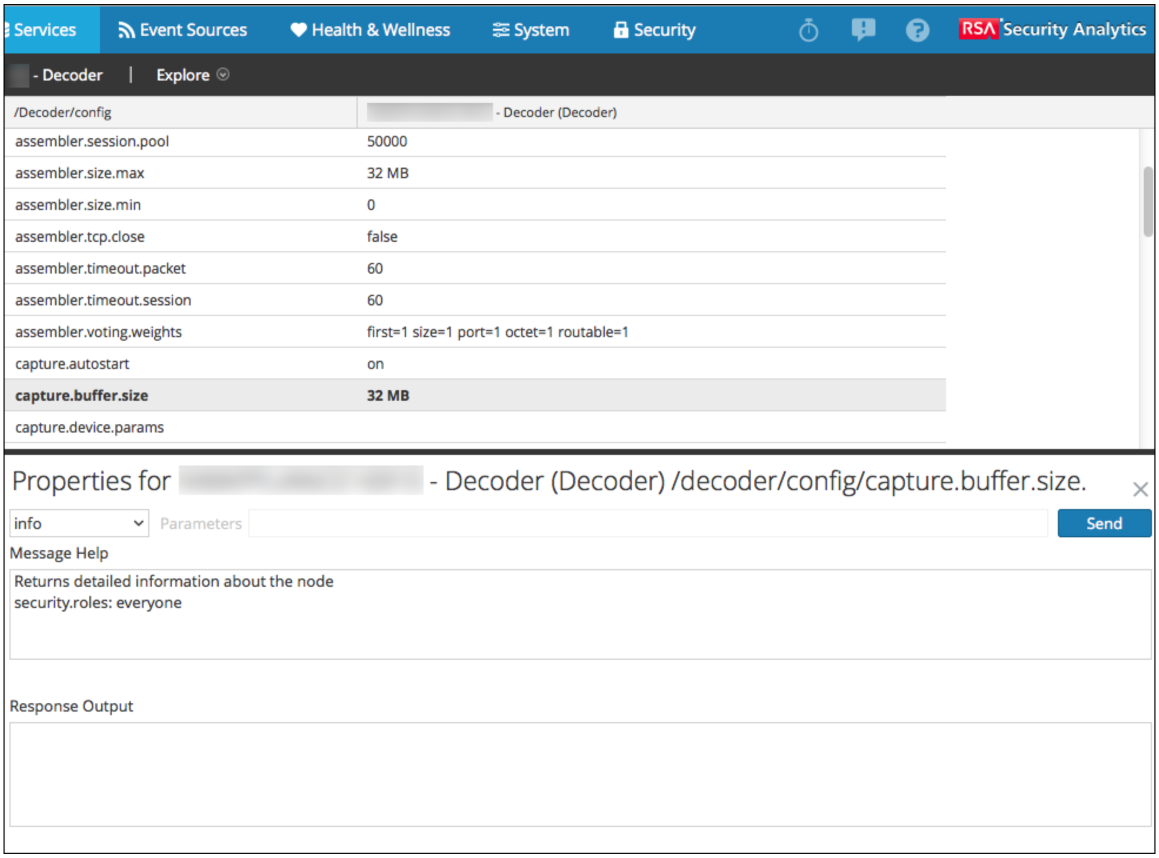
To access the Properties dialog:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. Select a service and select ⚙ ⌄ > **View > Explore**.
3. In the **Node** list, select a file.
4. In the **Monitor** panel, right-click a property and select **Properties**.

   The Properties dialog is displayed. You can also right-click any file in the Node list to display the Properties dialog.

The following example shows the Properties dialog with help for a message (**info**) displayed.



/Decoder/config	[redacted] - Decoder (Decoder)
assembler.session.pool	50000
assembler.size.max	32 MB
assembler.size.min	0
assembler.tcp.close	false
assembler.timeout.packet	60
assembler.timeout.session	60
assembler.voting.weights	first=1 size=1 port=1 octet=1 routable=1
capture.autostart	on
capture.buffer.size	**32 MB**
capture.device.params	

Properties for [redacted] - Decoder (Decoder) /decoder/config/capture.buffer.size.

Message Help

Returns detailed information about the node
security.roles: everyone

Response Output

Features

The Properties dialog has the following features.

Feature	Description
Message drop-down list	Lists all available messages for the current node. Select a message to send the node.
Parameters input field	Type the message parameters in this field.
Send button	Sends the message to the node.
Message Help	Displays help text for the current message.
Response Output	Displays the response to a message or output from a message.

Services Logs View

This topic introduces the Services Logs view.

The Services Logs view provides the ability to view and search the logs for a specific service. The Services Logs view is identical to the System Logging Panel with two exceptions:

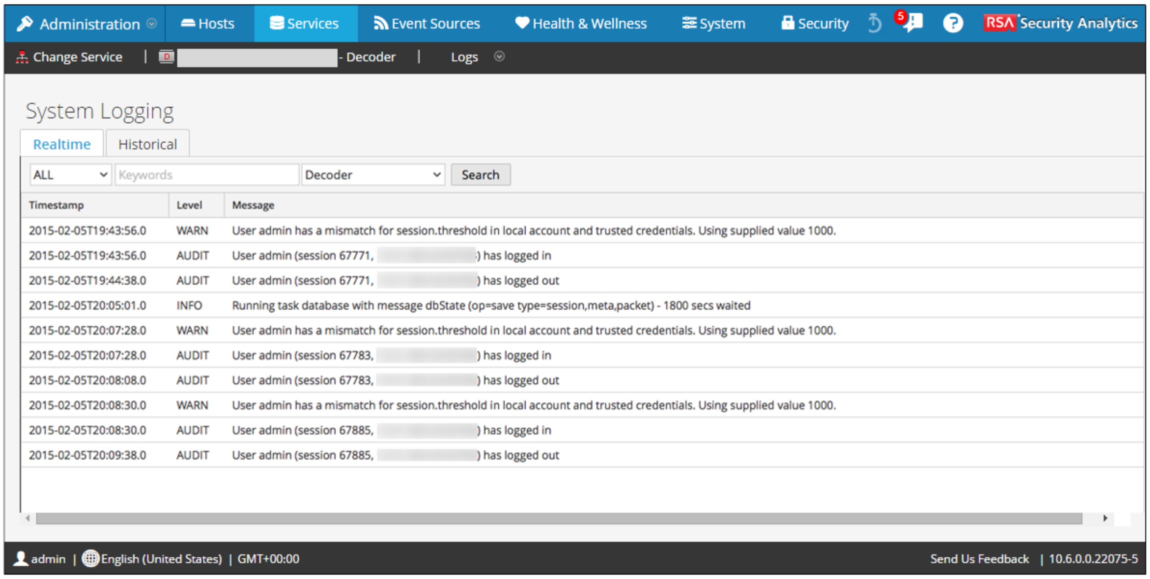
- The Services Logs view has an additional filter to select messages for the service or host.
- The System Logging panel has an additional tab for Settings.

Refer to System Logging Panel for a complete description of Security Analytics logging features.

To view a service log:

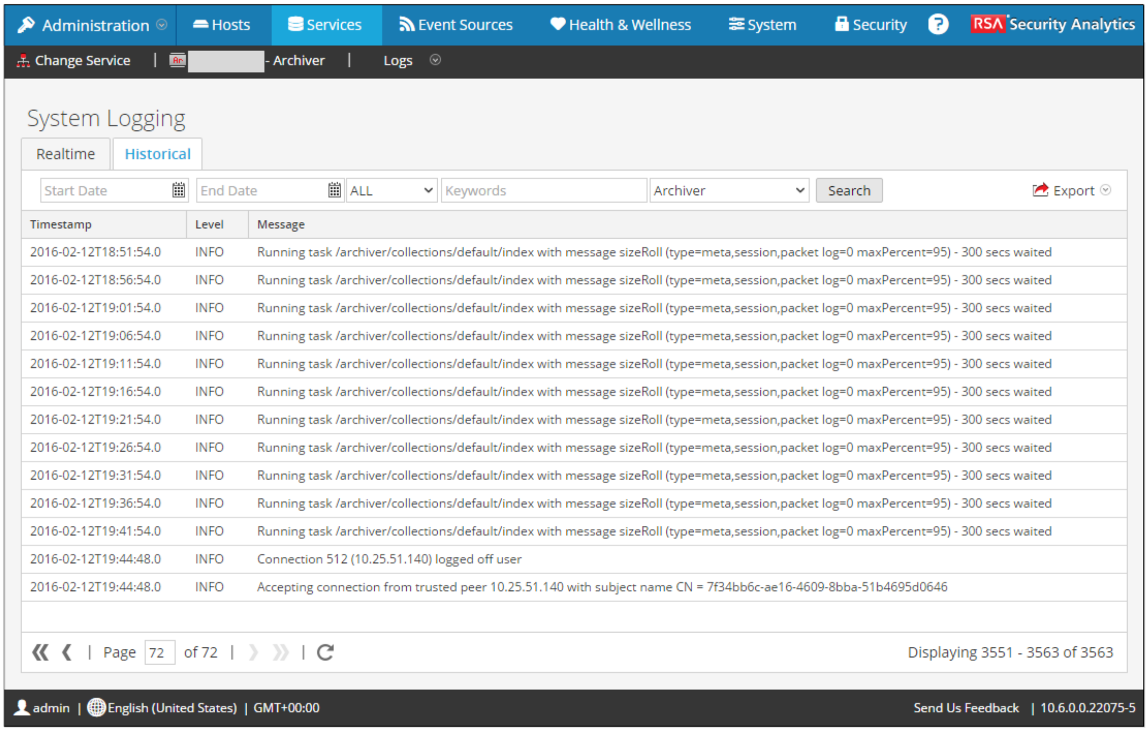
1. In the **Security Analytics** menu, select **Administration** > **Services**.
2. Select a service and select ⚙ ⌄ >**View** > **Logs**.

The following figure shows the Services Logs view Realtime tab.



Timestamp	Level	Message
2015-02-05T19:43:56.0	WARN	User admin has a mismatch for session.threshold in local account and trusted credentials. Using supplied value 1000.
2015-02-05T19:43:56.0	AUDIT	User admin (session 67771, [redacted]) has logged in
2015-02-05T19:44:38.0	AUDIT	User admin (session 67771, [redacted]) has logged out
2015-02-05T20:05:01.0	INFO	Running task database with message dbState (op=save type=session,meta,packet) - 1800 secs waited
2015-02-05T20:07:28.0	WARN	User admin has a mismatch for session.threshold in local account and trusted credentials. Using supplied value 1000.
2015-02-05T20:07:28.0	AUDIT	User admin (session 67783, [redacted]) has logged in
2015-02-05T20:08:08.0	AUDIT	User admin (session 67783, [redacted]) has logged out
2015-02-05T20:08:30.0	WARN	User admin has a mismatch for session.threshold in local account and trusted credentials. Using supplied value 1000.
2015-02-05T20:08:30.0	AUDIT	User admin (session 67885, [redacted]) has logged in
2015-02-05T20:09:38.0	AUDIT	User admin (session 67885, [redacted]) has logged out

The following figure shows the Services Logs view Historical tab.



Timestamp	Level	Message
2016-02-12T18:51:54.0	INFO	Running task /archiver/collections/default/index with message sizeRoll (type=meta,session,packet log=0 maxPercent=95) - 300 secs waited
2016-02-12T18:56:54.0	INFO	Running task /archiver/collections/default/index with message sizeRoll (type=meta,session,packet log=0 maxPercent=95) - 300 secs waited
2016-02-12T19:01:54.0	INFO	Running task /archiver/collections/default/index with message sizeRoll (type=meta,session,packet log=0 maxPercent=95) - 300 secs waited
2016-02-12T19:06:54.0	INFO	Running task /archiver/collections/default/index with message sizeRoll (type=meta,session,packet log=0 maxPercent=95) - 300 secs waited
2016-02-12T19:11:54.0	INFO	Running task /archiver/collections/default/index with message sizeRoll (type=meta,session,packet log=0 maxPercent=95) - 300 secs waited
2016-02-12T19:16:54.0	INFO	Running task /archiver/collections/default/index with message sizeRoll (type=meta,session,packet log=0 maxPercent=95) - 300 secs waited
2016-02-12T19:21:54.0	INFO	Running task /archiver/collections/default/index with message sizeRoll (type=meta,session,packet log=0 maxPercent=95) - 300 secs waited
2016-02-12T19:26:54.0	INFO	Running task /archiver/collections/default/index with message sizeRoll (type=meta,session,packet log=0 maxPercent=95) - 300 secs waited
2016-02-12T19:31:54.0	INFO	Running task /archiver/collections/default/index with message sizeRoll (type=meta,session,packet log=0 maxPercent=95) - 300 secs waited
2016-02-12T19:36:54.0	INFO	Running task /archiver/collections/default/index with message sizeRoll (type=meta,session,packet log=0 maxPercent=95) - 300 secs waited
2016-02-12T19:41:54.0	INFO	Running task /archiver/collections/default/index with message sizeRoll (type=meta,session,packet log=0 maxPercent=95) - 300 secs waited
2016-02-12T19:44:48.0	INFO	Connection 512 (10.25.51.140) logged off user
2016-02-12T19:44:48.0	INFO	Accepting connection from trusted peer 10.25.51.140 with subject name CN = 7f34bb6c-ae16-4609-8bba-51b4695d0646

Features

The System Logging Panel has the following tabs, and the logging functions are described as part of system maintenance (see **Monitor Health and Wellness of Security Analytics** in the *System Maintenance* guide).

Feature	Description
Realtime tab	This is the monitor mode of the service log.
Historical tab	This is a searchable view of the service log.

Services Security View

This topic provides an overview of service security management in the Services Security view.

In Security Analytics, each service has a separate configuration of users, roles, and role permissions, which are managed in the Services Security view.

To access service information and perform service operations through Security Analytics, a user must belong to a role that has permissions on that service. For 10.4 or later Security Analytics Core services that utilize trusted connections, it is no longer necessary to create Security Analytics Core user accounts for users that log on through the web client. You only need to create Security Analytics Core user accounts for aggregation, thick client users, and REST API users.

Note: Only the default admin user in Security Analytics is created by default on all services. As a prerequisite to managing service security, the default admin user account must be present in the Security Analytics Administration > Services view. For every other user, you must configure access to each particular service through Security Analytics.

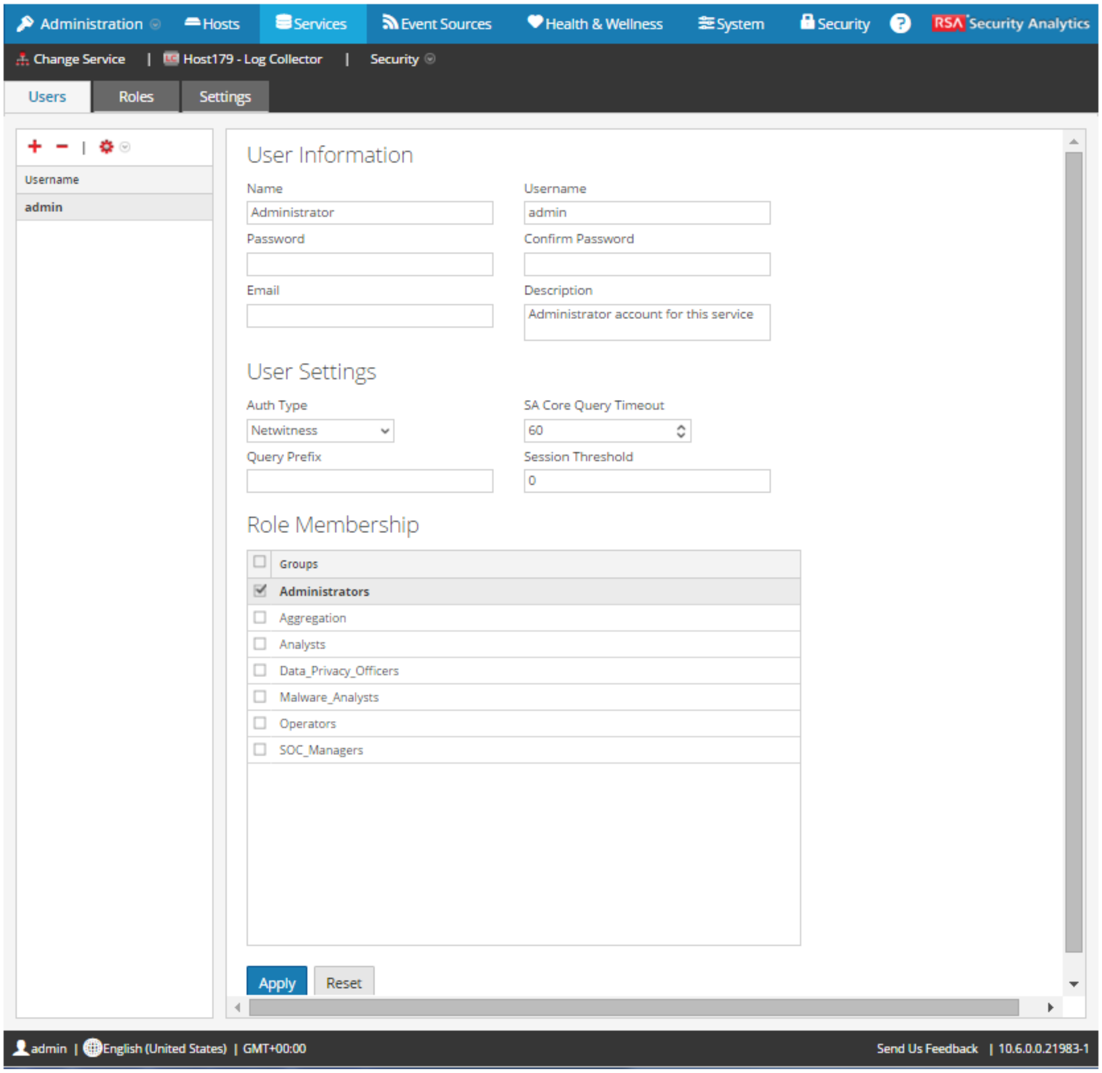
Procedures related to this tab are described in Service Procedures.

To access the Services Security view:

1. In the **Security Analytics** menu, select **Administration > Services.**

2. Select a service and select ⚙ > **View** > **Security**.

   The Services Security view for the selected service is displayed.



User Information

Name: Administrator	Username: admin
Password:	Confirm Password:
Email:	Description: Administrator account for this service

User Settings

Auth Type: Netwitness	SA Core Query Timeout: 60
Query Prefix:	Session Threshold: 0

Role Membership

□	Groups
☑	Administrators
□	Aggregation
□	Analysts
□	Data_Privacy_Officers
□	Malware_Analysts
□	Operators
□	SOC_Managers

Features

The Services Security view has three tabs, Users tab, Roles tab, and Settings tab.

Roles and Service Access

Primary considerations in configuring service security are defining the roles and assigning users to the roles. The Service Security view separates these two functions into the Users tab and the Roles tab.

- In the Roles tab, you can create roles and assign permissions to the roles for a selected service.
- In the Users tab, you can add a user, edit user settings, change the user password, and edit the role membership of the user for a selected service. Although you select a single service in the Services Security view, you can apply the settings for one service to other services.

Topics

- Roles Tab
- Service User Roles and Permissions
- Aggregation Role
- Settings Tab
- Users Tab

Roles Tab

This topic introduces the features of the Services Security View > Roles Tab.

The **Roles** tab enables you to create roles and assign permissions. Each role can have different permissions for different services. For example, the Analysts role can have different role permissions based on the selected service.

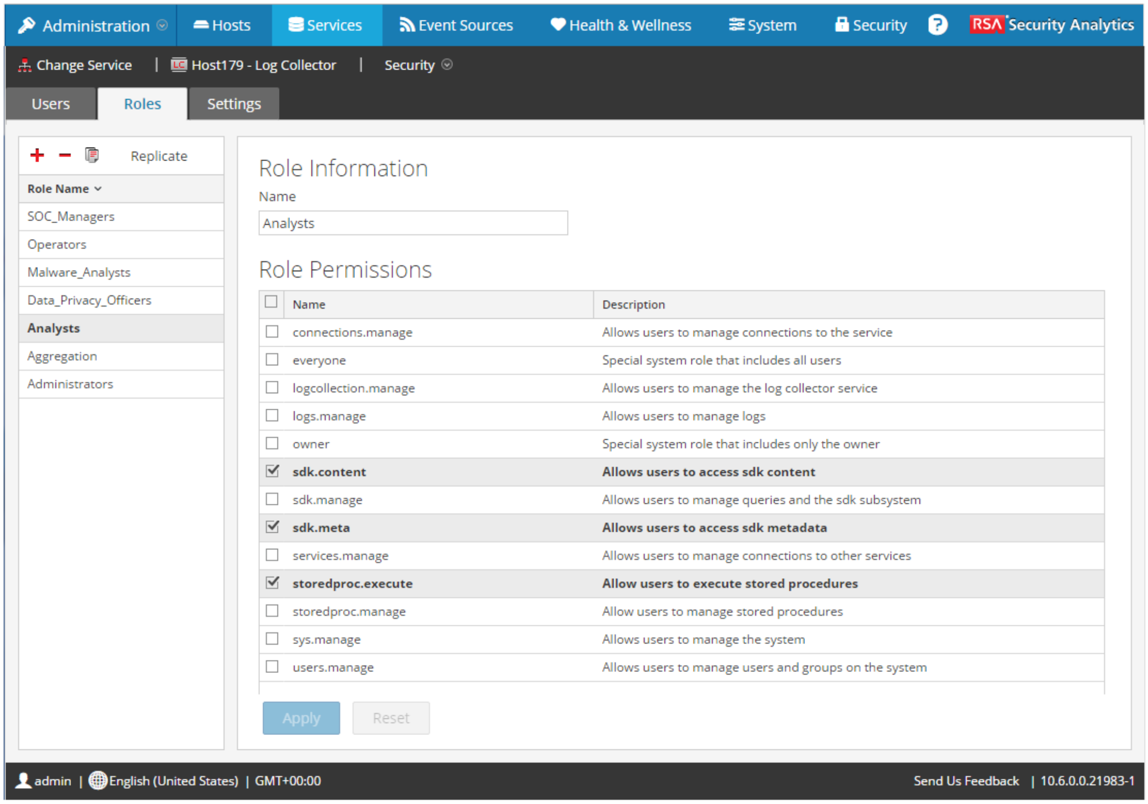
Before you can add users to roles, you need to define user roles, usually by function, and assign permissions to the roles.

Procedures related to this tab are described in Service Procedures.

To display the **Services Security View** > **Roles** tab:

1. In the **Security Analytics** menu, select **Administration** > **Services.**
2. Select a service to which you want to add a user, and select ⚙ > **View** > **Security**.
3. Select the **Roles** tab.

The following figure shows the Roles tab in the Services Security view.



Role Information

Name: Analysts

Role Permissions

□	Name	Description
□	connections.manage	Allows users to manage connections to the service
□	everyone	Special system role that includes all users
□	logcollection.manage	Allows users to manage the log collector service
□	logs.manage	Allows users to manage logs
□	owner	Special system role that includes only the owner
☑	**sdk.content**	**Allows users to access sdk content**
□	sdk.manage	Allows users to manage queries and the sdk subsystem
☑	**sdk.meta**	**Allows users to access sdk metadata**
□	services.manage	Allows users to manage connections to other services
☑	**storedproc.execute**	**Allow users to execute stored procedures**
□	storedproc.manage	Allow users to manage stored procedures
□	sys.manage	Allows users to manage the system
□	users.manage	Allows users to manage users and groups on the system

Features

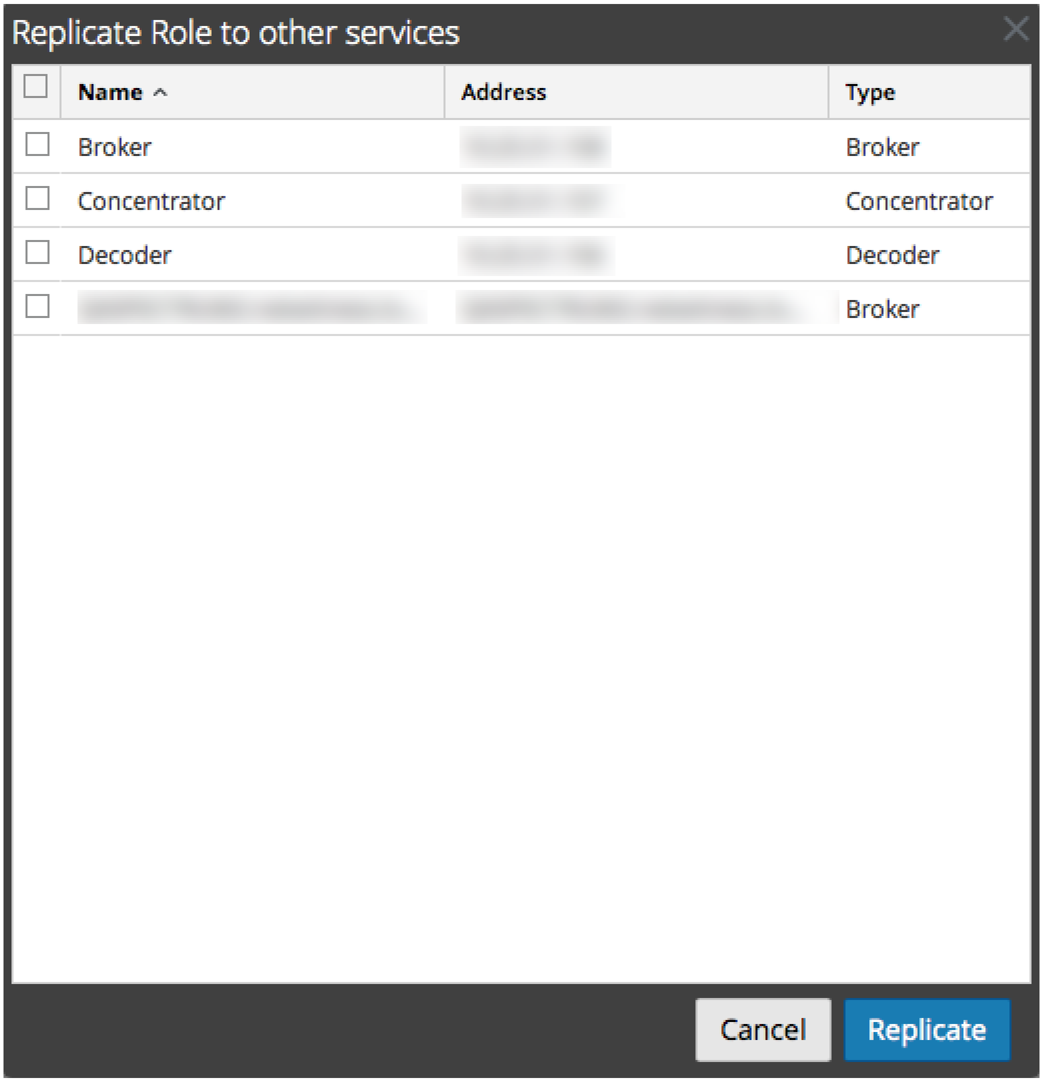
The Roles tab has a **Role Name** panel on the left. Selecting a role name shows the **Role Information** panel for the selected role on the right.

Role Name Panel

The **Role Name** panel has the following features.

Feature	Description
+	Adds a new group to the current service.
−	Deletes the selected group from the current service.
⧉	Copies a role and its assigned permissions to a new role. The name of the new role must be unique. For example, you can copy the **Analysts** role and create another role with a new name, such as **Analyst_Managers**.
Replicate	Pushes a role and its assigned permissions to other services. After you select a role and click **Replicate**, the **Replicate Role to other services** dialog is displayed. In the dialog, you can select the services where you want to replicate the role.

The following figure shows the **Replicate Role to other services** dialog.



Replicate Role to other services

□	Name ^	Address	Type
□	Broker	[redacted]	Broker
□	Concentrator	[redacted]	Concentrator
□	Decoder	[redacted]	Decoder
□	[redacted]	[redacted]	Broker

Role Information Panel

The **Role Information** panel defines role permissions.

There are two buttons:

- The **Apply** button saves the changes made in the Role Permissions panel and they become effective immediately.
- If you have not saved changes in the Role Permissions panel, the **Reset** button resets all fields and settings to their values before editing.

Service User Roles and Permissions

This topic describes the pre-configured service user roles and permissions.

The Services Security view Roles tab enables you to create service user roles and assign permissions. You can also use the pre-configured roles included with Security Analytics to assign user permissions.

Service User Roles

Security Analytics has the following pre-configured service user roles.

Role	Assigned Permissions	Personnel/Account
Administrators	All permissions	Security Analytics System Administrator
Aggregation	aggregate sdk.content sdk.meta sdk.packets	You can use this role to create an Aggregation account. This role provides the minimum permissions necessary to perform aggregation of data. It is only available on Security Analytics 10.5 and later services.
Analysts, Malware_Analysts, and SOC_Managers	sdk.meta sdk.content sdk.packets storedproc.execute	Users can use specific applications, run queries and view content for purposes of analysis.

Role	Assigned Permissions	Personnel/Account
Data_Privacy_Officers	sys.manage users.manage sdk.meta sdk.content sdk.packets sdk.manage logs.manage database.manage index.manage dpo.manage	Data Privacy Officer Data Privacy Officers have the dpo.manage permission on Decoders and Log Decoders.
Operators	sys.manage services.manage connections.manage users.manage logs.manage parsers.manage rules.manage database.manage index.manage sdk.manage decoder.manage archiver.manage concentrator.manage storedproc.manage	Operators are responsible for the daily operation of the services.

Service User Permissions

There are many permissions that you can assign a service role in Security Analytics. Users can have different permissions on each service, depending on their role assignments and the permissions selected for each role. This table describes the permissions that you can assign to a role.

Permission	Definition
sys.manage	Allows the user to edit the service configuration settings.
services.manage	Allows the user to manage connections to other services.
connections.manage	Allows the user to manage connections to the service.
users.manage	Allows the user to create individual users and user roles and specify user permissions.
aggregate	Allows the user to perform aggregation of data.
sdk.meta	Allows the user to run queries in the Investigation and Reporting applications and to view the metadata returned by the query.
sdk.content	Allows the user to access raw packets and logs from any client application (Investigations and Reporting).
sdk.packets	Allows users to access raw packets and logs from any client application.
appliance.manage	Allows the user to manage the appliance (host) tasks. This permission is required by the Appliance service.
decoder. manage	Allows the user to edit the configuration settings for the Decoder service.
concentrator.manage	Allows the user to edit the configuration settings for the Concentrator/Broker service.

Permission	Definition
logs.manage	Allows the user to view the service logs and edit the logging configuration settings for the specified service.
parsers.manage	Allows the user to manage all attributes under the parsers node.
rules.manage	Allows the user to add and delete all rules.
database.manage	Allows the user to set database locations, sizes, and the various configuration settings for the session, meta and/or packet/log databases.
index.manage	Allows the user to manage all index-related attributes.
sdk.manage	Allows the user to view and set all SDK configuration items.
storedproc.execute	Allows the user to execute a Lua stored procedure.
storedproc.manage	Allows the user to manage Lua stored procedures.
archiver.manage	Allows the user to modify the Archiver configuration.
dpo.manage	Allows the user to manage the transform configuration and the applicable keys.

Aggregation Role

This topic describes the Aggregation role and permissions that allow service users to perform aggregation.

The Aggregation role is a service user role intended only for aggregation of data. It has the minimum role permissions required to do aggregation:

- aggregate
- sdk.meta
- sdk.packets
- sdk.content

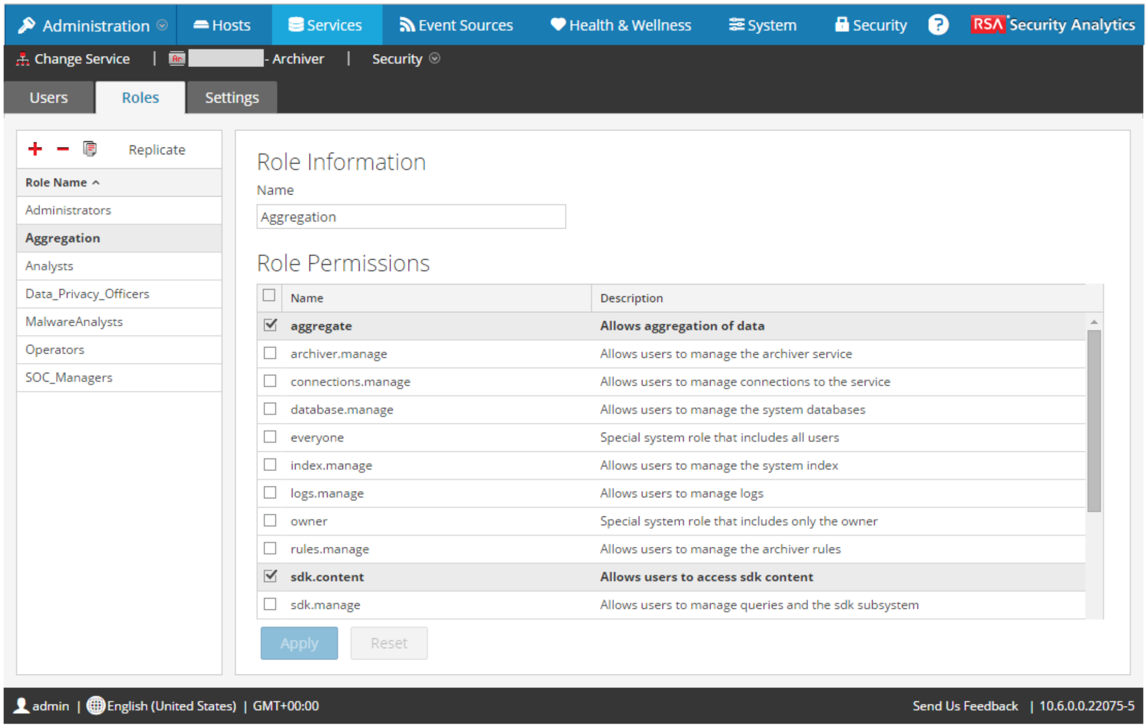
The Aggregation role is available only on Security Analytics 10.5 and later services and it can be used for an aggregation account. Members of this role or service users with these permissions can perform aggregation on Decoders, Concentrators, Archivers, and Brokers. The **aggregate** permission allows service users to perform aggregation of sessions and metadata along with raw packets and logs.

You can still use the decoder.manage, concentrator.manage, and archiver.manage permissions, but the Aggregation role permissions allow aggregation only and prevent the other available operations.

You access the service roles from the Administration > Services (select a service) > Actions > View > Security > Roles tab.

Procedures related to roles are described in Service Procedures. Service User Roles and Permissions provides detailed information on the pre-configured roles.

The following figure shows the permissions in the Aggregation role.



Role Name
Administrators
Aggregation
Analysts
Data_Privacy_Officers
MalwareAnalysts
Operators
SOC_Managers

Role Information

Name: Aggregation

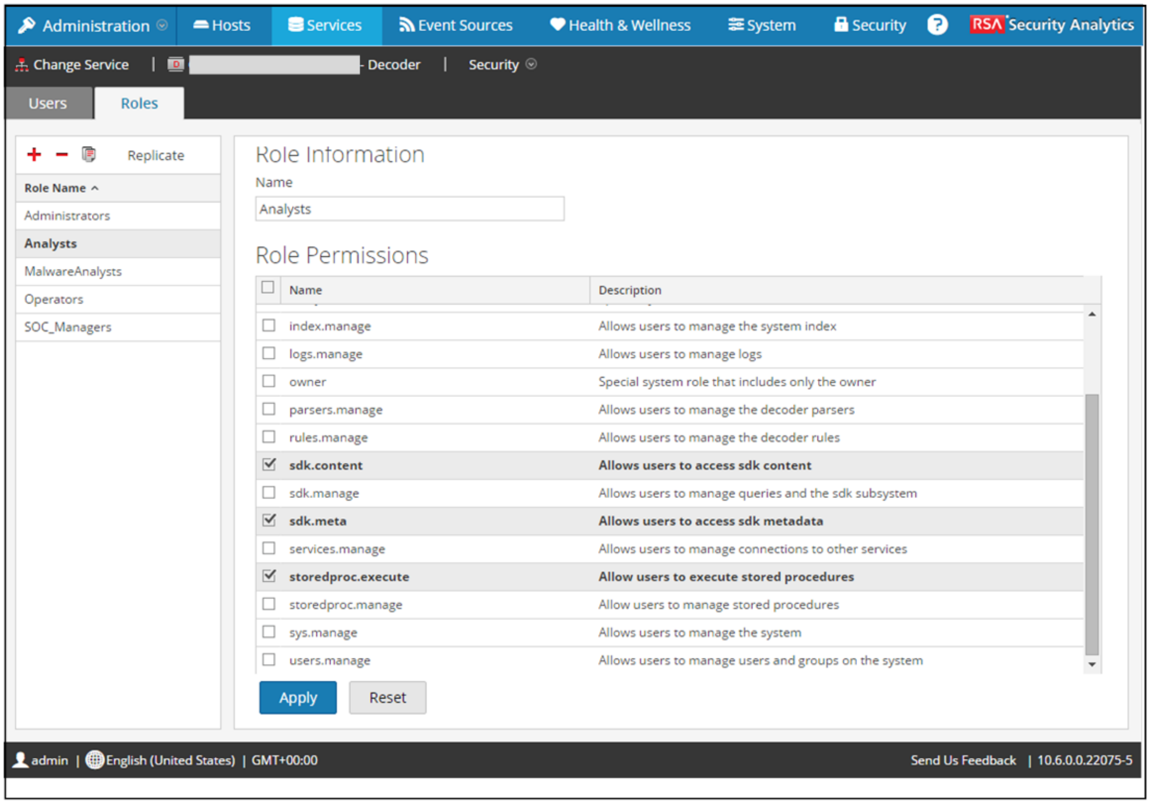
Role Permissions

□	Name	Description
☑	**aggregate**	**Allows aggregation of data**
□	archiver.manage	Allows users to manage the archiver service
□	connections.manage	Allows users to manage connections to the service
□	database.manage	Allows users to manage the system databases
□	everyone	Special system role that includes all users
□	index.manage	Allows users to manage the system index
□	logs.manage	Allows users to manage logs
□	owner	Special system role that includes only the owner
□	rules.manage	Allows users to manage the archiver rules
☑	**sdk.content**	**Allows users to access sdk content**
□	sdk.manage	Allows users to manage queries and the sdk subsystem

Settings Tab

This topic describes the features of the Services Security view > Settings tab.

In the Services Security view Settings tab, Administrators can enable and configure system roles that define permissions on a per meta key basis for individual Brokers, Concentrators, Decoders, and Log Decoders. Configuring this feature adds configurable meta keys to the Services Security view > Roles tab so that individual meta keys can be applied to specific roles on a specific service. The following figure illustrates the result of SDK meta key roles being enabled for a Decoder.



Role Information

Name: Analysts

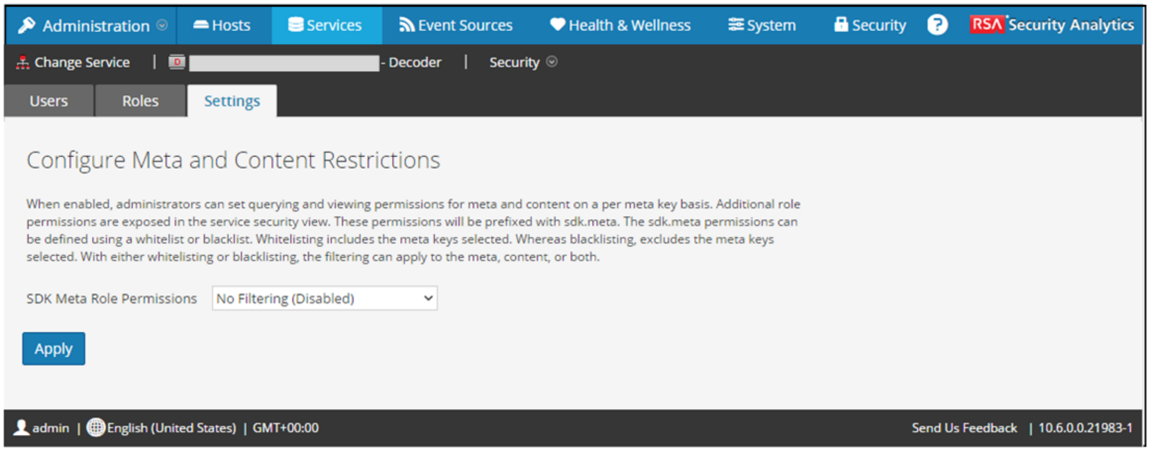
Role Permissions

□	Name	Description
□	index.manage	Allows users to manage the system index
□	logs.manage	Allows users to manage logs
□	owner	Special system role that includes only the owner
□	parsers.manage	Allows users to manage the decoder parsers
□	rules.manage	Allows users to manage the decoder rules
☑	**sdk.content**	**Allows users to access sdk content**
□	sdk.manage	Allows users to manage queries and the sdk subsystem
☑	**sdk.meta**	**Allows users to access sdk metadata**
□	services.manage	Allows users to manage connections to other services
☑	**storedproc.execute**	**Allow users to execute stored procedures**
□	storedproc.manage	Allow users to manage stored procedures
□	sys.manage	Allows users to manage the system
□	users.manage	Allows users to manage users and groups on the system

This configuration is generally part of a data privacy plan implemented to ensure that specific types of content consumed or aggregated by a service are kept secure by limiting visibility of the meta data and content to privileged users (see *Data Privacy Management*).

To display the tab:

1. In the **Security Analytics** menu, select **Administration > Services**.
2. In the **Services** grid, select a Decoder or Log Decoder service and ⚙ > **View > Security** and click the **Settings** tab.



Configure Meta and Content Restrictions

When enabled, administrators can set querying and viewing permissions for meta and content on a per meta key basis. Additional role permissions are exposed in the service security view. These permissions will be prefixed with sdk.meta. The sdk.meta permissions can be defined using a whitelist or blacklist. Whitelisting includes the meta keys selected. Whereas blacklisting, excludes the meta keys selected. With either whitelisting or blacklisting, the filtering can apply to the meta, content, or both.

SDK Meta Role Permissions: No Filtering (Disabled)

Features

The tab includes two features.

Feature	Description
SDK Meta Role Permissions field	Provides option for disabling or configuring meta key and content restrictions. The filtering options are described.
Apply button	Applies the selected configuration immediately. If not disabled, the meta keys are added to the Roles tab so they can be applied to specific roles.

SDK Meta Role Permissions Options

The following table lists the filtering options available in the SDK Meta Role Permissions selection list, and the numeric values used to disable (0) and the types of filtering (1 through 6).

Note: There is no need to know the numeric value unless configuring meta and content visibility manually in the system.roles node.

system.roles Node Value	Settings Tab Option	Description
0	No Filtering (Disabled)	System roles that define permissions on a per meta key basis are disabled.

system.roles Node Value	Settings Tab Option	Description
1	Whitelist meta and content	Meta and content for the specified SDK meta roles are white listed, or visible to users assigned the system role.
2	Whitelist only meta	Meta for the specified SDK meta roles is white listed, or visible to users assigned the system role.
3	Whitelist only content	Content for the specified SDK meta roles is white listed, or visible to users assigned the system role.
4	Blacklist meta and content	Meta and content for the specified SDK meta roles are black listed, or not visible to users assigned the system role.
5	Blacklist only meta	Meta for the specified SDK meta roles is black listed, or not visible to users assigned the system role.
6	Blacklist only content	Content for the specified SDK meta roles is black listed, or not visible to users assigned the system role.

Users Tab

This topic explains the features of the Services Security view > Users tab.

In the Services Security view, the Users tab enables you to configure the following for a service:

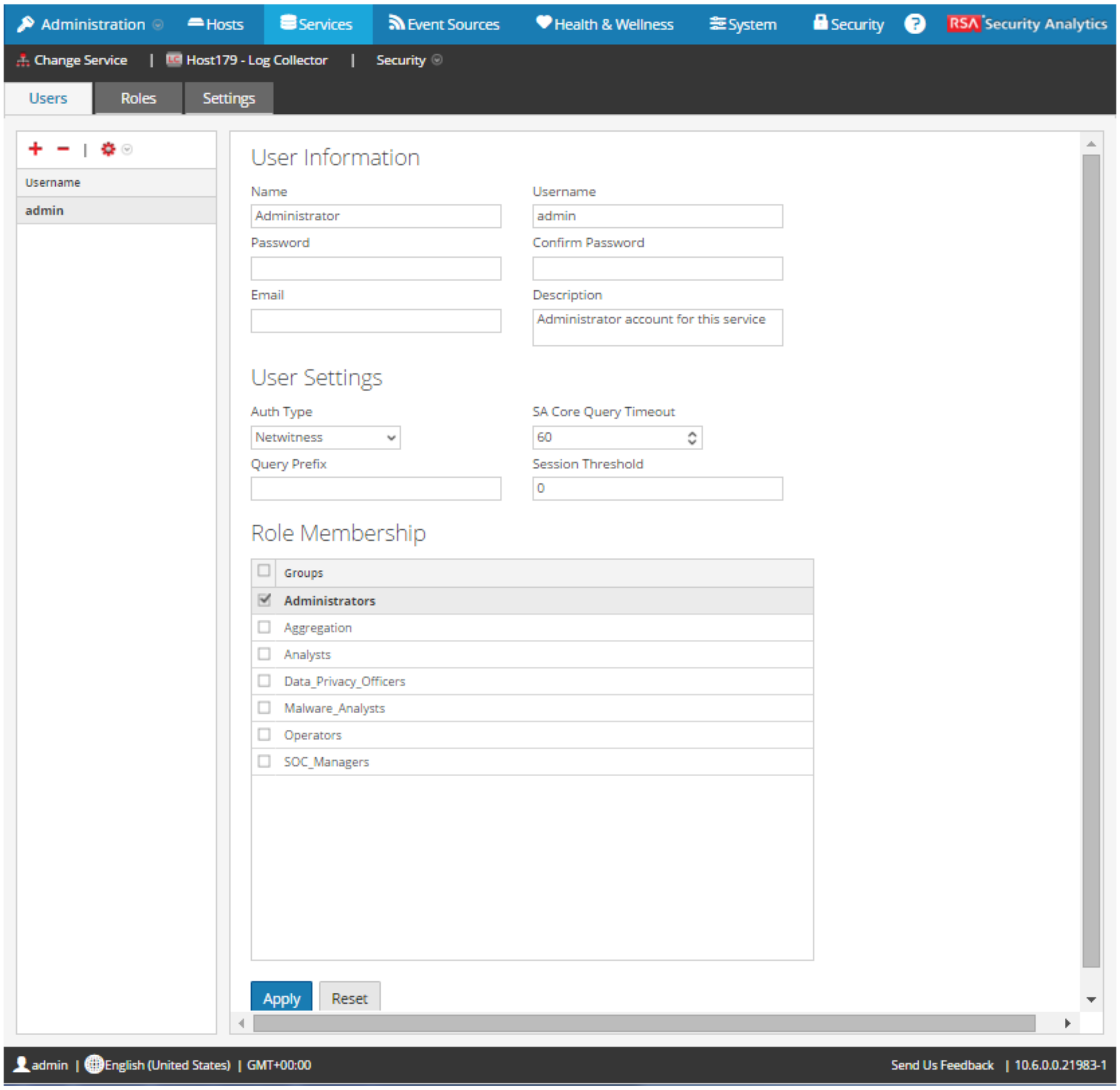
- Add user accounts.
- Change service user passwords.
- Configure user authentication properties and query handling properties for the service.
- Specify the user role membership, which specifies the roles that the user belongs to on the selected service.

Note: For 10.4 or later Security Analytics Core services that utilize trusted connections, it is no longer necessary to create Security Analytics Core user accounts for users that log on through the web client. You only need to create Security Analytics Core user accounts for aggregation, thick client users, and REST API users.

Procedures related to this tab are described in Service Procedures.

To access the Services Security view > Users tab:

1. In the **Security Analytics** menu, select **Administration > Services.**
2. Select a service to which you want to add a user, and select ⚙ ⌄ **> View > Security**.



User Information

Name: Administrator

Username: admin

Password:

Confirm Password:

Email:

Description: Administrator account for this service

User Settings

Auth Type: Netwitness

SA Core Query Timeout: 60

Query Prefix:

Session Threshold: 0

Role Membership

□	Groups
☑	Administrators
□	Aggregation
□	Analysts
□	Data_Privacy_Officers
□	Malware_Analysts
□	Operators
□	SOC_Managers

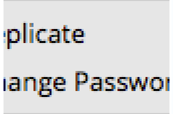
Features

The Users tab has a User List panel on the left. Selecting a username makes the User Definition panel on the right available.

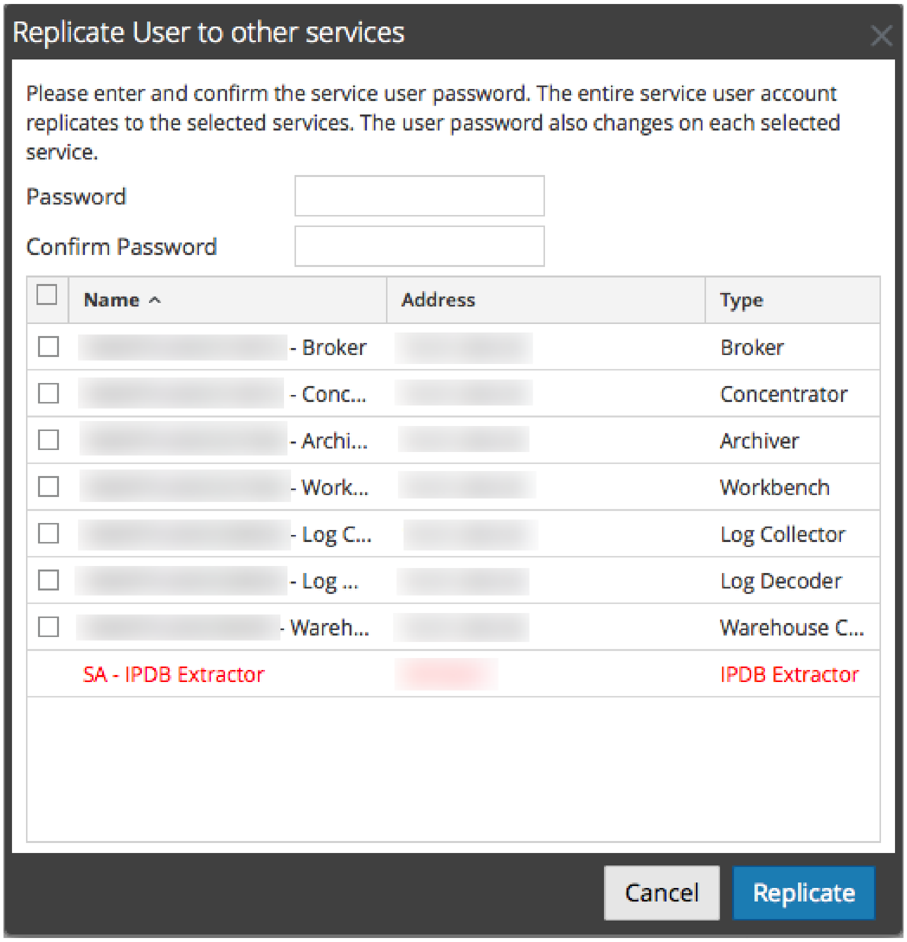
User List Panel

The User List panel has the following features.

Feature	Description
+	Adds a new user to the current service.

Feature	Description
−	Deletes the selected users from the service.
 plicate ange Passwor	Performs one of the following actions on the selected service user account: • **Replicate:** Replicates the entire service user account to selected services. • **Change Password:** Changes the password of a service user and replicates the new password to Core services with that user account defined. The Change Password option replicates only the password change to the Core services selected and does not replicate the entire user account.
Username	The user names for all user accounts that access the service. The username must be one used to log on to Security Analytics.

The following figure shows the **Replicate User to other services** dialog.



Replicate User to other services

Please enter and confirm the service user password. The entire service user account replicates to the selected services. The user password also changes on each selected service.

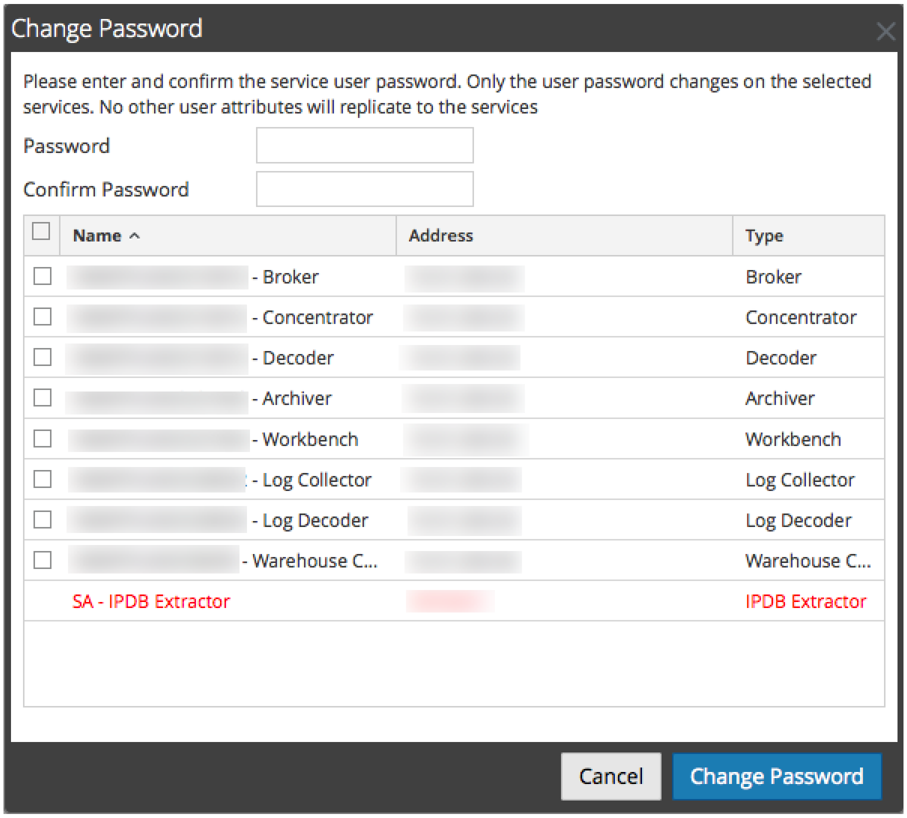
Password

Confirm Password

□	Name ^	Address	Type
□	[redacted] - Broker	[redacted]	Broker
□	[redacted] - Conc...	[redacted]	Concentrator
□	[redacted] - Archi...	[redacted]	Archiver
□	[redacted] - Work...	[redacted]	Workbench
□	[redacted] - Log C...	[redacted]	Log Collector
□	[redacted] - Log ...	[redacted]	Log Decoder
□	[redacted] - Wareh...	[redacted]	Warehouse C...
	SA - IPDB Extractor	[redacted]	IPDB Extractor

Cancel Replicate

The following figure shows the **Change Password** dialog.



Change Password

Please enter and confirm the service user password. Only the user password changes on the selected services. No other user attributes will replicate to the services

Password

Confirm Password

□	Name ^	Address	Type
□	[redacted] - Broker	[redacted]	Broker
□	[redacted] - Concentrator	[redacted]	Concentrator
□	[redacted] - Decoder	[redacted]	Decoder
□	[redacted] - Archiver	[redacted]	Archiver
□	[redacted] - Workbench	[redacted]	Workbench
□	[redacted] - Log Collector	[redacted]	Log Collector
□	[redacted] - Log Decoder	[redacted]	Log Decoder
□	[redacted] - Warehouse C...	[redacted]	Warehouse C...
	SA - IPDB Extractor	[redacted]	IPDB Extractor

User Definition Panel

The User Definition panel has three sections:

- User Information identifies the user as created in the Administration Security view.
- User Settings define parameters that apply to this user's access to the service.
- Role Membership defines user roles to which the user belongs.

There are two buttons:

- The **Save** button saves the changes made in the User Definition panel, and they become effective immediately.
- If you have not saved changes in the User Definition panel, the **Reset** button resets all fields and settings to their values before editing.

User Information

The User Information section has the following features.

Field	Description
Name	The name of the user.
Username	The username that this user enters to log on to the service. This is the Security Analytics username generated when the administrator added the user and the associated credentials in the **Administration Security** view (Administration > Security).
Password (and **Confirm Password**)	The password that the user enters to log on to the service. This is the Security Analytics password generated when the administrator added the user and the associated credentials in the **Administration Security** view. The Security Analytics account password and the service password must match in order to allow the user to connect to the service through Security Analytics.
Email	(Optional) The user's email address.
Description	(Optional) A general description field to describe this user.

User Settings

The User Settings section has the following features.

Field	Description
Auth Type	The authentication scheme for this user. The product line supports internal and external authentication. • **Netwitness** specifies internal authentication, and is enabled by default. In this mode, all users must authenticate with the user account and passwords that are generated when the administrator uses the Security Analytics Administration Security view (Administration > Security) to create the user and their associated credentials. • **External** specifies that authentication is enabled through the host interface with PAM (Pluggable Authentication Modules). For more information, see the **Configure PAM Login Capability** topic in the *System Security and User Management* guide.

Field	Description
Query Prefix	(Optional) Always append the query syntax to all queries by this user. For example, adding the query prefix **email != 'ceo@company.com'** prevents those email results from showing up in the sessions.
SA Core Query Timeout	**Note:** This field applies to Security Analytics 10.5 and later service versions and does not appear for 10.4 and earlier service versions. Security Analytics 10.4 and earlier services use Query Level instead of SA Core Query Timeout. Specifies the maximum number of minutes a user can run a query on the service. If this value is set to zero (0), the query timeout is not enforced for the user on the service. When replicating a user from a Security Analytics 10.5 or later service to a Security Analytics 10.4 service, Query Timeout migrates to Query Level based on the closest level. For example, if a user has a Query Timeout of 15 minutes, the user gets a Query Level of 3 after the migration. If a user has a Query Timeout of 35 minutes, the user gets a Query Level of 2 after the migration. If a user has a Query Timeout of 45 minutes, the user gets a Query Level of 2 after the migration.
Session Threshold	(Optional) Controls the behavior of the application when scanning meta values to determine session counts. Any meta value with a session count that is above the set threshold stops its determination of the true session count when the threshold is reached. If a threshold is set for a session, the Navigation view shows that the threshold was reached and the percentage of query time used to reach the threshold.

Role Membership

The Role Membership section shows the roles that a user is a member of for the selected service.

Services Stats View

This topic describes the features available in Security Analytics Services Stats view.

The Services Stats view provides a way to monitor the status and operations of a service. This view displays key statistics, service system information, and host system information for a service. In addition, more than 80 statistics are available for viewing as gauges and in timeline charts. In historical timeline charts, only statistics for session size, sessions, and packets are viewable.

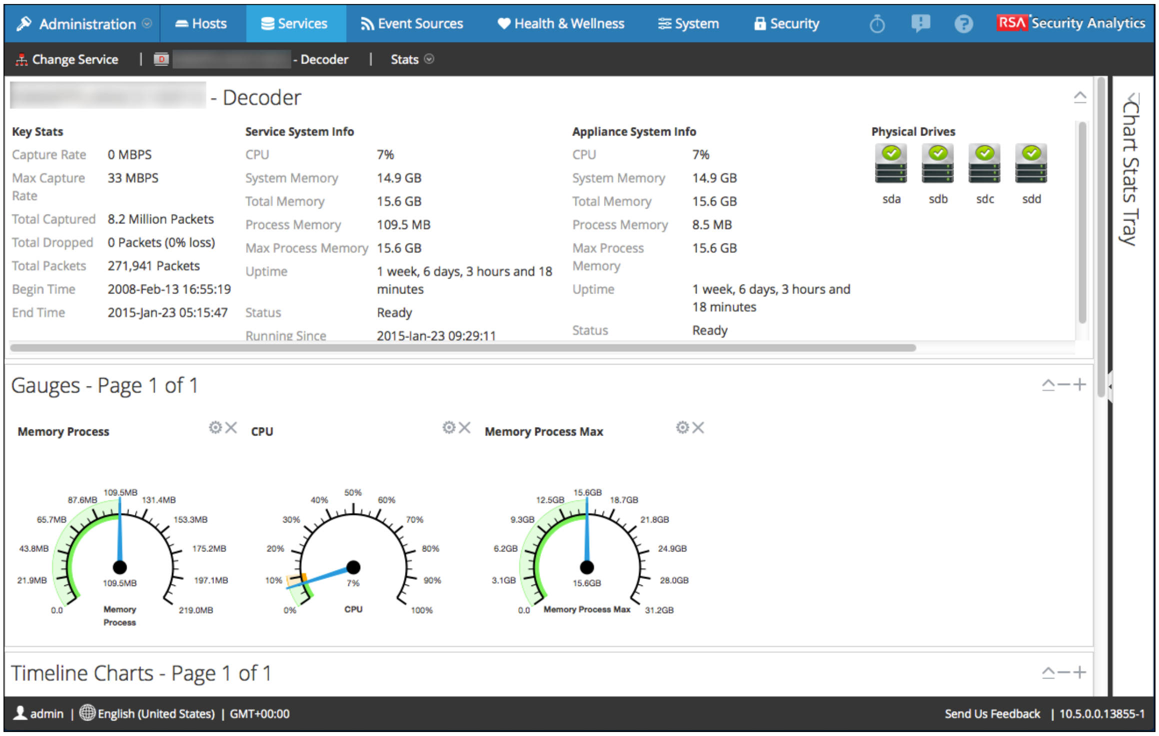
To access the Service Stats view:

1. In the **Security Analytics** menu, select **Administration** > **Services**.

   The Services view is displayed.

2. Select a service and select ⚙ > **View** > **Stats**.

The following example shows the Services Stats view for a Decoder.



[redacted] - Decoder

Key Stats

Capture Rate	0 MBPS
Max Capture Rate	33 MBPS
Total Captured	8.2 Million Packets
Total Dropped	0 Packets (0% loss)
Total Packets	271,941 Packets
Begin Time	2008-Feb-13 16:55:19
End Time	2015-Jan-23 05:15:47

Service System Info

CPU	7%
System Memory	14.9 GB
Total Memory	15.6 GB
Process Memory	109.5 MB
Max Process Memory	15.6 GB
Uptime	1 week, 6 days, 3 hours and 18 minutes
Status	Ready
Running Since	2015-Jan-23 09:29:11

Appliance System Info

CPU	7%
System Memory	14.9 GB
Total Memory	15.6 GB
Process Memory	8.5 MB
Max Process Memory	15.6 GB
Uptime	1 week, 6 days, 3 hours and 18 minutes
Status	Ready

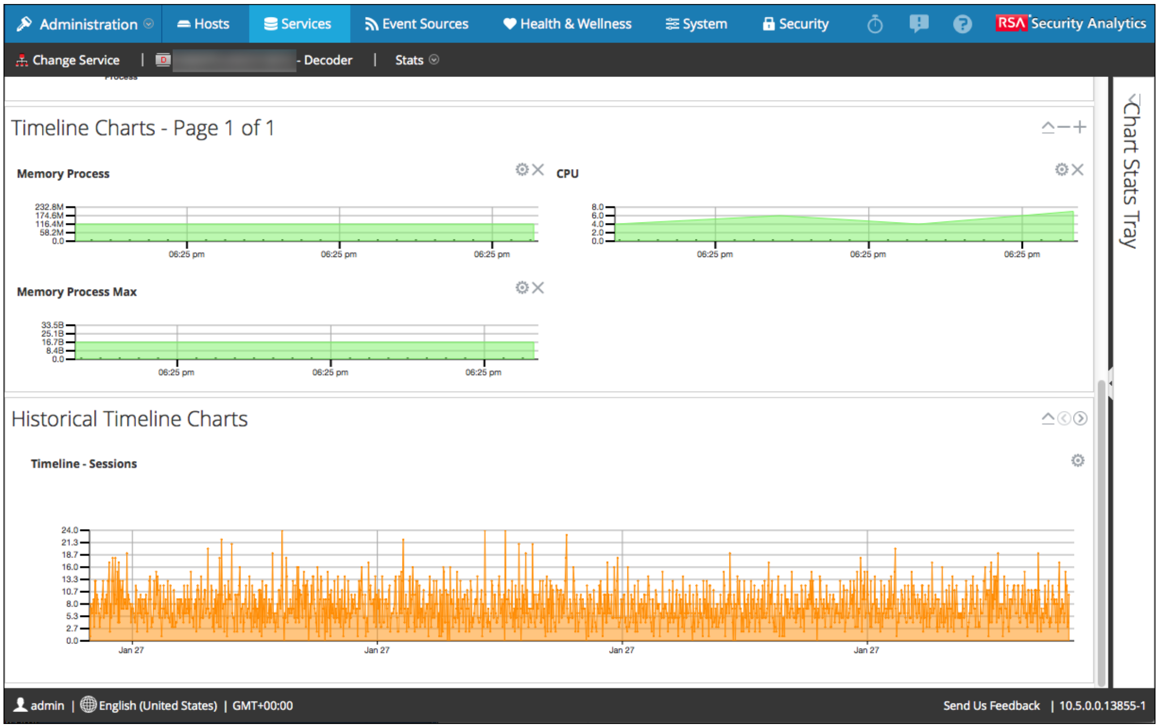
Physical Drives

✓ sda ✓ sdb ✓ sdc ✓ sdd

Gauges - Page 1 of 1

Timeline Charts - Page 1 of 1

The following example shows the additional charts available after scrolling down.



The following example shows the Chart Stats Tray expanded.

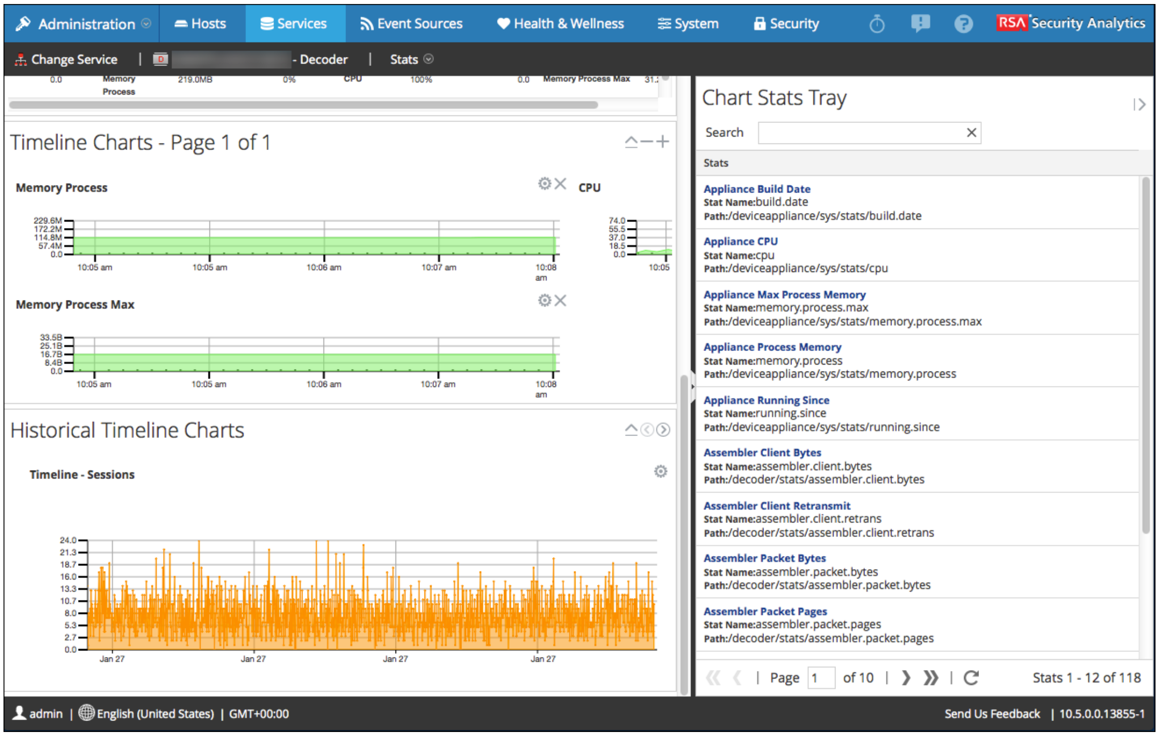


Chart Stats Tray

Search

Stats

Appliance Build Date
Stat Name:build.date
Path:/deviceappliance/sys/stats/build.date

Appliance CPU
Stat Name:cpu
Path:/deviceappliance/sys/stats/cpu

Appliance Max Process Memory
Stat Name:memory.process.max
Path:/deviceappliance/sys/stats/memory.process.max

Appliance Process Memory
Stat Name:memory.process
Path:/deviceappliance/sys/stats/memory.process

Appliance Running Since
Stat Name:running.since
Path:/deviceappliance/sys/stats/running.since

Assembler Client Bytes
Stat Name:assembler.client.bytes
Path:/decoder/stats/assembler.client.bytes

Assembler Client Retransmit
Stat Name:assembler.client.retrans
Path:/decoder/stats/assembler.client.retrans

Assembler Packet Bytes
Stat Name:assembler.packet.bytes
Path:/decoder/stats/assembler.packet.bytes

Assembler Packet Pages
Stat Name:assembler.packet.pages
Path:/decoder/stats/assembler.packet.pages

Page 1 of 10 | Stats 1 - 12 of 118

Features

Although different statistics are available for different types of services, certain elements are common to the Services Stats view for any Core service:

- Summary Stats section
- Gauges section
- Timelines section
- Historical Timelines section
- Chart Stats Tray

Summary Stats Section

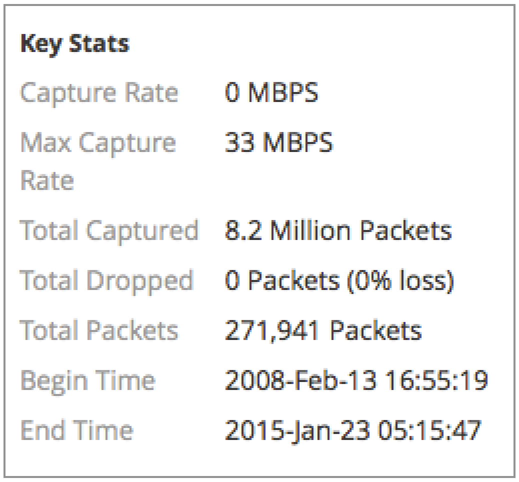
The Summary Stats section is at the top of the default view, and has no editable fields.

There are five panels in the Summary Stats section. The **Key Stats** panel displays different statistics for different types of services. The remaining panels in the Summary Stats section are the same for all types of services.

Key Stats

The Key Stats panel displays different statistics for different types of services.

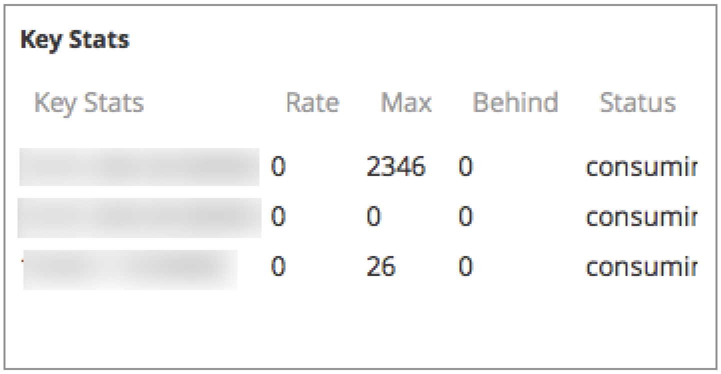
- For a Decoder or Log Decoder, key statistics include capture statistics, such as capture rate, total packets or logs captured, total packets or logs dropped, the data capture begin time and end time.



Key Stats

Capture Rate	0 MBPS
Max Capture Rate	33 MBPS
Total Captured	8.2 Million Packets
Total Dropped	0 Packets (0% loss)
Total Packets	271,941 Packets
Begin Time	2008-Feb-13 16:55:19
End Time	2015-Jan-23 05:15:47

- A Broker or Concentrator aggregates data from multiple services. Therefore, the key statistics for all aggregate services are presented in a grid. The columns in the grid provide the service name, the capture rate, the maximum capture rate, the number of session behind (that need to be aggregated), and the service status.

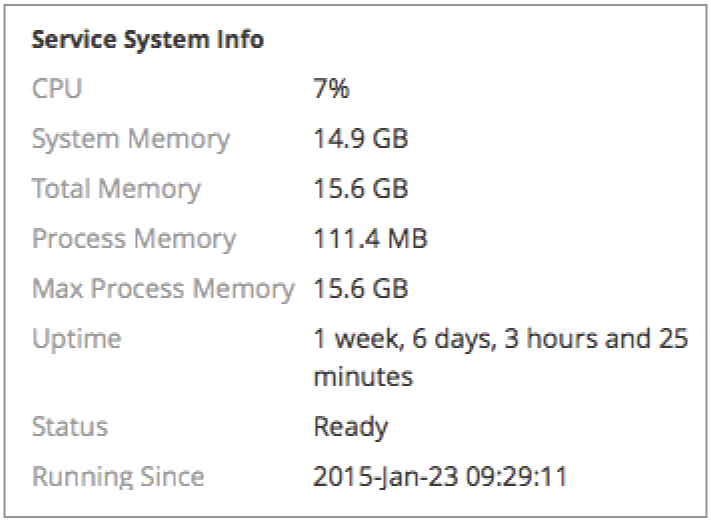


Key Stats

Key Stats	Rate	Max	Behind	Status
[redacted]	0	2346	0	consumir
[redacted]	0	0	0	consumir
[redacted]	0	26	0	consumir

Services System Info

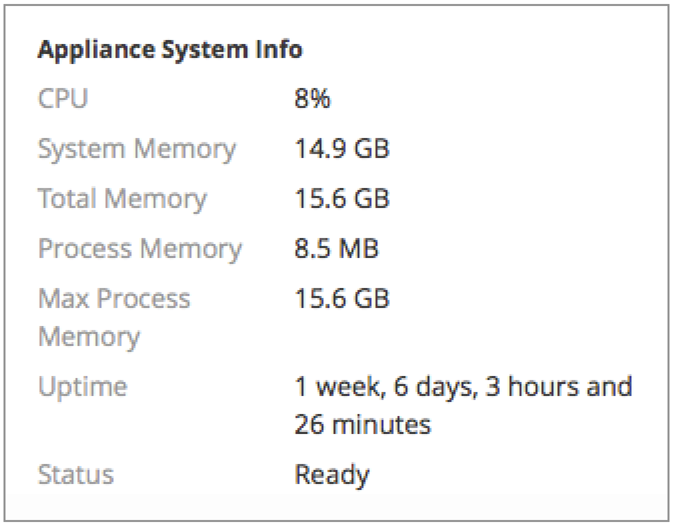
The Services System Info panel includes the percentage of CPU used by the service, the memory usage statistics (system, total, process, and maximum process), service uptime, status, running since time, and the current time.



Service System Info

CPU	7%
System Memory	14.9 GB
Total Memory	15.6 GB
Process Memory	111.4 MB
Max Process Memory	15.6 GB
Uptime	1 week, 6 days, 3 hours and 25 minutes
Status	Ready
Running Since	2015-Jan-23 09:29:11

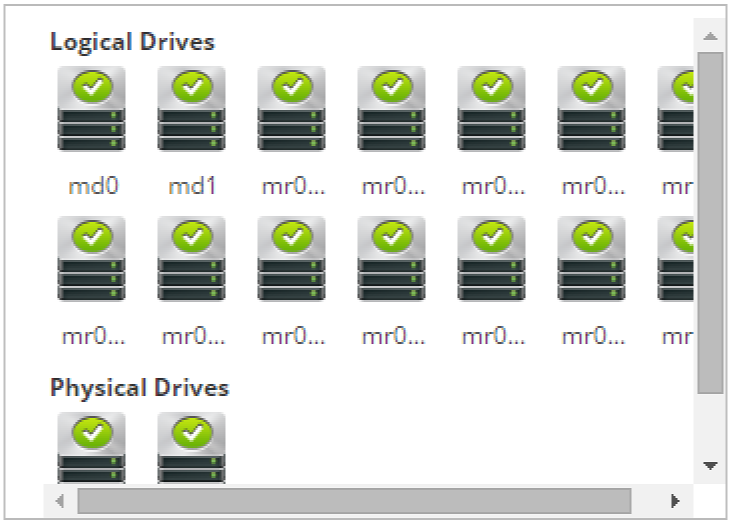
Host System Info includes percentage of CPU used by the host, the memory usage statistics (system, total, process, and maximum), host uptime, status, running since time, and the current time.



Appliance System Info

CPU	8%
System Memory	14.9 GB
Total Memory	15.6 GB
Process Memory	8.5 MB
Max Process Memory	15.6 GB
Uptime	1 week, 6 days, 3 hours and 26 minutes
Status	Ready

Logical Drives and **Physical Drives** are shown with an icon for the drive name and state. Drive types used in the names and the drive status options are listed below.



Drive Types and Status

Drive Type	Description	Comment	Status Options
sd	SCSI block device	Directly connected SAS, SATA MegaRAID volumes	OK (green) FAIL (red)

Drive Type	Description	Comment	Status Options
ld	MegaRAID Logical Volume	Defined in BIOS or with MegaCLI tool	OK (green) DEGRADED (yellow) BUILDING (yellow) FAIL (red)
pd	MegaRAID Physical Disks	Not directly exposed to Linux	OK (green) FAIL (red)
md	Linux software RAID Volume		OK (green) DEGRADED (yellow) BUILDING (yellow) FAIL (red)

Gauges

The Gauges section in the Stats View presents statistics in the form of analog gauges. See Gauges for details on configuring gauges.

Timelines

Timeline charts display the selected statistics in a running timeline with focus on the current time. This is the same for all types of services, and only the display name of the timeline is editable. See Timeline Charts for details on configuring timelines.

Historical Timelines

Historical timeline charts display statistics for session size, sessions, and packets in a historical timeline. This is the same for all types of services, and has an editable display name, begin date, and end date. See Timeline Charts for details on configuring timelines.

Note: Historical Timeline charts is being deprecated for Log Collector, Virtual Log Collector (VLC) and Windows Legacy Collector services.

Chart Stats Tray

The Chart Stats Tray lists all available statistics for the selected service type. Different services have different statistics to monitor. See Chart Stats Tray for a detailed description.

Topics

- Chart Stats Tray
- Gauges
- Timeline Charts

Chart Stats Tray

This topic describes the Chart Stats Tray in the Services Stats view.

In the Services Stats view, the Chart Stats Tray provides a way to customize the monitored statistics for individual services. The Chart Stats Tray lists all available statistics for the service. The number of statistics varies according to the type of service being monitored. Any statistic in the Chart Stats Tray can be displayed in a gauge or a timeline chart. Only statistics for session size, sessions, and packets are viewable in historical timeline charts.

To access the Services Stats view:

1. In the **Security Analytics** menu, select **Administration > Services**

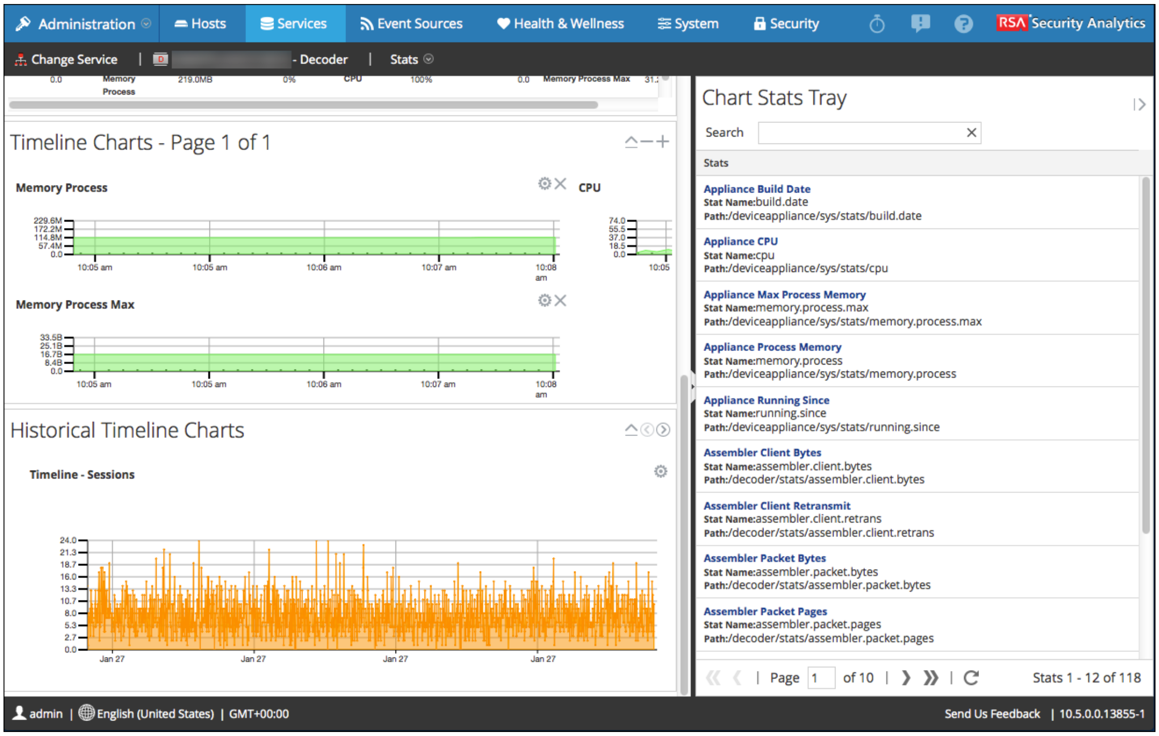
   The Administration Services view is displayed.

2. Select a service and select ⚙ ⌄ **> View > Stats.**

   The Chart Stats Tray is on the right side.

3. If the tray is collapsed, click <| to view the list of available statistics.

The following example shows the Services Stats view for a Decoder. The Chart Stats Tray is open in the right panel.



Stats

Appliance Build Date
Stat Name:build.date
Path:/deviceappliance/sys/stats/build.date

Appliance CPU
Stat Name:cpu
Path:/deviceappliance/sys/stats/cpu

Appliance Max Process Memory
Stat Name:memory.process.max
Path:/deviceappliance/sys/stats/memory.process.max

Appliance Process Memory
Stat Name:memory.process
Path:/deviceappliance/sys/stats/memory.process

Appliance Running Since
Stat Name:running.since
Path:/deviceappliance/sys/stats/running.since

Assembler Client Bytes
Stat Name:assembler.client.bytes
Path:/decoder/stats/assembler.client.bytes

Assembler Client Retransmit
Stat Name:assembler.client.retrans
Path:/decoder/stats/assembler.client.retrans

Assembler Packet Bytes
Stat Name:assembler.packet.bytes
Path:/decoder/stats/assembler.packet.bytes

Assembler Packet Pages
Stat Name:assembler.packet.pages
Path:/decoder/stats/assembler.packet.pages

Page 1 of 10 | Stats 1 - 12 of 118

Components

The Chart Stats Tray has different statistics for different types of services. In the example above, 111 statistics are available for the Decoder. The following table describes features of the Chart Stat Tray.

Feature	Description
⟨|	Click to expand the panel horizontally.
|⟩	Click to collapse the panel horizontally.
Search	Type a search term in the field and press **RETURN**. Statistics that match are displayed with the matching word highlighted.
«	Click to go to the first page.
‹	Click to go to the previous page.
ge 3 of	Type a page number in the Page field.
›	Click to go to the next page.
»	Click to go to the last page.
↻	Click to refresh the view.
Stats 1 - 1	Displays the range of statistics being displayed. The total number statistics varies by service type.

Gauges

This topic introduces the features of the Gauges section in the Services Stats view.

The Gauges section of the Services Stats view presents statistics in the form of an analog gauge. You can drag any statistic available in the Chart Stats Tray to the Gauges section. The properties of each individual gauge are editable; all gauges have an editable title and some have additional editable properties.

To access the Services Stats view:

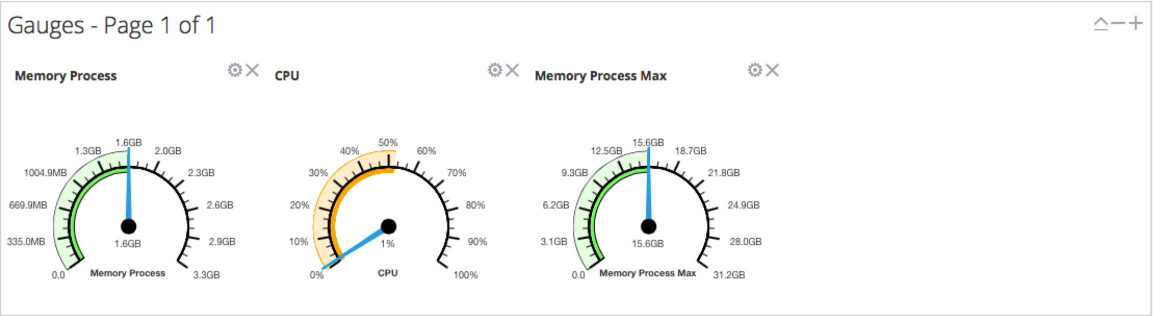
1. In the **Security Analytics** menu, select **Administration > Services**

   The Administration Services view is displayed.

2. Select a service and select ⚙ ⌄ > **View > Stats**.

   The Services Stats view includes the Gauges section.

The following figure shows the default gauges in the Services Stats view for a Log Decoder.



Features

The default gauges show these statistics:

- Process memory use
- CPU use
- Maximum process memory used

The controls in the Gauges title bar and in each gauge are the standard dashlet controls.

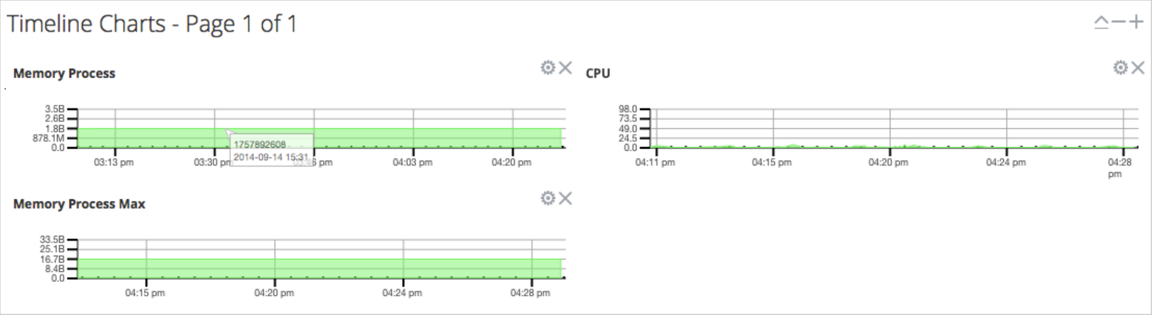
- In the Gauges title bar, you can collapse and expand the section and page forward or back.
- In each gauge, you can edit properties (⚙) and delete (✕) the gauge.

Timeline Charts

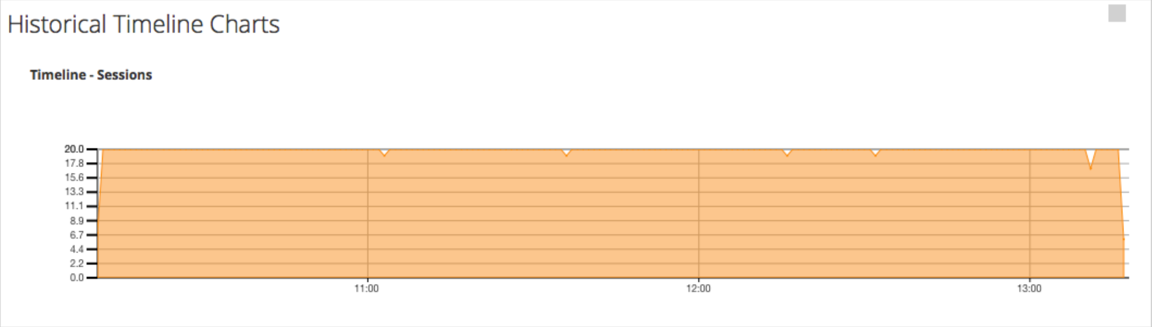
This topic describes the features of the timeline charts in the Services Stats view.

Timeline charts display statistics in a running timeline. The Services Stats view includes two types of timelines: current time and historical. You can drag any statistic available in the Chart Stats Tray to the Timeline Charts section. Only statistics for session size, sessions, and packets are viewable in historical timeline charts. The properties of an individual timeline chart are editable; all timeline charts have an editable title and some have additional editable properties.

The following figure is an example of a current timeline showing the value and timestamp of a data point.



The following figure is an example of a historical timeline chart.



The default current timeline charts show these statistics:

- Memory Process
- CPU
- Memory Process Max

The historical time charts show these statistics:

- Sessions
- Packets

- Session Size

The controls in the Timeline Charts title bar and in each timeline are the standard dashlet controls.

- In the Timeline Charts title bar, you can collapse and expand the section and page forward or back.
- In each timeline, you can edit Properties (⚙) and delete (✕) the timeline.
- Hovering over a data point in the chart, displays the value and timestamp for the selected point.

Services Stats View - Malware Analysis

This topic describes the features available in Security Analytics Services Stats view for Malware Analysis.

The Services Stats view provides a way to monitor the status and operations of a service.

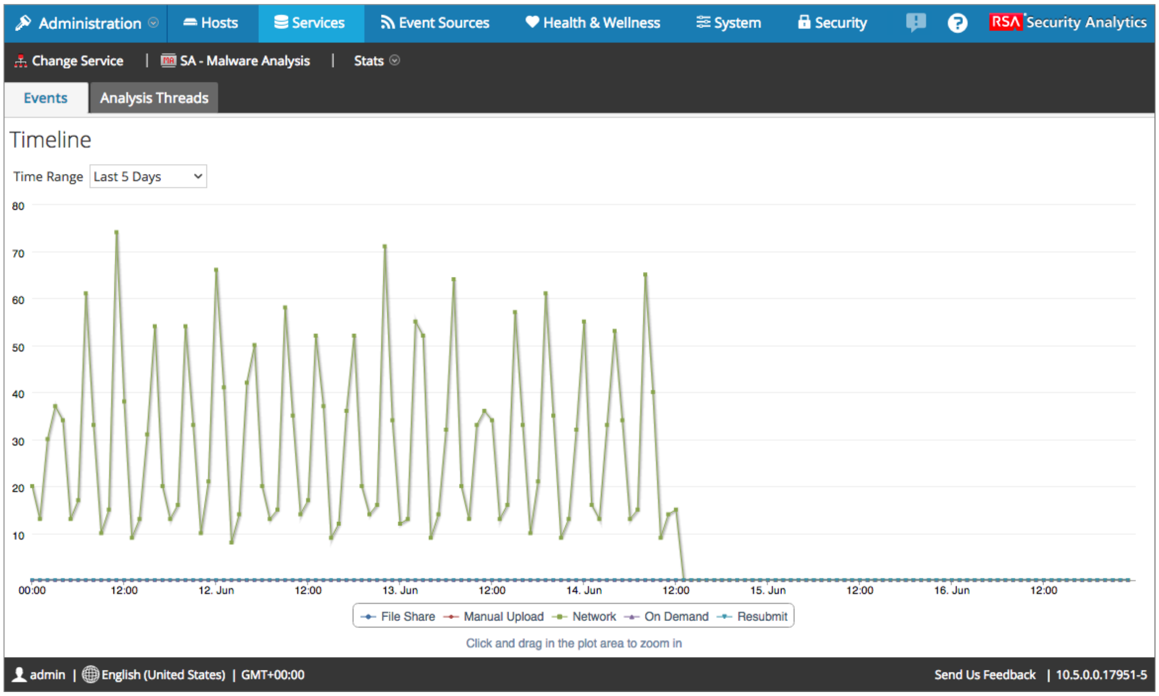
To access the Service Stats view for Malware Analysis:

1. In the **Security Analytics** menu, select **Administration** > **Services**.

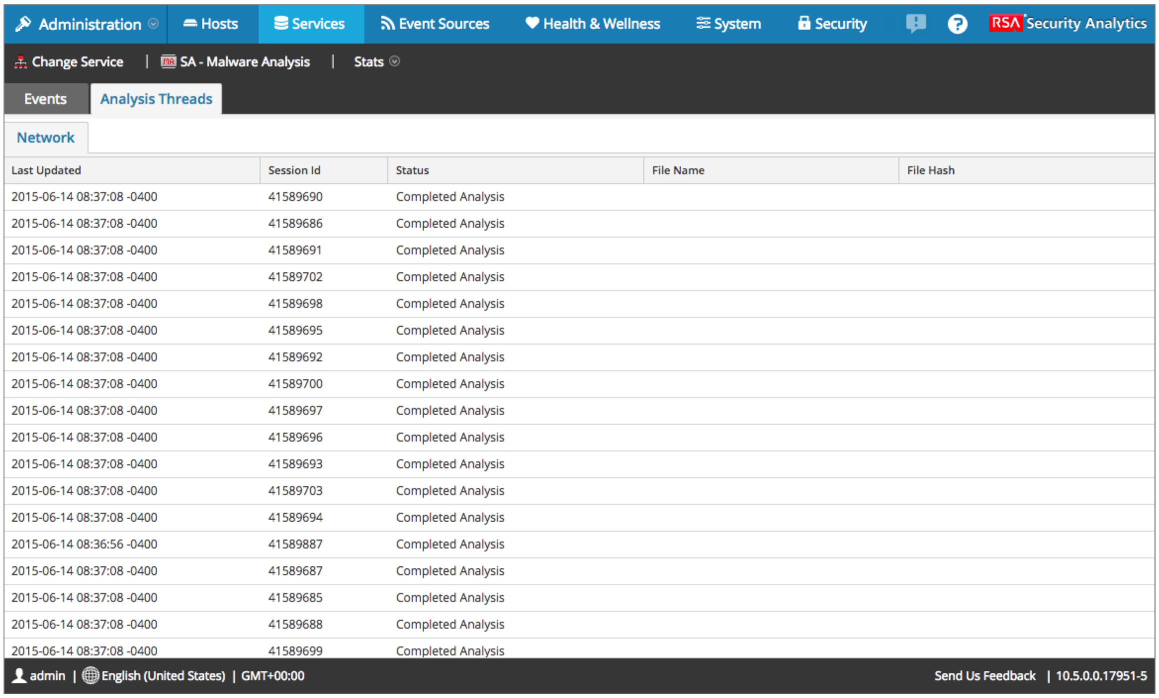
   The Services view is displayed.

2. Select a service and select ⚙ > **View** > **Stats**.

The following figure shows the Services Stats view for Malware Analysis. The default tab is the Events tab.



The following figure shows the Analysis Threads tab.



Last Updated	Session Id	Status	File Name	File Hash
2015-06-14 08:37:08 -0400	41589690	Completed Analysis		
2015-06-14 08:37:08 -0400	41589686	Completed Analysis		
2015-06-14 08:37:08 -0400	41589691	Completed Analysis		
2015-06-14 08:37:08 -0400	41589702	Completed Analysis		
2015-06-14 08:37:08 -0400	41589698	Completed Analysis		
2015-06-14 08:37:08 -0400	41589695	Completed Analysis		
2015-06-14 08:37:08 -0400	41589692	Completed Analysis		
2015-06-14 08:37:08 -0400	41589700	Completed Analysis		
2015-06-14 08:37:08 -0400	41589697	Completed Analysis		
2015-06-14 08:37:08 -0400	41589696	Completed Analysis		
2015-06-14 08:37:08 -0400	41589693	Completed Analysis		
2015-06-14 08:37:08 -0400	41589703	Completed Analysis		
2015-06-14 08:37:08 -0400	41589694	Completed Analysis		
2015-06-14 08:36:56 -0400	41589887	Completed Analysis		
2015-06-14 08:37:08 -0400	41589687	Completed Analysis		
2015-06-14 08:37:08 -0400	41589685	Completed Analysis		
2015-06-14 08:37:08 -0400	41589688	Completed Analysis		
2015-06-14 08:37:08 -0400	41589699	Completed Analysis		

Features

The Services Stats view for Malware Analysis has two tabs:

- Events tab
- Analysis Threads tab

Events Tab

The Events tab contains the Timeline chart, which displays the number of events at various times throughout the day.

The following table describes the features of the Events tab.

Feature	Description
Time Range drop-down menu	This menu offers different options for the time range shown on the graph. You can choose a custom time range by selecting **Custom** and choosing a start and end date from the drop-down menus.

Feature	Description
Plot area	Each type of event is represented by a different color on the graph. You can zoom in on sections of the graph by clicking and dragging to select the section you want to see closer.
Event Type key	At the bottom of the tab, the types of events shown in the plot area are displayed, with their respective line colors. For example, the Network line is green, and the On Demand line is purple. To disable any of the options from appearing in the chart, click the option. It is grayed out and its line is removed from the graph.

Analysis Threads Tab

Malware Analysis is capable of analyzing many files simultaneously, each represented by a thread. Each file goes through a linear process when it is analyzed:

1. Network meta analysis
2. Request file from Decoder
3. Static
4. Community (if enabled)
5. Sandbox (if enabled)

This tab gives you the status of each thread to see where the file is currently residing in the analysis process. Thread statuses are sorted by the type of file analysis, which is the method in which Malware Analysis received the file, such as a Network session, Manually Uploaded file, or an On Demand scan.

This is useful particularly for finding which part of analysis is the limiting factor for time. For example, you might go to the tab and see all 20 threads Requesting Files from NextGen. This means the Decoder is having problems or is overwhelmed, and cannot deliver quickly.

If threads have not updated their status for long periods of time, it may indicate that Malware Analysis is stuck.

The following table provides descriptions of the list columns.

Column	Description
Last Updated	The most recent date and time when the thread updated.
Session Id	The ID number of the session.
Status	The status of the file analysis.
File Name	The name of the file being analyzed.
File Hash	The hash of the file being analyzed.

Services System View

This topic introduces features and functions of the Services System view.

The Services System view provides a services summary for Security Analytics Core services and some other services, for example Reporting Engine.

The summary information for Security Analytics Core services (Broker, Concentrator, Decoder, and Log Decoder) is similar, including information about:

- Service
- Appliance Service
- Service user information
- Host user information
- License information
- Session information

The toolbar for Security Analytics Core services is also similar. The options provide a way to run command-line host tasks, control services and hosts, and other service-specific tasks such as uploading packet capture or log files to a service.

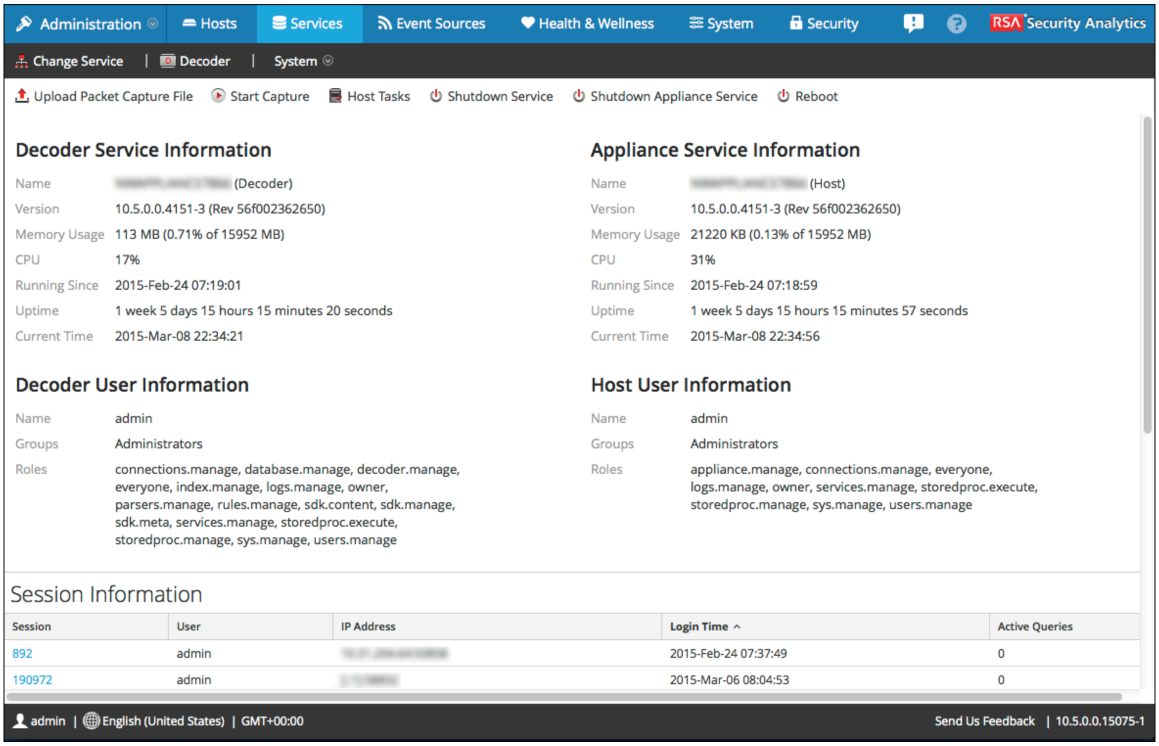
To access the Services System view:

1. In the **Security Analytics** menu, select **Administration > Services**.

   The Administration Services view is displayed.

2. Select a service and select ⚙ > **View> System**.

The following is an example of the Services System view for a Decoder.



Decoder Service Information

Name	[redacted] (Decoder)
Version	10.5.0.0.4151-3 (Rev 56f002362650)
Memory Usage	113 MB (0.71% of 15952 MB)
CPU	17%
Running Since	2015-Feb-24 07:19:01
Uptime	1 week 5 days 15 hours 15 minutes 20 seconds
Current Time	2015-Mar-08 22:34:21

Appliance Service Information

Name	[redacted] (Host)
Version	10.5.0.0.4151-3 (Rev 56f002362650)
Memory Usage	21220 KB (0.13% of 15952 MB)
CPU	31%
Running Since	2015-Feb-24 07:18:59
Uptime	1 week 5 days 15 hours 15 minutes 57 seconds
Current Time	2015-Mar-08 22:34:56

Decoder User Information

Name	admin
Groups	Administrators
Roles	connections.manage, database.manage, decoder.manage, everyone, index.manage, logs.manage, owner, parsers.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Host User Information

Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Session Information

Session	User	IP Address	Login Time ^	Active Queries
892	admin	[redacted]	2015-Feb-24 07:37:49	0
190972	admin	[redacted]	2015-Mar-06 08:04:53	0

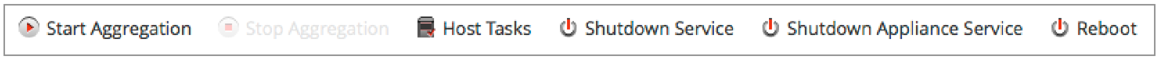
Features

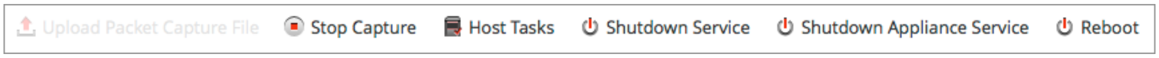
This section describes common features for Security Analytics Core service types.

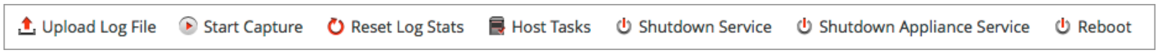
- Features specific to Brokers and Concentrators are described in the **Services System View - Broker** topic in the *Broker and Concentrator Configuration Guide*.
- Features specific to Decoders and Log Decoders are described in Decoder Services System View.

Services System View Toolbar

At the top of the Services System view is a toolbar. While some options in the toolbar apply to a specific service type, four options are common to all. The examples below show the options for a Concentrator, for a Decoder, and for a Log Decoder.







This table describes the Services System View toolbar options common to all Core services.

Action	Description
Host Tasks	Displays the Host Task List dialog, which provides a way to run command-line host tasks from a selection list. See Host Task List Dialog for detailed information.
Shutdown Service	Shuts down and restarts the service for a Decoder, Log Decoder, Broker, or Concentrator.
Shutdown Appliance Service	Stops all services running on the host, then shuts down and restarts the appliance service for a Log Decoder, Log Decoder, Broker, or Concentrator.
Reboot	Shuts down and restarts the host on which the Core services are running.

Services Summary Information

The top section of the Services System view summarizes information about the selected service. This applies to all Core service types: Decoders, Brokers, Concentrators, and Log Decoders.

Category	Description
Service and Appliance Service Information	This Includes the service name, service version, memory usage in megabytes, memory usage as a percentage of total memory, the time and date the service started running, the duration of time the service has been running, and the current time.
Service and Host User Information	Displays users who have access to this service and the user role to which they belong.
License Information	Displays the computer ID for the service and the licenses installed for that ID. • In Security Analytics 10.1 and later, the license information is the license key provided for the service by the Security Analytics local license server. • In Security Analytics 10.0, each license has an expiration date and some have other parameters such as maximum storage on system.

Session Information Grid

The bottom section of the Services System view provides a list of active sessions. In this view, you can:

- End a session
- End an active query

This table describes the Session Information grid columns.

Category	Description
Session	The ID for the session. Clicking the session ID displays a dialog with the option to kill the session. You can approve the action or cancel the action.
User	The name of the session owner.
IP Address	The IP address of the service where the session is running.
Login Time	The time the user logged in.
Active Queries	The count of active queries. Clicking a non-zero count displays a dialog in which you can stop execution of a query.

Topics

- Host Task List Dialog
- Decoder Services System View

Host Task List Dialog

This topic introduces the Services System view > Host Task List dialog.

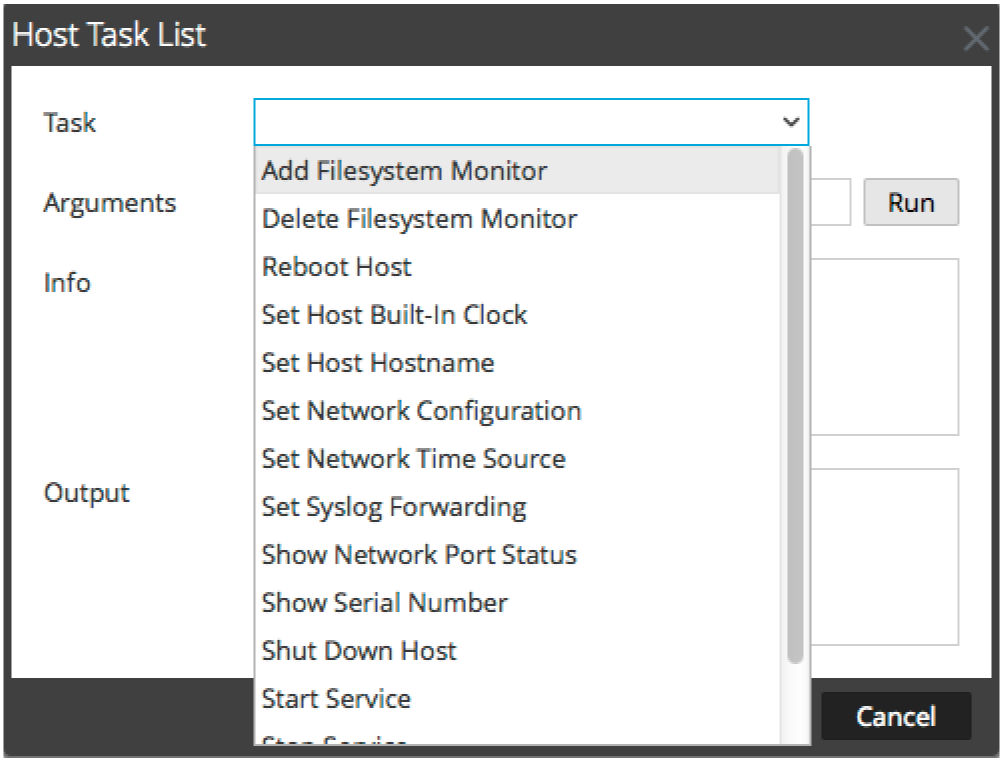
In the RSA Security Analytics Services System view, you can use the Host Tasks option to manage tasks that relate to a host and its communications with the network. Several service and host configuration options are available for Core services.

To access the Host Tasks dialog:

1. In the **Security Analytics** menu, select **Administration >Services**.
2. Select a service and select ⚙ > **View> System**.

   The System View for the service is displayed.

3. In the **Services System view** toolbar, click **Host Tasks**.
   The Host Task List dialog is displayed. The **Task** list offers a list of supported messages for the associated host.



Features

The table below describes the dialog features.

Field	Description
Task	An entry field in which you type or select a message for a Core host. When you click in this field a drop-down list of available host tasks is displayed.
Arguments	An entry field in which you enter the arguments, if any, for the message.
Run	Executes the task and arguments in the entry fields.
Info	Information about the message purpose and syntax.
Output	The output or result of an executed task.
Cancel	Closes the Host Task list dialog.

Host Task Selection List

These tasks are displayed as a drop-down list in the Task field. The available options are regulated by the security role required to execute the option.

Task	Description
Add Filesystem Monitor	Starts monitoring the storage services attached to the specified filesystem (see Add and Delete a Filesystem Monitor.
Delete Filesystem Monitor	Stops monitoring the storage services attached to the specified filesystem (see Add and Delete a Filesystem Monitor).
Reboot Host	Shuts down and restarts the host (see Reboot a Host).
Set Host Built-in Clock	Sets the host local clock (see Set Host Built-In Clock).
Set Host Hostname	This method of changing the hostname is deprecated in Security Analytics 10.6; replaced by the procedure described in Change the Name and Hostname of a Host
Set Network Configuration	Sets network address parameters (see Set Network Configuration).

Task	Description
Set Network Time Source	Sets the clock source for this host (see Set Network Time Source).
Set Syslog Forwarding	Enables or disables syslog forwarding from a remote server to the selected service (see Set Syslog Forwarding).
Show Network Port Status	Shows the network interface information for a host (see Show Network Port Status).
Show Serial Number	Gets the host serial number (see Show Serial Number).
Shut Down Host	Shuts down the physical host and the host remains off (see Shut Down Host).
Start Service	Starts a service on this host (see Stop and Start a Service on a Host).
Stop Service	Stops a service on this host (see Stop and Start a Service on a Host).
setSNMP	Enables or disables the SNMP service on a host (see Set SNMP).

Decoder Services System View

This topic introduces features in the System view that pertain specifically to Decoders and Log Decoders.

A Log Decoder is a special type of Decoder, and is configured and managed in a similar way to a Decoder. Therefore, most of the information in this section refers to both types of Decoders. Differences for Log Decoders are noted.

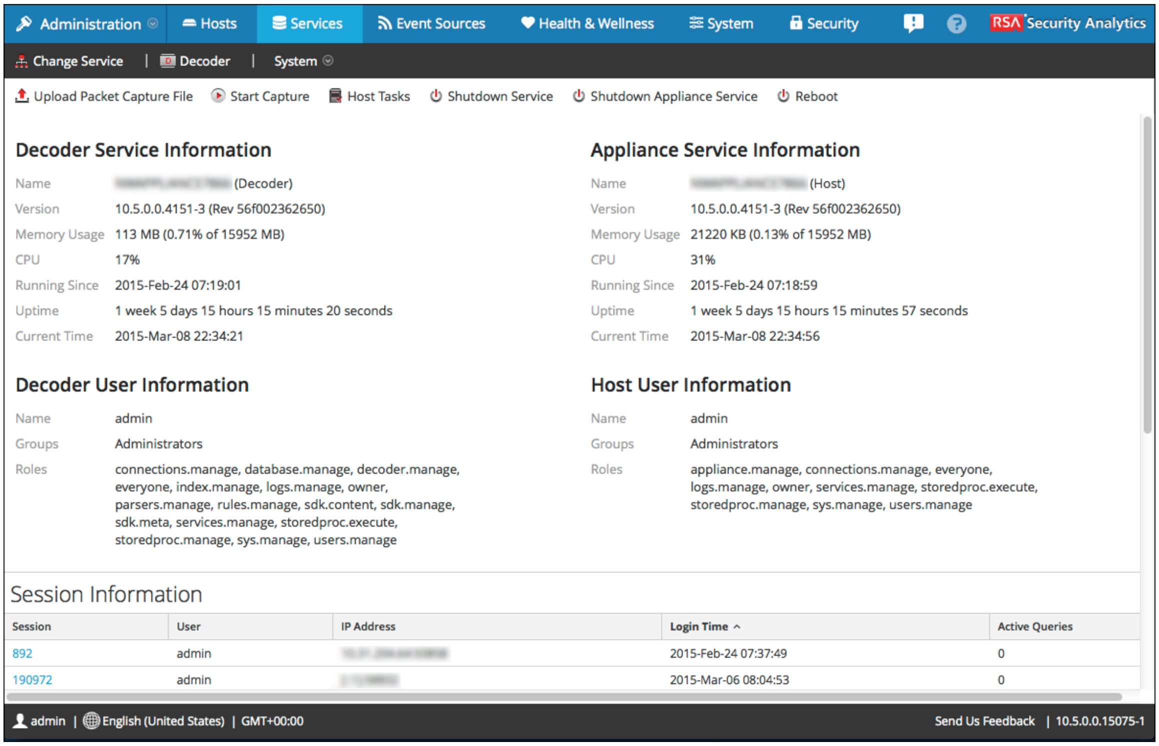
To access the Services System view for a Decoder:

1. In the **Security Analytics** menu, select **Administration** > **Services**.

   The Administration Services view is displayed.

2. Select a service and select ⚙ ⌄ > **View**> **System**.

The following figure shows an example of the Services System view for a Decoder.



Decoder Service Information

Name	[redacted] (Decoder)
Version	10.5.0.0.4151-3 (Rev 56f002362650)
Memory Usage	113 MB (0.71% of 15952 MB)
CPU	17%
Running Since	2015-Feb-24 07:19:01
Uptime	1 week 5 days 15 hours 15 minutes 20 seconds
Current Time	2015-Mar-08 22:34:21

Appliance Service Information

Name	[redacted] (Host)
Version	10.5.0.0.4151-3 (Rev 56f002362650)
Memory Usage	21220 KB (0.13% of 15952 MB)
CPU	31%
Running Since	2015-Feb-24 07:18:59
Uptime	1 week 5 days 15 hours 15 minutes 57 seconds
Current Time	2015-Mar-08 22:34:56

Decoder User Information

Name	admin
Groups	Administrators
Roles	connections.manage, database.manage, decoder.manage, everyone, index.manage, logs.manage, owner, parsers.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

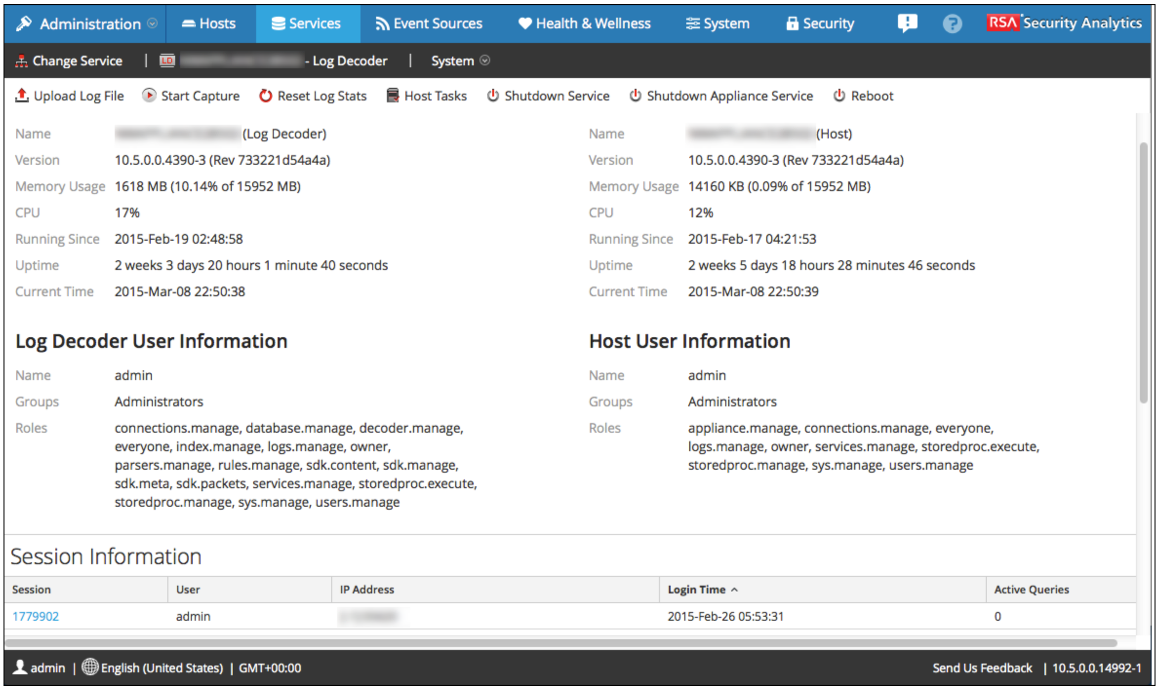
Host User Information

Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Session Information

Session	User	IP Address	Login Time ^	Active Queries
892	admin	[redacted]	2015-Feb-24 07:37:49	0
190972	admin	[redacted]	2015-Mar-06 08:04:53	0

The following figure shows the Services System view for a Log Decoder.



Name	[redacted] (Log Decoder)	Name	[redacted] (Host)
Version	10.5.0.0.4390-3 (Rev 733221d54a4a)	Version	10.5.0.0.4390-3 (Rev 733221d54a4a)
Memory Usage	1618 MB (10.14% of 15952 MB)	Memory Usage	14160 KB (0.09% of 15952 MB)
CPU	17%	CPU	12%
Running Since	2015-Feb-19 02:48:58	Running Since	2015-Feb-17 04:21:53
Uptime	2 weeks 3 days 20 hours 1 minute 40 seconds	Uptime	2 weeks 5 days 18 hours 28 minutes 46 seconds
Current Time	2015-Mar-08 22:50:38	Current Time	2015-Mar-08 22:50:39

Log Decoder User Information

Name	admin
Groups	Administrators
Roles	connections.manage, database.manage, decoder.manage, everyone, index.manage, logs.manage, owner, parsers.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, sdk.packets, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Host User Information

Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Session Information

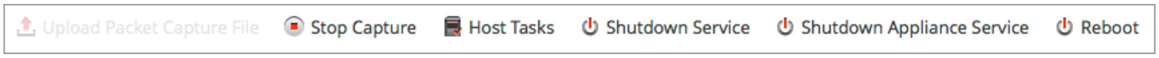
Session	User	IP Address	Login Time ^	Active Queries
1779902	admin	[redacted]	2015-Feb-26 05:53:31	0

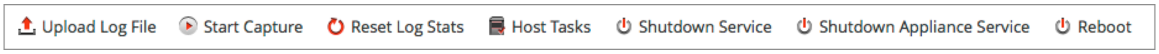
admin | English (United States) | GMT+00:00 Send Us Feedback | 10.5.0.0.14992-1

Features

Services Info Toolbar

The following toolbars show the options specific to Decoders and Log Decoders.





In addition to the common options in the Services System viewServices System View toolbar, you can start and stop capture of packets or logs. The upload file options are different for the standard Decoder (packet capture file) and the Log Decoder (log file).

Action	Description
Upload Packet Capture File	Displays a dialog that provides a way to select a packet capture (.pcap) file for upload to the selected Decoder. For more information, see the **Upload Packet Capture File** topic in the *Decoder and Log Decoder Configuration Guide*. **Note:** This option does not apply to Log Decoders.

Action	Description
Upload Log File	Displays a dialog that provides a way to select a log (.log) file for upload to the selected Log Decoder. For more information, see the **Upload Log File to a Log Decoder** topic in the *Decoder and Log Decoder Configuration Guide*.
Start/Stop Capture	Starts packet capture on the selected Decoder. When packet capture is in progress, the option in the toolbar changes to Stop Capture, and the option to upload a file is unavailable.

Services System View

This topic introduces features and functions of the Services System view.

The Services System view provides a services summary for Security Analytics Core services and some other services, for example Reporting Engine.

The summary information for Security Analytics Core services (Broker, Concentrator, Decoder, and Log Decoder) is similar, including information about:

- Service
- Appliance Service
- Service user information
- Host user information
- License information
- Session information

The toolbar for Security Analytics Core services is also similar. The options provide a way to run command-line host tasks, control services and hosts, and other service-specific tasks such as uploading packet capture or log files to a service.

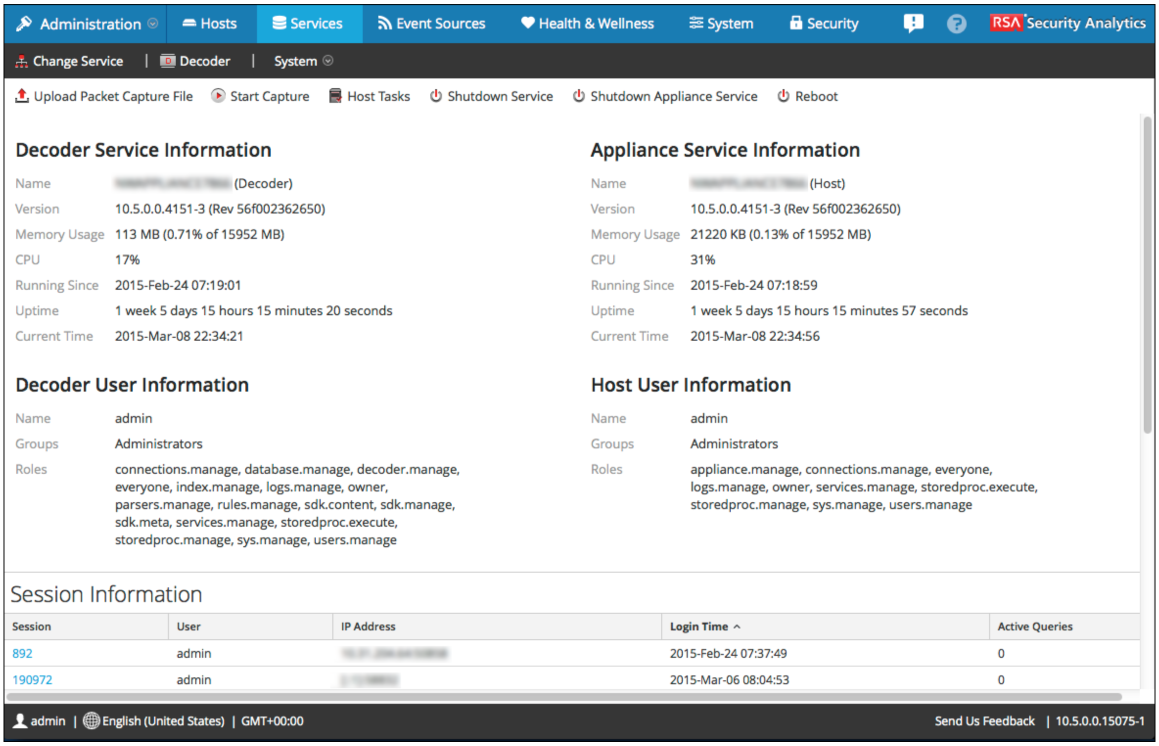
To access the Services System view:

1. In the **Security Analytics** menu, select **Administration > Services**.

   The Administration Services view is displayed.

2. Select a service and select ⚙ ⌄ > **View> System**.

The following is an example of the Services System view for a Decoder.



Decoder Service Information

Name	[redacted] (Decoder)
Version	10.5.0.0.4151-3 (Rev 56f002362650)
Memory Usage	113 MB (0.71% of 15952 MB)
CPU	17%
Running Since	2015-Feb-24 07:19:01
Uptime	1 week 5 days 15 hours 15 minutes 20 seconds
Current Time	2015-Mar-08 22:34:21

Appliance Service Information

Name	[redacted] (Host)
Version	10.5.0.0.4151-3 (Rev 56f002362650)
Memory Usage	21220 KB (0.13% of 15952 MB)
CPU	31%
Running Since	2015-Feb-24 07:18:59
Uptime	1 week 5 days 15 hours 15 minutes 57 seconds
Current Time	2015-Mar-08 22:34:56

Decoder User Information

Name	admin
Groups	Administrators
Roles	connections.manage, database.manage, decoder.manage, everyone, index.manage, logs.manage, owner, parsers.manage, rules.manage, sdk.content, sdk.manage, sdk.meta, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Host User Information

Name	admin
Groups	Administrators
Roles	appliance.manage, connections.manage, everyone, logs.manage, owner, services.manage, storedproc.execute, storedproc.manage, sys.manage, users.manage

Session Information

Session	User	IP Address	Login Time ^	Active Queries
892	admin	[redacted]	2015-Feb-24 07:37:49	0
190972	admin	[redacted]	2015-Mar-06 08:04:53	0

admin | English (United States) | GMT+00:00
Send Us Feedback | 10.5.0.0.15075-1

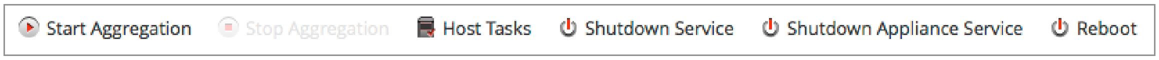
Features

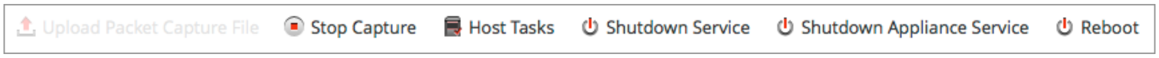
This section describes common features for Security Analytics Core service types.

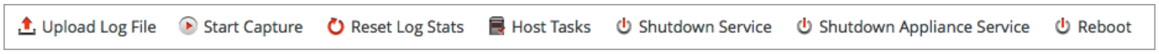
- Features specific to Brokers and Concentrators are described in the **Services System View - Broker** topic in the *Broker and Concentrator Configuration Guide*.
- Features specific to Decoders and Log Decoders are described in Decoder Services System View.

Services System View Toolbar

At the top of the Services System view is a toolbar. While some options in the toolbar apply to a specific service type, four options are common to all. The examples below show the options for a Concentrator, for a Decoder, and for a Log Decoder.







This table describes the Services System View toolbar options common to all Core services.

Action	Description
Host Tasks	Displays the Host Task List dialog, which provides a way to run command-line host tasks from a selection list. See Host Task List Dialog for detailed information.
Shutdown Service	Shuts down and restarts the service for a Decoder, Log Decoder, Broker, or Concentrator.
Shutdown Appliance Service	Stops all services running on the host, then shuts down and restarts the appliance service for a Log Decoder, Log Decoder, Broker, or Concentrator.
Reboot	Shuts down and restarts the host on which the Core services are running.

Services Summary Information

The top section of the Services System view summarizes information about the selected service. This applies to all Core service types: Decoders, Brokers, Concentrators, and Log Decoders.

Category	Description
Service and Appliance Service Information	This Includes the service name, service version, memory usage in megabytes, memory usage as a percentage of total memory, the time and date the service started running, the duration of time the service has been running, and the current time.
Service and Host User Information	Displays users who have access to this service and the user role to which they belong.
License Information	Displays the computer ID for the service and the licenses installed for that ID. • In Security Analytics 10.1 and later, the license information is the license key provided for the service by the Security Analytics local license server. • In Security Analytics 10.0, each license has an expiration date and some have other parameters such as maximum storage on system.

Session Information Grid

The bottom section of the Services System view provides a list of active sessions. In this view, you can:

- End a session
- End an active query

This table describes the Session Information grid columns.

Category	Description
Session	The ID for the session. Clicking the session ID displays a dialog with the option to kill the session. You can approve the action or cancel the action.
User	The name of the session owner.
IP Address	The IP address of the service where the session is running.
Login Time	The time the user logged in.
Active Queries	The count of active queries. Clicking a non-zero count displays a dialog in which you can stop execution of a query.

Topics

- Host Task List Dialog
- Decoder Services System View

Troubleshooting Host Updates

This section contains instructions on how to troubleshoot Host updates.

It lists pre-update conflicts, update errors, and log messages that can occur when you update a host It also proves the cause for conflicts, update errors, and log messages and how to resolve them.

Topics

- Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors
- Troubleshooting 10.6 Update Service Log Messages

Troubleshooting 10.6 Pre-Update and Update Warnings, Conflicts, and Errors

This section contains the 10.6.0 Hosts View pre-update check and update error messages with a description of each message and instructions on how to respond to these messages.

Pre-Update Warnings

Pre-Update warnings are anomalies or potential issues in your current configuration that do not prevent you from updating to the new version. If Security Analytics encounters a potential issue, it displays Update warning. View details in the **Status** column of the Hosts view. Click on **View details** to display the full message.

Warning Message	**Pre-Update Warning** Please review the following prior to updating. 1. **Kernel version on the host is older than the version 2.6.32-504.1.3 supported by Security Analytics. If you click Begin Update kernel version 2.6.32-504.1.3 will be installed on the host.** 2. **After updating to 10.6.0.0, correlation rules written in deprecated syntax may cause Concentrator to start in a failed state. Rules that match the strict formatting do not cause this issue.** **For more information, see the Security Analytics 10.6 online help topic "Rule and Query Guidelines"**
Cause	1. The CentOS kernel on the host is older than the kernel supported by the update version you chose. 2. If this host is a Concentrator and it starts in a failed state, you may have correlation rules written using deprecated syntax. **Note: Current Status** displays the current Security Analytics/Operating System version of the host before updating to 10.6.
Recommended	1. Click **Begin Update** in the warning dialog to install the supported kernel.

Action	2. Make sure that your correlated rules conform to strict formatting as described in the **Rule and Query Guidelines** topic in the *Archiver Configuration Guide*.

Pre-Update Conflicts

Pre-Update conflicts are issues in your current configuration or your Local Update Repository that prevent you from updating to the new version. If Security Analytics encounters:

- Incompatible configuration settings, it displays Update conflict. View details in the **Status** column.
- Problems downloading the version update files, it displays Download error. View Details in the **Status** column.

For additional information on Local Update Repository, see the **Populate Local Update Repository** topic in the *System Maintenance* guide.

Conflict Message	**Downloading Error** Failed to download because of the following errors. **Error setting up repositories: Cannot retrieve repository metadata (repomd.xml) for repository: SA. Please verify its path and try again.**
Cause	Security Analytics cannot connect to the Live Update Repository from which RSA distributes version updates from the RSA Live Update Repository through your Live connection.
Recommended Action	Make sure that you: 1. Set up Live Services. For more information, see the **Set Up Live Services on Security Analytics** topic in the *Live Services Management* guide. 2. Selected the **Connect to Live Update Repository** checkbox in the **Administration** > **System** > **Updates** tab.

Download Error Message	**Downloading Error** Failed to download because of the following errors. **Local Update Repository does not have valid updates. See Populate Local Update Repository for instructions on how to get valid**

	updates.
Cause	Security Analytics did not find the version update that you selected in your Local Update Repository.
Recommended Action	Review the instructions on how to Populate Local Update Repository and try to populate your Local Repository with the desired update version. See the **Populate Local Update Repository** topic in the *System Maintenance* guide. If you cannot remediate this conflict after reviewing these instructions, contact Customer Care.

Conflict Message	**Pre-Update Check Error** Cannot start the Update. Resolve the following errors and try again. **File system check failed** **Insufficient space in `/var/lib/rabbitmq` partition.** **Used space for this partition should be less than 80%.** **Current Status: *`percentage-used`*%**
Cause	Messages are accumulating in the`/var/lib/rabbitmq` partition.
Recommended Action	Investigate why the messages are accumulating in the partition and resolve this issue. If you cannot resolve this issue, contact Customer Care.

Conflict Message	**Pre-Update Check Error** Cannot start the Update. Resolve the following errors and try again. **Kernel version on the host is newer than the version 2.6.32-504.1.3 supported by Security Analytics.** Contact Customer Care
Cause	You cannot update to the version you chose because the kernel version on the host is newer than version 2.6.32-504.1.3 supported by Security Analytics for that version.

Recommended Action	Contact Customer Care to resolve the issue.

Conflict Message	**Update Path Not Supported** The update path to *selected-update-version* is: • *version-range* • *version-range* • . • . • . **Caution:** 1. If you are running version 9.8, please contact Customer Care for update instructions. 2. If you are running 10.3.x, you must update to 10.4.1 before you can update to 10.6.x.x. See the *RSA Security Analytics 10.4.1 Upgrade Guide* on SCOL (https://knowledge.rsasecurity.com/) for detailed instructions on updating from 10.3.x to 10.4.1 (If you use Event Stream Analysis in 10.3.x, you must migrate your rules to 10.4.1). **You cannot access the 10.4.1 update RPMs from the Live Update Repository. This means that you must download the 10.4.1 update RPMs from SCOL.**
Cause	The version on the host is not supported as an update path for the update version you chose.
Recommended Action	Update the host to a supported path.

Update Errors

Update errors are errors that stop the update process. If Security Analytics encounters an update error, it displays Update error. View details in the **Status** column of the Hosts view. Click on **View details** to display one of the following update error dialogs:

Error Message	**System did not receive expected response**
Cause	Security Analytics cannot identify the Host status because a **/var/lib/puppet/state/agent_catalog_run.lock** file exists on the Host. When the Puppet agent is running, it creates a lock file called **agent_catalog_run.lock**. Occasionally, this lock file is present on the Host, even though the Puppet agent is not running.
Recommended Action	Try one of the following actions to resolve the error: • Remove the **/var/lib/puppet/state/agent_catalog_run.lock** from the Host. • Check the time on the non-Security-Analytics-Server hosts and the Security Analytics Server Host and make sure that they are in sync. • Try the update again at another time. If it fails, contact Customer Care to resolve the issue.

Troubleshooting 10.6 Update Service Log Messages

This section contains the Security Analytics 10.6 pre-update, update, and post-update log messages with a description of each message and instructions on how to respond to these messages.

System Management Service (SMS)

SMS logs are posted to `/var/log/install/sms_install.log` on the SA host.

Java Version

Message	*timestamp host*: SMS_PostInstall: WARN: Java Keystore file /opt/rsa/carlos/keystore is missing
Cause	The Java keystore is missing.
Required Action	Make sure that Java v1.8 is installed on the host.

Messages	*timestamp host*: SMS_PostInstall: INFO: Installed Java version is : java version "1.7.0_71" *timestamp host*: WARN: Java version is old and not compatible with the current SMS server.
Cause	Java version that installed on the host is not compatible with Security Analytics 10.5.1.
Required Action	Make sure that Java v1.8 is installed on the host.

Disk Space

Message	*timestamp host*: SMS_PostInstall: INFO: Free disk space on /opt is *n*GB *timestamp host*: SMS_PostInstall: WARN: Disk space check

	`failed on /opt. The available disk space `*`n`*`GB is less than the recommended minimum disk space of 10GB.`
Cause	Low or insufficient disk space allocated for the SMS service.
Required Action	RSA recommends that you provide a minimum of 10 GB of disk space for the SMS service to run optimally.

Services

Message	*`timestamp host`*`: INFO RabbitMQ server is not installed.`
Cause	The required `RabbitMQ` service is **not** installed.

Required Action	Install and restart the RabbitMQ service using the following commands.
	`yum install rabbitmq-server`
	`service rabbitmq-server restart`

Message	*`timestamp host`*`: INFO RabbitMQ Server is not running.`
Cause	The required `RabbitMQ` service is **not** running.
Required Action	Restart RabbitMQ service using the following commands. `service rabbitmq-server restart`

Message	*`timestamp host`*`: INFO TokuMX Server is not running.`
Cause	The required `TokuMX` service is **not** running.
Required Action	Restart TokuMX service using the following commands. `service tokumx-server restart`

Message	*`timestamp host`*`: SMS_PostInstall: INFO: Puppet Server is`

	`not running.`
Cause	The required `Puppet` service is **not** running.
Required Action	Restart Puppet service using the following commands. `service puppet-server restart`

Log Collector Service (nwlogcollector)

Log Collector logs are posted to `/var/log/install/nwlogcollector_install.log` on the host running the `nwlogcollector` service.

Lock Box Verification Logs

Message	`timestamp.NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: The lockbox stable value threshold was not met because the system fingerprint has changed. To reset the system fingerprint, open the lockbox using the passphrase.`
Cause	The Log Collector Lockbox failed to open after the update.
Required Action	Log in to Security Analytics and reset the system fingerprint by resetting the stable system value password for the Lockbox as described in the **Reset the Stable System Value** topic under the **Configure Lockbox Security Settings** topic in the *Log Collection Configuration Guide*.

Message	`NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: Lockbox tampering was detected, so it cannot be read.` `NwLogCollector_PostInstall: Lockbox Status : Failed to open lockbox: Lockbox tampering was detected, so it cannot be read.`
Cause	The Log Collector Lockbox was compromised.
Required	Log in to Security Analytics and reconfigure the Lockbox as

Action	described in the **Configure Lockbox Security Settings** topic in the *Log Collection Configuration Guide*.

Message	*`timestamp`* `NwLogCollector_PostInstall: Lockbox Status : Not Found`
Cause	The Log Collector Lockbox is not configured after the update.
Required Action	(Conditional) If you use a Log Collector Lockbox, log in to Security Analytics and configure the Lockbox as described in the **Configure Lockbox Security Settings** topic in the *Log Collection Configuration Guide*.

Message	`timestamp: NwLogCollector_PostInstall: Lockbox Status : Lockbox maintenance required: The lockbox stable value threshold requires resetting. To reset the system fingerprint, select Reset Stable System Value on the settings page of the Log Collector.`
Cause	You need to reset the stable value threshold field for the Log Collector Lockbox.
Required Action	Log in to Security Analytics and reset the stable system value password for the Lockbox as described in **Reset the Stable System Value** topic under the **Configure Lockbox Security Settings** topic in the *Log Collection Configuration Guide*.

Event Stream Analysis (ESA)

Pre-Update Check

Pre-update check ESA logs are posted to`/var/log/esa-rpm-pre-upgrade.log` on the host running the ESA service.

Message	`Pre_upgrade_alert_count=`*`number-of-alerts`*

Cause	Tells you the number of ESA alerts that exist on the host when you initiate the update.
Required Action	None (Informational)

Message	`Pre_upgrade_rule_count=`*`number-of-rules`*
Cause	Tells you the number of ESA rules that exist on the host when you initiate the update.
Required Action	None (Informational)

Message	`Pre_upgrade_enrichment_connection_count=`*`number-of-enrichment-sources`*
Cause	Tells you the number of ESA enrichment sources that exist on the host when you initiate the update.
Required Action	None (Informational)

Post-Update Check

Post-update check ESA logs are posted to`/var/log/esa-rpm-post-upgrade.log` on the host running the ESA service.

Message	`Post_upgrade_alert_count=`*`number-of-alerts`*
Cause	Tells you the number of ESA alerts that exist on the host after the host is updated.
Required Action	None (Informational)

Message	`Post_upgrade_rule_count=`*`number-of-rules`*
Cause	Tells you the number of ESA rules that exist on the host after the host is updated.
Required Action	None (Informational)

Message	`Post_upgrade_enrichment_connection_count=`*`number-of-enrichment-sources`*
Cause	Tells you the number of ESA enrichment sources that exist on the host after the host is updated.
Required Action	None (Informational)

Reporting Engine Service

Update Check

Reporting Engine Update logs are posted to to`/var/log/re_install.log` file on the host running the Reporting Engine service.

Message	*`timestamp`*` : Available free space in /home/rsasoc/rsa/soc/reporting-engine [ `*`existing-GB`*` ] is less than the required space [ `*`required-GB`*` ]`
Cause	Update of the Reporting Engine failed because you do not have enough disk space.
Required Action	Free up the disk space to accommodate the required space shown in the log message. See the **Add Additional Space for Large Reports** topic in the *Reporting Engine Configuration Guide* for

	instructions on how to free up disk space.