

# Junos<sup>®</sup> WebApp Secure 5.0.0-10

## (formerly Mykonos)



Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
408 745 2000 or 888 JUNIPER  
[www.juniper.net](http://www.juniper.net)  
April, 2013

## Contents

Junos® WebApp Secure 5.0.0-10.....	1
(formerly Mykonos).....	1
Installing and Deploying Junos WebApp Secure .....	3
Update Notes.....	3
Noteworthy Changes Introduced in Release 5.0.0-10 .....	3
Known Issues and Limitations Fixed in Release 5.0.0-10 .....	4
Known Issues and Limitations with 5.0.0-10 .....	4
Junos Spotlight Secure Integration .....	4
SRX Integration .....	4
New User Interface.....	5
New Configuration System.....	5
Role Based Access Control.....	5
Search Engine Handling.....	5
Logging Enhancements.....	5
Radius Authentication Support.....	5
REST API .....	6
Requesting Technical Support .....	6

For additional information about Junos WebApp Secure, please refer to the *JWAS User Guide* and *JWAS Developer Guide*.

## Installing and Deploying Junos WebApp Secure

The installation procedure for Juniper Networks® Junos® WebApp Secure (JWAS) remains the same. As soon as the update is available to the customer, it will be downloaded by the system automatically if the system is connected to the JWAS Support System.

Please contact JWAS support to access to the VM ESX version of the JWAS 5.0 or an update package.

### Update Notes

Due to changes in the Web UI SSL Certificate and Web UI Session Management, an update from any previous version will appear to hang, despite the update actually completing successfully. The manifestation and workaround is slightly different depending on what mode your system is running in.

- In a High Availability or Clustered setup, the update status will hang after the first node is updated and the failover process completes. Typically, this is at around the 20% mark.
- In a Standalone system, the update status will hang after the update is complete.

In either case, to recover, users should first hit the 'refresh' button in their browser, re-accept the SSL certificate, and re-login to the UI.

In a High Availability setup, the update will likely still be running. If the UI reflects this fact after you have re-logged in, no further intervention is required, and the update should complete successfully.

After logging in, if your system is running in the Standalone mode, or if the UI progress bar is captioned "DOWNLOADING FILES (UNDEFINED/UNDEFINED)", you must SSH into the system and run the "sudo /etc/init.d/mykonos-pyro restart" command or the "restart mykonos-pyro" command from within the "services" context of the CLI.

## Noteworthy Changes Introduced in Release 5.0.0-10

- Spotlight integration - Junos Spotlight Secure is a cloud-based global attacker intelligence solution that will identify individual attackers at the device level (versus the IP address), track them in a global database, and share them globally with security devices. Spotlight Secure is a licensable feature. Please contact your local Juniper sales representative for details on how to acquire licenses for Spotlight Secure
- SRX Integration - The SRX series by Juniper is an enterprise-level Secure Gateway for networks. Junos WebApp Secure now has the ability to integrate with this solution and prevent high volume tools from being handled at the firewall level. Specifically JWAS can send IPs to the SRX to achieve a block (or other configurable response) at the gateway level.
- New user interface – Security Monitor and Configuration UI are now a single optimized interface, with new user preferences, multiple skins, improved navigation and performance improvements. Note: With an upgrade to 5.0 customers no longer need to have port 8080 open for JWAS Security Monitor. Since it has been merged with Configuration into a single interface – port 5000 is enough.
- Configuration CLI – All configuration tasks can now be executed from either the UI or dedicated command line interface.
- Role-based Access Control – This allows assignment of specific system rights based on pre-defined roles. Users can be assigned to one or more groups allowing for finer access control to JWAS management.
- Search engines handling – Non-standard behavior of some search engines (notably Google and Bing) will no longer trigger false positives in Junos Web App Secure.
- Cleaner log separation – Logs are separated by type and configured for local and remote logging. In addition a new security log for all security related events has also been created making it easier for integration with SIEM tools.
- **mykonos** user password restore – if mykonos user password lost it can be reset to the original state of the system upon reboot.

- Radius - Authentication via connections to Radius servers is now supported.

## Known Issues and Limitations Fixed in Release 5.0.0-10

- Upgrade process has been improved to handle slower connections with higher latency. The process now downloads software in parts, and if the download process fails for any reason – it will resume where it stopped
- Additional LB options (Sticky session and IP hash) were added to JWAS's load balancing to address prior deployments limitations in load balanced environments
- HTML pages with a lot of white space (between tags, in comments) could cause excessive CPU usage and in some case deadlock when processed
- In cases where user loses “mykonos” account password, they can now reset the mykonos user password at reboot; given this hash support staff can recover user's password in the support system
- Database Cleanup services can cause internal excessive load on the system adding significant latency to processing traffic
- Several areas of the documentation were out of date
- OpenSSL security vulnerability [http://www.openssl.org/news/secadv\\_20130204.txt](http://www.openssl.org/news/secadv_20130204.txt) (855712)
- In some cases of customer's web-sites requiring large file upload JWAS would enforce a limit which would break the upload (844074)

## Known Issues and Limitations with 5.0.0-10

- In certain cases after update download has finished the new package will not be shown on the Update screen automatically misleading a customer that the download failed; the customer will simply need to refresh the page – it show be visible after that.
- In an HA pair, when a manual failover is triggered through the UI, the user may encounter a 500 error. This is not an indication of an incomplete failover; it is simply a problem with the UI. If encountered, customers should re-login to the UI

## Junos Spotlight Secure Integration

- Juniper Networks Junos Spotlight Secure is a cloud-based global attacker intelligence solution that will identify individual attackers at the device level (versus the IP address), track them in a global database, and share them globally with security devices. The product will create a persistent fingerprint of attacker devices based on more than 200 unique attributes to deliver precision identification and blocking of attackers without false positives that could impact valid users. Once an attacker is identified and fingerprinted on a subscriber's web application using JWAS the new global attacker intelligence service will immediately share the attacker profiles with other subscribers, providing advanced real-time security intelligence across multiple networks. When compared with currently available reputation feeds that rely on IP addresses, Junos Spotlight Secure will offer customers more reliable security against attackers and all but eliminate false positives with its unique fingerprinting technique.
- Additional details can be found at <http://www.juniper.net/us/en/products-services/security/junos-webapp-secure/spotlight/#literature>

## SRX Integration

- Added capabilities for JWAS to issue IP level blocks on the SRX device directly, which allow for a more effective block response to a confirmed offending IP address.
- JWAS need to be configured with SRX username/password combination, commands to issue, filter name and the address of the SRX and the integration service enabled

- Compatible with SRX devices running Junos 11.4 or higher
- Tested on both virtual and hardware SRXs
- Customer must have a JWAS dedicated filter setup on SRX tied to an interface

## New User Interface

- New Look & Feel
- Improved navigation, search function, export data to PDF and RSS
- Per user preferences like skins available such as “Light”, “Dark”, “Juniper”, timezone, refresh rate, etc.
- Performance and workflow enhancements
- Combined Configuration and Security Monitor into a unified interface

## New Configuration System

- Newly redesigned configuration interface completely integrated into the New interface for monitoring mentioned earlier
- CLI command line management interface, making most of the configuration scriptable over SSH connection. It is a full featured CLI that has its own help, supports auto-complete, provides in session change differences, export to file and multi-parameter edits
- Moved majority of the options from TUI into Configuration UI leaving only Network Configuration, appliance re-initialization and Send of the support bundle in the TUI

## Role Based Access Control

- Adds granular access to the management of the JWAS device.
- The following roles were added: Device Administrator, RBAC administrator, Security Administrator, Security Support Staff, Security User, Super Administrator, Web UI administrator.
- Configuration UI provides mapping of any user to the JWAS Roles. Once authenticated (LDAP/Radius), the user's permissions will be enforced based on the role(s) they are assigned.

## Search Engine Handling

- Addresses occasional identification of search engine behavior as malicious
- Added Client Classification processor which is designed to detect popular legitimate search engine bots. These types of bots are notorious for performing aggressive spider activity on websites, and often this activity can trigger security related incidents. Using this processor to define the conditions used to identify such bots, allows the system to ignore security incidents from those clients. This will remove search engine related false positives, as well as prevent errors in indexed and cached results. The popular search engines are included by default, but if additional search engines should be allowed, new rules can be created.
- The most popular search such as Google, Bing, Yandex, Archiver were added by default , however additional can be added by the customer if necessary

## Logging Enhancements

- Separated security events into their own separate log file.
- Added 2 additional security events on top of the existing incident creation: Create profile and Auto-Response.
- Added support for simultaneous remote and local logging, remove logging to multiple servers and separate log settings per log file.

## Radius Authentication Support

- Added support for Radius server
- Settings are available in the Users & Groups section of configuration

- Supports authentication only (Groups/Permissions are driven by the users to roles assignment – see Role Based Access Control feature)

## REST API

- JWAS now supports programmatic access to the data available in the monitoring UI via a REST API. The REST API offers further refinements, such as custom sort orders and date ranges not currently available in the UI itself.
- Note: No external authentication is available at present. API Consumers are therefore limited to standalone scripts that run directly on the appliance.
- Additional information is available in the Developer Guide in the JWAS Help section

## Requesting Technical Support

To open a case or to obtain support information, please visit the Juniper Networks Support Site:  
<http://www.juniper.net/support>.