

# EXHIBIT 4

## Sky Advanced Threat Prevention New Features

---

This document describes the new features introduced in Sky Advanced Threat Prevention.

Please refer to the [Supported Platforms Guide](#) for feature support on various SRX Series devices.

### January 2018

- **Download STIX Reports**—You can now download a STIX report from the HTTP File Download page. STIX and TAXII are an open community-driven effort of specifications that assist with the automated exchange of threat information. This allows threat information to be represented in a standardized format for sharing and consuming. Sky ATP uses this information as well as other sources. View this report from **Monitor > File Scanning > HTTP File Download**. Click on the **File Signature** link to reach the **Details** page.
- **Threat Intelligence Sharing**—Using the TAXII service, Sky ATP can contribute to STIX reports by sharing the threat intelligence it gathers from file scanning. Enable TAXII from **Configure>Global Configuration>Threat Sharing**.
- **Operations for Multiple Infected Hosts**—You can now change the following settings for multiple hosts at one time: Policy Override and Investigation Status. Configure this from the new pull down options at the top of the **Monitor > Hosts** page.
- **Hash Lookup Only for Files**—When creating a device profile here **Configure > File Inspection Profiles**, you can now select to only do a hash file lookup. Instead of the file, a sha256 hash of the file is sent for matching against known malware.
- **Proxy Servers**—You can now add trusted proxy server IP addresses to Sky ATP. When you add trusted proxy servers IP addresses to the list in Sky ATP, by matching this list against the IP address in an HTTP header (X-Forwarded-For field) for a request sent from an SRX Series device, Sky ATP can determine the originating IP address of the request. Configure this through **Configure > Proxy Servers**.

### November 2017

- **IMAP Email Scanning**—Sky ATP now supports IMAP email management. Enrolled SRX devices transparently submit potentially malicious email attachments to the cloud for inspection. Once an attachment is evaluated, Sky ATP assigns the file a threat score between 0-10 with 10 being the most malicious. Configure this through the **Configure > Email Management > IMAP** window.

### October 2017

- **External threat feeds**—You can now enable external feeds for integration with Sky ATP through the **Configure > Threat Intelligence Feeds** window. For each feed, click the Details link to view information, including the contents of the feed. For more information, see the GUI online help.
- **Download malware files**—A Download Zipped File option lets you download quarantined malware (as a password-protected zip file) for analysis. You can access this option from both the Email attachment scanning details page and the HTTP file download details page. For more information, see the GUI online help.

### September 2017

- **Password reset**— If you forget your password to login to the Sky ATP dashboard, you can reset it when you click Forgot Password from the Sky ATP login screen. An email with a link for resetting your password is sent to the address associated with your account. For more information, see the GUI online help.
- **Feed-based URL redirection**—The set services security-intelligence profile CLI command now has a feed-name option that lets you perform an action based on feeds, such as URL redirection. For more information, see [set services security-intelligence](#).

### May 2017

- Basic (threat feeds only) license—A basic service level is available and adds filters using the following threat feed types: Command and Control, GeolIP, custom filtering and threat intel feeds. With the basic license, there is no file processing or advanced malware protection.
- Customer feedback—An option is available on the toolbar for providing feedback to improve the product usability.
- IP Filter Open APIs—APIs to update the IP Filter feeds. See [Threat Intelligence Open API Setup Guide](#) for more information.
- Infected Host Open APIs—APIs to update the infected host feeds. See [Threat Intelligence Open API Setup Guide](#) for more information.
- MAC address—For use by Policy Enforcer customers, this field (in the Host Details page) displays the host MAC address.
- Editable host identifier— Sky ATP will generate and assign an identifier to the host that is editable in the Host Details pages. Any change to the host identifier will be reflected in the C&C Server Details page, Host details page, and File Scanning Details page.

### April 2017

- Logging—Logging options are now available in the Global Configuration window (**Configure > Global Configuration**) to configure syslog event types.
- License expiration—A column is added to the Enrolled Devices table that displays the license expiration date for that device.
- C&C Blocked by—A Blocked Via column is added to the C&C Servers window (**Monitor > C&C Servers**) that displays the feed name that blocked that server.

### March 2017

- SMTP E-Mail attachments—An E-Mail Management window is added to the Configure menu to inspect and management e-mail attachments sent over SMTP. See the [Supported Platforms Guide](#) for information on supported platforms.
- File Scan details—The Behavior Analysis tab now shows a Behaviors by Severity illustration to provide a quick overview of what the malware is targeting.
- File Scan details—A Behavior Details tab is added to the File Scan details page, providing information on what the file did when it was opened in the sandbox.
- Printable View—A Printable View link is added to the File Scan details page, allowing you to print the general and network activity information to a PDF file or to a local or network printer.

### February 2017

- Windows 10 support—Sandboxing now supports the Windows 10 operating system. See the [Supported Platforms Guide](#) for information on supported OS versions.

### January 2017

- File Scan details—Enhancements have been made to the file scan details page, providing more details on the threat and network activity.

### December 2016

- SYSLOG support—Malware and host status SYSLOG messages are now created. See the [Supported Platforms Guide](#) for information on supported versions of JSA and QRadar SIEM.
- URL-based lists—Support for both URL-based and IP-based C&C, blacklist and whitelists.
- Security Director 16.1 support—Sky ATP now supports SD 16.1 and later releases. For more information on using Sky ATP in SD, see the SD online help.

**November 2016**

- Android file types—Android operating system, and the APK (Android application package) file type are now supported.

**October 2016**



- C&C server details—Click an IP address in the C&C servers table (**Monitor > C&C Servers**) to view more information about that C&C server, such as hosts that have contacted that server, associated domains, etc.
- New platform support—Junos OS Release 15.1X49-D65 now supports Sky ATP running on SRX4100 and SRX4200. See the [Supported Platforms Guide](#) for a complete list of supported platforms.

**September 2016**

- New platform support—Junos OS Release 15.1X49-D60 and later releases support Sky ATP running on the SRX340, SRX345 and SRX550M devices and vSRX instances, in addition to existing support for SRX1500, SRX5400, SRX5600 and SRX5800 devices.
- Reporting false positives—An option to report false positives and false negatives is added to the file scanning details page and to the C&C page.
- RESTful APIs—RESTful APIs are now available to provide:
  - Custom feed support for C&C
  - Custom whitelists and blacklists for malware detection.
  - Hash submission and file submission.

**July 2016**

- Hide number of rows—Tables (for example, File Scanning and Hosts) no longer display the number of returned rows at the bottom of the table.
- File scanning table updates—Select **Monitor > File Scanning**. The following changes have been made:
  - Threat level legend—A color-coded threat level legend is added to the top of the file scanning table to easily identify the threat levels of files listed in the table.

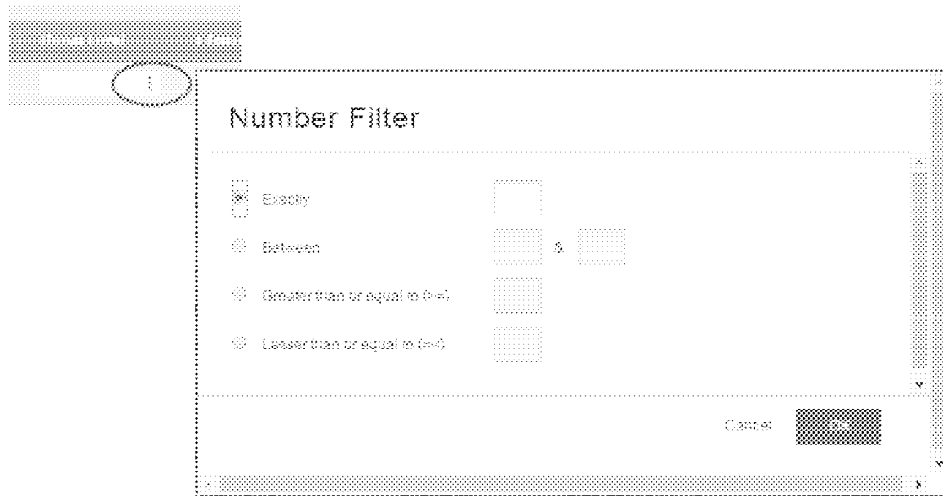
Threat level:  High  Medium  Low  None/clean

- Hide scans with lower threat level—By default, only files with a threat level of 4 or higher are now displayed in the file scanning table. To view all files, click **Clear All** located in the upper-right corner of the table or click the close icon (x) next to threat\_level ge 4. To return to the default view, click **File Scanning** in the left pane to refresh the window.



- Rename Device Serial Number —Click a file signature to view file scanning details. In the Hosts That Have Downloaded File table, the *Device Serial Number* column is changed to *Device Name*. Clicking a device name in the table continues to show details of that particular device.

- Filter by threat level—A numeric filter has been added to allow you to display rows by threat level. This option is also available in the Hosts table (Select **Monitor > Hosts**) for the Threat Level, C&C Hits, and Malware Hits columns.



- Policy override for this host menu—Select **Monitor > Hosts** and then click a host in the table to view detailed host information. The *Blocking setting for this host* pulldown menu is changed to *Policy override for this host*, and the new options are:
  - Use configured policy (included in infected host feeds)
  - Always include host in infected host feeds
  - Never include host in infected host feeds
- Reorder host details page—When you view detailed host information (select **Monitor > Hosts** and then click a host in the table), the current threat table is now reordered to show the most recent event at the top of the table.

#### June 2016

- Manually upload files for inspection—You can now manually upload suspicious files to the cloud for malware inspection. For more information, see the Web GUI tooltips (click the question marks (?) to view the tooltips) and online Help.
- Download file scanning activity—A report of scanned files and their results can be downloaded to an Excel spreadsheet. For more information, see the Web GUI tooltips (click the question marks (?) to view the tooltips) and online Help.
- Support for SRX5400, SRX5600, and SRX5800—Junos OS Release 15.1X49-D50 and later releases support Sky Advanced Threat Prevention running on SRX5400, SRX5600 and SRX5800 devices.
- Full support for IDP and Sky Advanced Threat Prevention—Full support for Sky Advanced Threat Protection inline blocking and IDP configured together in the same security policy is provided in Junos OS Release 15.1X49-D50 and later releases.
- Additional command & control information—The Web GUI C&C page now lists the external server hostname and the category for which the server is classified as a C&C server.
- Efficacy improvements.