opentext™

Reflection for the Web Release Notes

Reflection for the Web Release Notes

13.3 SP1

Table of contents

Reflection for the Web Release Notes

June 2024

Reflection for the Web version 13.3 SP1 Update 1 (13.3.1.1) released June 2024.

What's New

Reflection for the Web has adopted a new architecture that simplifies deployment, tightens security, improves scaling and high availability, and eases ongoing maintenance. There are two new deployment options: a virtual software appliance and Linux installers.

See the Reflection for the Web Deployment Guide (page for information about how to choose the deployment option that best fits your needs.

Features and Fixes

Fixed a defect caused by a too short HTTP timeout that prevented two appliances from being clustered. (13.3.1.1)

- Updated third-party libraries, including Java, to address security vulnerabilities. (13.3.1.1)
- Personalization (p13n) has been re-introduced using the new architecture (13.3.1). See these Knowledge Base articles for more information:

  Using the Personalization Feature in Reflection for the Web (page

  Personalizing Reflection for the Web Using the SQL Plug-in (page

- Security updates including Java and third party libraries have been made. (13.3.1)

Applied security updates to address multiple CVEs. (13.3.1)

Added instructions for upgrading when using the Linux installer and updating when using the Appliance to the Deployment Guide (page under the Update section. (13.3.0.1)

- Applied security updates to address multiple CVEs. (13.3.0.1)

> 💡 **Note**
>
> To apply the most recent security updates, you must update the RWeb Launcher on client computers.

- Addressed an issue that prevented the administrative advanced Kubernetes dashboard from loading in a deployment that was not connected to the internet. (13.3.0.1)

Added strict Transport Security Headers (HSTS) to enhance security. (13.3.0.1)

SiteMinder Agent name is now automatically replicated between nodes. (13.3.0.1)

Changes in Behavior

- The SiteMinder and Single sign-on through IIS authentication methods have been deprecated and will be removed in an upcoming update release and in the next major long-term support release.

  If you use either of these methods, we recommend migrating to OIDC, Kerberos, or SAML, which are more secure and compatible with modern authentication standards. Please contact Support with any concerns regarding this change. (13.3.1.1)

- RSA key exchange cipher suites in TLS connections are deprecated and will be removed in a future release. (13.3.1)

The process for configuring X.509 authentication has changed. Please see the X.509 authentication documentation (page for the updated steps. (13.3.0.1)

- The minimum disk space requirement for the Appliance and Linux based installers has been increased from 60GB to 100GB. (13.3.0.1)

- Reflection for the Web is installed via a virtual appliance or a Linux installer. (See What's New (page 3) .)

- The configuration process for the Security Proxy, Terminal ID Manager, and Metering have changed. See the MSS documentation (page for more information. (13.3)

- Support for NTLM-based authentication has been removed and replaced with support for Kerberos. (13.3)

- Microsoft has retired Internet Explorer 11, and as such, our ability to resolve IE 11 browser-specific issues in older versions of MSS is limited. Support for IE 11 has been removed from MSS 14.0 and greater. However, we will continue to support IE 11 for older versions of MSS that currently support it, as per the Product Support Lifecycle. (13.3)

Known Issues

- When joining a node to a cluster, the node shuts down before it joins the cluster. This can result in a delay of perhaps 20 minutes. Let the process continue; it will eventually complete or error-out if there is a problem. (13.3.1)

- If the firewall status on a node changes, the pods on that node become inaccessible. Reboot the node to make the pods accessible. (13.3.1)

- Following initial installation, server node restarts, or adding new nodes to the cluster, it may take approximately 15 minutes for the cluster to stabilize and report itself as "Healthy." Numerous warning events may appear in the Cluster Management - Events view during startup. These events are part of the normal operation and will be cleared after approximately 15 minutes. **Always wait** for the cluster to be reported as healthy before proceeding with cluster operations. (13.3)

- When using the migration tool to migrate from a system with Terminal ID Manager configured, Terminal ID Manager will fail to start on the new system after migration. To work around this issue please contact Support. (13.3)

- Support for X.509 authentication through a load balancer is not currently functioning. Contact Support for more information.(13.3)

Resources

Check these online resources.

- Reflection for the Web Security updates (page

- Reflection for the Web Documentation (page :

Deployment Guide (page

Reference Guide (page , which includes API and Scripting, Using ECL, Applet Attributes and Parameters, HTML Samples, Host-initiated RCL Support

- MSS Product Documentation (page

For specific product issues, contact Customer Support (page .

Online Support Resources (page

Legal Notice

© 1998 - 2024 Rocket Software, Inc. or its affiliates. All Rights Reserved.