

Juniper NETWORKS Release 13 Security Director Cloud Secure Edge Instructions

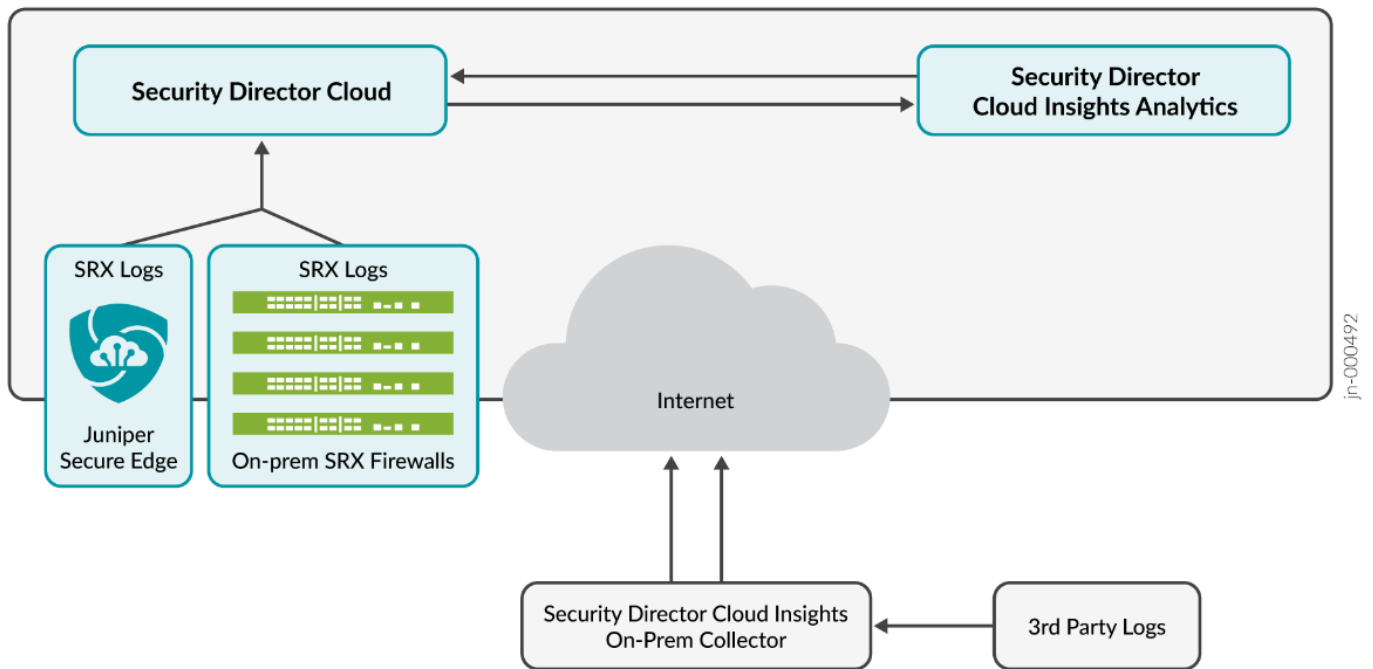
[Home](#) » [JUNIPER NETWORKS](#) » Juniper NETWORKS Release 13 Security Director Cloud Secure Edge Instructions 

Contents

- [1 Juniper NETWORKS Release 13 Security Director Cloud Secure Edge](#)
- [2 Product Information](#)
- [3 Product Usage Instructions](#)
- [4 Frequently Asked Questions](#)
- [5 Introduction](#)
- [6 What's New](#)
- [7 What's Changed](#)
- [8 Resolved Issues](#)
- [9 Upgrade and Downgrade Instructions](#)
- [10 Documents / Resources](#)
 - [10.1 References](#)



Juniper NETWORKS Release 13 Security Director Cloud Secure Edge



Product Specifications

- **Product Name:** Juniper Secure Edge CASB and DLP
- **Release Version:** 23.3
- **Release Date:** 2024-03-25
- **Managed by:** Juniper Security Director Cloud

Product Information

Juniper Secure Edge provides Firewall as a Service (FWaaS) in a single-stack software architecture managed by Juniper Security Director Cloud.

Juniper Secure Edge empowers organizations to secure their workforce wherever they are. With consistent security policies that follow the user, device, and application without having to copy over or re-create rule sets, Juniper Secure Edge makes it easy to deploy cloud-delivered application control, intrusion prevention content and Web filtering and effective threat prevention without breaking the visibility or security enforcement.

Product Usage Instructions

Deployment of Security Policies

1. Access the Juniper Security Director Cloud.
2. Configure security policies for users, devices, and applications.
3. Ensure consistent security policies are applied across the workforce.

Cloud-Delivered Application Control

1. Enable cloud-delivered application control feature in Juniper Secure Edge.
2. Configure application control settings as per organizational requirements.
3. Monitor and manage application usage through the Juniper Security Director Cloud interface.

Intrusion Prevention and Web Filtering

1. Activate intrusion prevention and web filtering capabilities in Juniper Secure Edge.
2. Set up custom rules for intrusion prevention and web filtering.
3. Regularly review and update the rules to enhance security measures.

Threat Prevention

1. Utilize the threat prevention features offered by Juniper Secure Edge.
2. Stay updated with threat intelligence feeds to enhance threat prevention capabilities.
3. Analyze threat reports generated by Juniper Security Director Cloud for proactive security measures.

Frequently Asked Questions

Q: What are the trademarks associated with Juniper Secure Edge?

A: Juniper Networks, Inc., Juniper, the Juniper logo, and Juniper Marks are registered trademarks of Juniper Networks, Inc.

Q: How can I report errors found in the document?

A: Please report any errors you find in writing to the specified contact provided in your license agreement.

Copyright and Disclaimer

- Copyright © 2024 Lookout, Inc. and/or its affiliates. All rights reserved.
- Lookout, Inc., Lookout, the Shield Logo, and Everything is OK are registered trademarks of Lookout, Inc. Android is a trademark of Google Inc. Apple, and the Apple logo and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries. App
- The store is a service mark of Apple Inc. UNIX is a registered trademark of The Open Group. Juniper Networks, Inc., Juniper, the Juniper logo, and Juniper Marks are registered trademarks of Juniper Networks, Inc.
- All other brand and product names are trademarks or registered trademarks of their respective holders.
- This document is provided under a license agreement containing restrictions on its use and disclosure and is protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means.
- The information contained in this document is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.
- This document may provide access to or information on content, products, and services from third parties. Lookout, Inc. and its affiliates are not responsible for and expressly disclaim all warranties of any kind for third-party content, products, and services. Lookout, Inc. and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Introduction

- Juniper Secure Edge provides Firewall as a Service (FWaaS) in a single-stack software architecture managed by Juniper Security Director Cloud. Juniper Secure Edge empowers organizations to secure their workforce wherever they are.
- With consistent security policies that follow the user, device, and application without having to copy over or re-create rule sets, Juniper Secure Edge makes it easy to deploy cloud-delivered application control, intrusion prevention content and Web filtering and effective threat prevention without breaking the visibility or security enforcement.
- These release notes describe new and changed features and known and resolved problems in the software.
- For details about working with product features, refer to the [Juniper Secure Edge CASB and DLP Administration Guide](#).

What's New

- You can now configure Quarantine as a policy action, enable Quarantine review, and release workflow for Salesforce API mode protection. You now have a choice to disable file downloads until the DLP and Malware scan is complete.
- For Salesforce applications, the onboarding workflow now provides an additional prompt that enables you to specify restrictions for file downloads. The Block Downloads for the security scan prompt include two options: 1) Never, and 2) Until the scan is complete. A text box is also available to provide information about any file not available for download.
- With this update, we perform Luhn check validation for Credit Card Regex patterns, even when the rule is not combined with a keyword dictionary.
- When a Google Drive label sync action fails more than twice, further sync actions stop, and administrators receive a system-generated email.

What's Changed

- We made these improvements to the User Directory sync capability using Ping Identity:
- The platform now has an API connector for Ping Identity to facilitate the User Directory sync action. After successful integration, the platform syncs the User Directory from Ping Identity periodically.
- The platform also supports SCIM functionality for Ping Identity, enabling automated user provisioning to prevent delays in user sync when you add, delete, or modify a user.
- We revamped these reports to offer enhanced data, providing deeper insights into data security.
- **Anomaly Reports:** These reports focus on the User and Entity Behavioral Analysis (UEBA) capability provided by the platform. They show anomalous user and content activity, which can indicate insider threats or potential malware or ransomware.
- **Compliance Reports:** These reports help you gain insights into your organization's compliance status and adherence to security policies.
- They show findings from observations of policy violations, users and applications involved, and remediation steps to address noncompliance issues.

Resolved Issues

- None for this release.

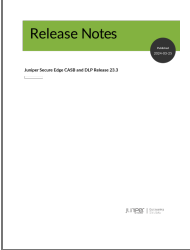
Known Issues

- None for this release.

Upgrade and Downgrade Instructions

- None for this release.

Documents / Resources

	<p>Juniper NETWORKS Release 13 Security Director Cloud Secure Edge [pdf] Instructions Release 13, Release 23.3, Release 13 Security Director Cloud Secure Edge, Release 13, Security Director Cloud Secure Edge, Director Cloud Secure Edge, Cloud Secure Edge, Secure Edge, Edge</p>
---	---

References

- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.