Security Analytics 8.2.1-55066 Release Notes

Table of Contents

..... 3
Introduction..... 4
New Features..... 5
Upgrade Instructions..... 10
Issues Addressed..... 14
Known Issues..... 15
Resources..... 16

Copyright

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom.

Copyright ©2020 Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Introduction

Symantec Security Analytics is a sophisticated network forensic device that delivers full network visibility, advanced network forensics, and real-time content inspection for all network activity.

New Features

OAuth Support

This release includes preview support for version 2.0 of the Open Authentication standard, OAuth. Details on OAuth can be found here: https://oauth.net/2/.

> **NOTE**
>
> This feature is listed as a preview feature in this release. OAuth 2.0 support in Security Analytics has been configured, tested, and verified to function in Windows ADFS environments with Implicit Grant Flow and Authorization Grant Flow authorization workflows. If your organization uses OAuth with a different authentication back-end, please reach out to your sales point of contact or Symantec support to submit a request to support additional deployment types.

Configure OAuth on Security Analytics

1. Log in to the Web UI.
2. Click **Settings** > **Authentication**.
3. Check **Enable OAuth**.
4. Define your OAuth server address in the **Server** field.
5. Define the client_id for the OAuth application server in the **Client ID** field.
6. (Optional) Define your ADFS **Resource** URL.
7. Click **Save**.

Proceed to **Settings** > **Users and Groups** to add the roles defined on the OAuth server by adding them to the LDAP Groups for the corresponding SA Group.

See Configure OAuth for User Authorization and Authentication for additional configuration details.

New Menu

All menu items in the Web interface have been moved from the ellipsis (hamburger) menu to a sidebar for easier and more succinct access. The new menu features hover-over tooltips, adaptive scaling based on the browser size, and the ability to right-click an option (or control-click on a Mac) to open a specific menu item in a new browser tab or window.

The new menu layout includes the following main sections:

Analyze

The Analyze menu contains all options for data analysis. This reworked menu groups logical sections together and adds the most commonly used analysis pages to reduce the number of clicks required to reach them.

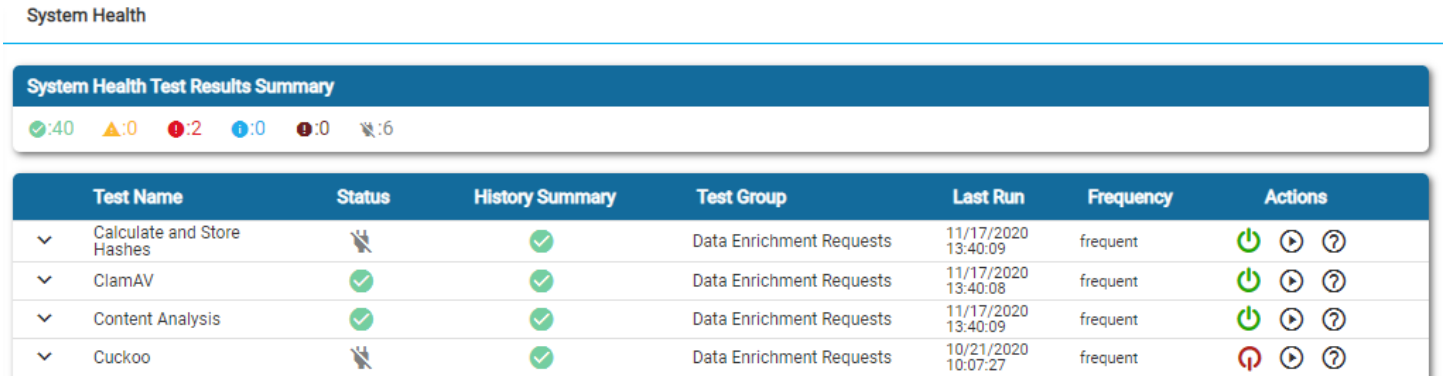
Capture

The Capture menu includes the familiar Summary and Import PCAP options, but adds the **Watch Folders** feature, where you can configure monitoring of a network location for new capture data.

System Health

The System Health menu provides access to familiar sections for **Network**, **Data Sizes**, and **Storage**, and also provides access to the new item, **Tests**.

The **Tests** page includes a summary of all system health tests, their status history, and associated test data. It also provides options for managing each service.



See System Healthfor more details.

Settings

The Settings menu includes the same list of items as in previous releases.

Help

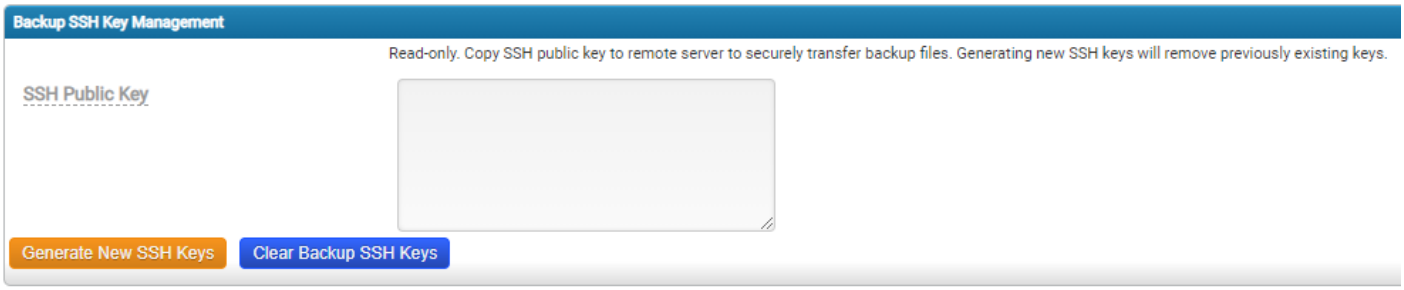
The help icon takes you directly to a page with information on contacting to the Symantec support team, accessing the support knowledge base and documentation sites, or to load the Security Analytics on-box help.

Automated Configuration Backup and Restore

Building on previous CLI functionality, this release introduces the option in the Web UI to perform backup and restore tasks. Now you can archive your system configuration to a remote server, enable regularly scheduled updates of that backup, and restore your system configuration from the Web UI.

Configure an Automated Backup of your configuration:

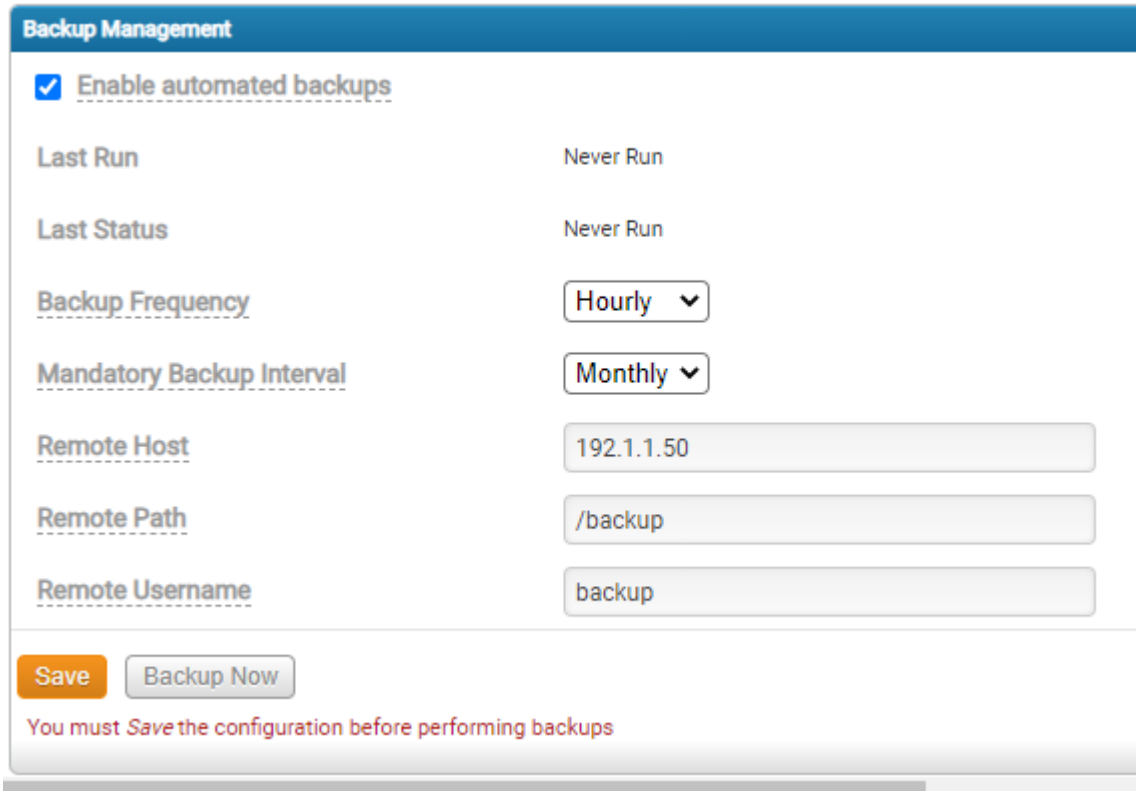
1. Browse to **Settings** > **System**.
2. Under Backup SSH Key Management, click **Generate New SSH Keys**.



Copy the generated key and install it on the SSH server to which you'll be saving backups.
Consider the following as you install the keys on your SSH server:

- Permissions for the remote home directory `~`, `~/.ssh` directory and the `~/.ssh/authorized_keys` file on the remote machine must be writable only by the user: `rwx------` and `rwxr-xr-x` are acceptable permission levels, but `rwxrwx---` is not.
- Permissions on the remote `~/.ssh/authorized_keys` file must be set to readable (at least 400), but also writable (600) if you intend to write additional keys to that file.

3. Under **Backup Management**, set the frequency for your backups.

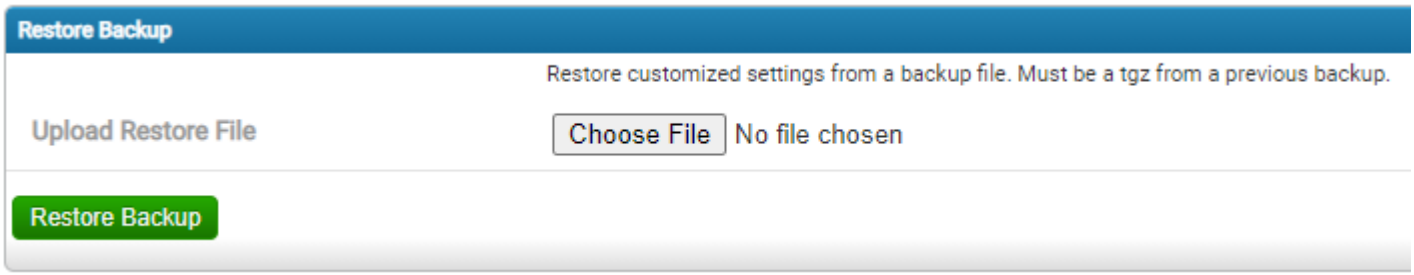


   Backup Frequency and Mandatory Backup Interval options will take effect after your initial successful backup.
   a. **Backup Frequency** sets how often the system will check for updates to your configuration. If there are any, a new backup will be captured and stored on the SSH server.
   b. **Mandatory Backup Interval** sets how often the system will back up the configuration even when no changes have been made.
4. Define your server host and path in the appropriate fields. The username field is provided for test cases where an SSH key is not shared.
5. Click **Save** to commit any pending system configuration changes.
6. Click **Backup Now** to create your first backup.

From that moment forward, additional backups are performed based on your frequency and interval settings.

Restore

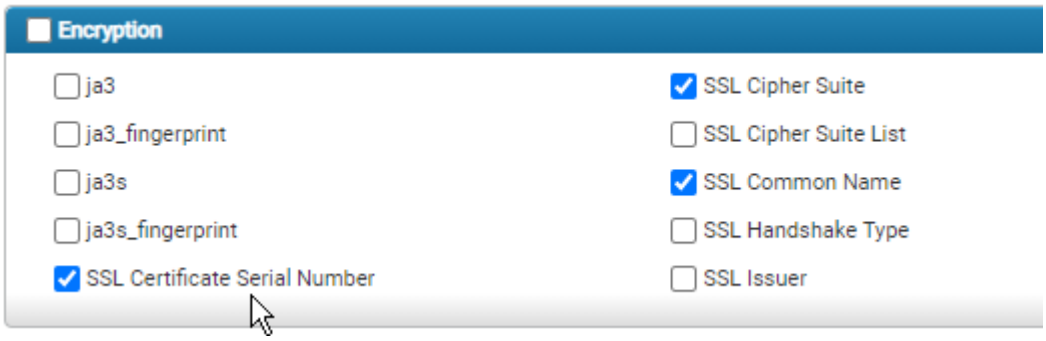
To restore your configuration, click **Choose File** to browse your system or network for the appropriate configuration file.



Support for JA3 and Community ID

JA3 is a Transport Layer Security (TLS) fingerprinting method used to identify malicious encrypted communications. With this support, you can now configure Security Analytics to validate **JA3 fingerprints** against abuse.ch's (https://abuse.ch/) public SSL Blacklist database to identify malicious traffic.

Configure JA3 metadata in the Web UI under **Settings** > **Metadata** > **Encryption**. Once enabled, a restart is required.



SA provides the following four JA3 attributes:

- JA3 (client side signature)
- JA3s (server side signature)
- JA3_fingerprint (the MD5 hash of the JA3–aka the client-side fingerprint)
- JA3s_fingerprint (the MD5 hash of the JA3s string–aka the server-side fingerprint)

> **NOTE**
> JA3 fingerprints are not available in the Extraction UI. If SA is behind an SSL-V service, the JA3 fingerprint components would be SSL-V certificate based rather than the external source. If SA is not behind an SSL-V service the encrypted traffic would yield no extractions. Thus, Extraction support is not necessary.

Community ID version 1 is a flow hash that overcomes weaknesses in using simple flow tuples. You may find **Community ID flow identifiers** to be more useful than SA's flow IDs or tuples when pivoting from one dataset to another.

Configure monitoring and reporting for Community ID metadata in the Web UI under **Settings** > **Metadata** > **Network Layer**.

NOTE
Indicators, rules, and alerting are not supported for Community ID since these flow IDs are only used for reference. Community ID is supported for reporting, filtering, and Session View.

Deprecation Notices

- After this release, support for Instant Messenger Extractions will no longer be available.

Behavioral Changes

- Time/Date format in raw.tsv.

In Security Analytics version 8.0.3 and earlier, the raw.tsv timestamp format was **seconds:nanoseconds**, as seen here:

```
#slot_id  element_id  flow_id       start_time

20761720 4199        753827699495  1577994239:605353218
```

In 8.1.1 and 8.2.1, the raw.tsv format is entirely different. From Security Analytics 8.1.1 and later, ra.tsv uses the International date format (ISO), which uses the sequence **YYYY-MM-DD**. This format appears as follows:

```
#slot_id  element_id  flow_id       start_time
 5091030  2454        21475266796   2020-01-30_14:49:33.277455129-0700
```

Upgrade Instructions

This section details the steps to upgrade your Security Analytics appliances - both your Central Manager Console (CMC) and the individual sensor appliances in your network.

Security Analytics 8.x employs a unique file system from 7.x. As a result, upgrading from SA 7.x to 8.x will remove all packet data on your sensors' disks, and all current metadata will either need to be migrated to the new file system or purged before the upgrade. Upgrading from 8.0.x to 8.1.x does not require this consideration.

CAUTION
Before you proceed, ensure that all SA appliances in your network have the same time. A divergence of ninety seconds or more can result in your sensors failing to connect to your CMC post-upgrade. Time and date settings are available in the UI, under **Menu** > **Settings** > **Date/Time**.

Upgrade the Central Manager Console (CMC)

Any time you upgrade your infrastructure, it's critical that you start with the CMC. This ensures that, when complete, all appliances in your SA infrastructure speak the same language.

1. Retrieve the upgrade file:
   a. For **7.x > 8.2.1**: From the CMC 's web user interface, click the cog wheel in the top-right and select **Upgrade**. The web ui shows the available upgrade version and your configured source. The web ui shows a download progress bar as the file is retrieved from the upgrade server.
   b. For **8.x > 8.2.1**: From the CMC's web user interface, click the ellipsis (hamburger) menu in the top left, and select **Upgrade**. Click the up arrow to the far right of the upgrade details page to retrieve the upgrade file. The web ui shows a download progress bar as the file is retrieved from the upgrade server.
2. Once the download is complete, click Initiate **Upgrade**. The web ui displays a window with the potential upgrade version.
3. Click **Continue** to confirm and proceed with staging the upgrade.
4. When the upgrade preparations are complete, the system prompts you to click **Reboot** to complete the upgrade. The CMC restarts with the new version of Security Analytics.

CAUTION
While metadata can be preserved during the upgrade from 7.x to 8.1.x, doing so will significantly increase the time it takes to upgrade your sensor appliances. In some cases, the upgrade can take several days to complete when existing metadata is present on disk during the upgrade. To avoid these delays, see **Reformatting the Index Volumes** for steps to purge the content on your sensors' disks prior to the upgrade.

Current Version	Upgrade Path	Commen
8.0.x, 8.1.x	8.2.1	Standard upgrade; no data is erased.
7.3.5, 7.3.6	8.2.1	All captured packet data is erased; metadata is retained
7.3.2	NSR-53 - 7.3.6 > 8.2.1	The NSR-53 patch is required prior to upgrade from 7.3.2 to 7.3.6. All captured packet data is destroyed during the upgrade to 8.2.1; metadata is retained
7.3.1	7.3.6 > 8.2.1	All captured packet data is erased during the upgrade to 8.2.1; metadata is retained

Current Version	Upgrade Path	Commen
7.2.x	7.3.1 - 7.3.6 > 8.2.1	All captured packet data is erased during the upgrade to 8.2.1; metadata is retained
All Virtual Appliances	none	All Virtual Appliances require a fresh install.

Further Considerations

- Although metadata and settings will be preserved when upgrading from versions 7.3.1–7.3.x, all packet data will be overwritten. See Preserving Capture Data.
- The migration of metadata from 7.x to 8.x will take many hours, and in some cases a day or more, depending on the volume of metadata. See Reformatting the Index Volumes to mitigate the upgrade time.
- You cannot upgrade virtual appliances from 7.x to 8.x.
- You cannot revert a virtual appliance from 8.x to 7.x.

Preserving Capture Data

To preserve your packet data from 7.x, Symantec recommends that prior to upgrade you do one or both of the following:

- Save the PCAPs that you want to keep on an external device.
- Install 8.x on another appliance to which you can migrate data from the 7.x appliance.

Use the CLI command, dsmigrate.sh to transfer capture data from a 7.x appliance or external device to an 8.x appliance. Instructions for using dsmigrate.sh are in the Help Files under **Reference > CLI Commands > dsmigrate**.

Reformatting the Index Volumes

Use this method to delete all indexing data (metadata). This procedure will destroy all of your indexing metadata but will also speed up the upgrade process.

1. Identify the volume for each metadata file system by running df -h. The metadata file systems will be listed as /var/lib/solera/metaX, for example:
   ```
   /dev/sdb1 9.6T 315M 9.1T 1% /var/lib/solera/meta1
   /dev/sdb2 9.6T 78M 9.1T 1% /var/lib/solera/meta2
   ```
2. Run the CLI command, scotus stop to stop all services and unmount capture and indexing volumes.
3. Verify that the indexing volume was unmounted by looking for the message umount /var/lib/solera/metaX. Rundf -h to make sure/var/lib/solera/metaX is not visible. If the volume did not unmount, runumount /var/lib/solera/metaX for each mounted file system.

   If the volume still fails to unmount, a working directory from a CLI session may be occupying the file system. Runlsof -n -P | grep var/lib/solera/meta to search for a corresponding PID. Terminate the process and then attempt to unmount the volume again.
4. Is this a sensor with Fibre Channel–attached storage?

- **Yes**–Go to Sensor with Fibre Channel–attached storage.
- **No**—Go to All other sensor configurations.

Sensor with Fibre Channel–attached storage

1. Runvi /etc/fstab and look for the metadata file systems, designated as/var/lib/solera/meta1,/var/lib/solera/meta2, etc. The readout should appear similar to the example below, which shows two metadata file systems:
   ```
   /dev/mapper/360080e500043d30400001cf95c6c009e1 /var/lib/solera/meta1 ext4
   noauto,data=writeback,barrier=0,noatime,nodiratime,commit=20,nouser_xattr,nosuid 1 2
   dev/mapper/360080e500043b1600000155f5c6bfbef1 /var/lib/solera/meta2 ext4
   noauto,data=writeback,barrier=0,noatime,nodiratime,commit=20,nouser_xattr,nosuid 1 2
   ```

2. Runmkfs on each metadata file system, for example:
```
mkfs.ext4 -q -T largefile /dev/mapper/360080e500043d30400001cf95c6c009e1
mkfs.ext4 -q -T largefile /dev/mapper/360080e500043b1600000155f5c6bfbef1
```

All other sensor configurations

1. Run `vi /etc/fstab` and look for the metadata file systems, designated as `/var/lib/solera/meta1` , `/var/lib/solera/meta2` , etc. The readout should look something like the example below, which shows two metadata file systems:
```
LABEL=DSINDEX1 /var/lib/solera/meta1 ext4
noauto,data=writeback,barrier=0,noatime,nodiratime,commit=20,nouser_xattr,nosuid 1 2
LABEL=DSINDEX2 /var/lib/solera/meta2 ext4
noauto,data=writeback,barrier=0,noatime,nodiratime,commit=20,nouser_xattr,nosuid 1 2
```
2. Runmkfs for each file system/volume, for example:
```
mkfs.ext4 -q -T largefile -L DSINDEX1 /dev/sdb1
mkfs.ext4 -q -T largefile -L DSINDEX2 /dev/sdb2
```

Upgrade the Sensors

1. Retrieve the upgrade file:
   a. For **7.x > 8.2.1**: From the sensor's web user interface, click the cog wheel in the top-right and select **Upgrade**. The web ui shows the available upgrade version and your configured source. The web ui shows a download progress bar as the file is retrieved from the upgrade server.
   b. For **8.x > 8.2.1**: From the sensor's web user interface, click the ellipsis (hamburger) menu in the top left, and select **Upgrade**. Click the up arrow to the far right of the upgrade details page to retrieve the upgrade file. The web ui shows a download progress bar as the file is retrieved from the upgrade server.
2. Once the download is complete, click Initiate **Upgrade**. The web ui displays a window with the potential upgrade version.
3. Click **Continue** to confirm and proceed with staging the upgrade.
4. When the upgrade preparations are complete, the system prompts you to click **Reboot** to complete the upgrade. The sensor restarts with the new version of Security Analytics.

Compatibility

> **WARNING**
> Security Analytics management traffic (onbond0) cannot be subjected to SSL intercept. If your Security Analytics appliance is deployed behind SSL-intercept devices such as Symantec SSL Visibility Appliance, ProxySG, or a next-generation firewall, you must configure those devices to exclude traffic from the Security Analytics management interface.

Licensing Security Analytics

Security Analytics license keys are available from the Solera licensing portal, which if your appliance has Internet access, it can reach directly - follow the steps labelled Appliance with Internet Access. If not, follow the steps labelled Appliance without Internet Access.

1. Log in to the web UI with these credentials:admin |Solera
2. On the *`Initial Configuration`* page, input the requested information and click **Save**.

3. The *License Details* dialog is displayed. Does your Security Analytics appliance have access to the Internet (license.soleranetworks.com port 443)?

Yes — Follow the instructions in *Appliance with Internet Access*.	No — Follow the instructions in *Appliance without Internet Access*.

Appliance with Internet Access

1. Under *Retrieve License*, input the **License Key** and click **Send Request**.
2. As applicable, select the desired license type.
3. The appliance sends the license key and the license seed file to the license server, which generates the appropriate license file (license.tgz) and returns it to the appliance, which automatically reboots.
4. Once the system has rebooted, select **Settings > About > License Details** to verify that the items are correct.
5. Click **Download** to create an archive copy of the license file (license.tgz). Store this file in a safe location that is not on the appliance.

Appliance without Internet Access

1. Click **Download DS Seed** to download the seed file (dsseed.tgz) to your workstation.
2. On a workstation that has Internet access, go to license.soleranetworks.com .
3. Enter your license key as username and password, upload dsseed.tgz, and click **Update**.
4. As applicable, select the desired license type and click **Update**.
5. Save the license file (license.tgz) to your workstation.
6. Return to the *License Details* dialog.
7. Click **Browse** and select license.tgz.
8. The license is uploaded and the appliance automatically reboots.
9. Once the system has rebooted, select **Settings > About > License Details** to verify that the items are correct.
10. Click **Download** to create an archive copy of the license file (license.tgz). Store this file in a safe location that is not on the appliance.

Issues Addressed

Security Analytics 8.2.1 addresses the following issues:

- **SADEV-2393** - IM Extractions: Artifact Timeline. As noted in the deprecations section of this release note, the IM Extractions Artifact Timeline will be removed in the next release.
- **SADEV-2960** - The system time changes following upgrade to SA 8.2.1.
- **SADEV-2985** - Two `solera-restartauditd*` services are in a failed state.

Other Issues

In addition to the issues listed above, issues in the following categories have been resolved:

- 14 Security and Vulnerability Issues
- 11 Capture, DPI, and Data Enrichment Issues
- 15 API and UI Issues
- 30 Utilities and Other/Miscellaneous Issues

Customers with a current support contract who have specific questions may request additional details under non-disclosure agreement.

Known Issues

The Security Analytics engineering team are aware of the following issues in this release.

- **SADEV-2119** - Login Correlation Service (LCS) installation fails to check for existing, older installations.
  - **Workaround**: Before initiating the installation of LCS, check to see if LCS is already installed. If it is, uninstall it before installing the latest version.
- **SADEV-3323** - When deploying SA on Azure, a new ssh key is generated during the first reboot. This renders the initial ssh key obsolete.
  - **Workaround**: When installation is complete, ssh to the appliance as root using the appropriate password to obtain the new ssh key.
- **SADEV-2333** - When the **Enable Radius** check is enabled, the LDAP configuration option, **Use Radius for Authentication** is disabled.
- **SADEV-2376** - In rare cases, DNS rebind can intermittently exhibit unexpected behavior where capitalized hostnames are involved.
- **SADEV-392** - Advanced filter by subject does not find multi-word subjects.
- **SADEV-3380** - Restart the appliance whenever the time of day is manually changed.
- **SADEV-3328** - Attempting to edit a user that was added by the OAUTH login generates an error. There is no impact.

Resources

Consult these resources for assistance with your Security Analytics implementation:

- Sign up for a Broadcom support account, so you can log support cases and access the support knowledge base: https://www.broadcom.com/support/symantec/getting-started.
- All Security Analytics documentation: http://techdocs.broadcom.com/content/broadcom/techdocs/us/en/symantec-security-software/web-and-network-security/security-analytics/8-1.html
- Broadcom Support Site: https://support.broadcom.com/security

Symantec™
A Division of Broadcom