Change Guardian 6.2.1.1 Release Notes

September 2022

Change Guardian provides security intelligence to rapidly identify and respond to unauthorized activities of privileged users that indicate a security breach or compliance gaps. Change Guardian helps security teams to detect and respond to potential threats in real-time. The Change Guardian server has been deployed in SaaS environment and an on-premises forwarder is used to manage agents and configure policies.

Change Guardian 6.2.1.1 release includes new features, security fixes, and usability improvements. Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us to ensure that our product meets all your needs.

The documentation for this product is available on the Micro Focus website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the Change Guardian Documentation page. To download this product and patches, see the Micro Focus Downloads website.

What is New?

The following sections outline the key features and functions provided by this version, as well as issues resolved in this release:

Change Guardian SaaS Deployment

As a part of Change Guardian deployment in SaaS environment, the following features have been introduced:

- **Deployment of Regional and Master server**: A regional server is deployed to collect event data from the regions that are on premises and a master server is deployed to provide a consolidated view of event data across all the regions.
- **Script based Deployment of Infrastructure and Change Guardian Server**: Users can configure communication between the Change Guardian Server and Connectors using scripts.

- **Regional Server Load Balancing**: Regional server load balancing enables the even distribution of the incoming event data. It processes and creates a balance within the flow of data between the deployed regional servers.
- **Backup and Disaster Recovery**: Users can backup the event data on cloud and restore the data during a system failure.

For more information, see Change Guardian in SaaS.

Federated View of Events

- Change Guardian has provisioned a federated view of the event data from regional servers to the master server.
- The users can view all the events collectively from a particular region by grouping the regional servers.

Forwarding Event Data to Cloud

Users can send event data from the Forwarder to the cloud layer by configuring integrators at the Forwarder level.

Performance Improvement Tweaks

The performance of Change Guardian has been enhanced and improvised to process additional number of agents and increased inflow of data.

Forwarder Communication through Proxy

Change Guardian enables the flow of data through proxy servers which act as intermediaries between the client applications and other servers.

Export Import Tool

Export import tool enables the users to source policy configuration from a single server to other single or multiple servers.

Agent Cache Increase

The event caching for Windows and UNIX agents has been increased to 10 MB. When the communication between agent and forwarder is disrupted, the agent can store events up to the cache size.

Configuring Communication through Scripts

Users can configure Connectors and Integrators using scripts to enable communication between the Agent, Forwarder, and the Cloud Layer.

AWS Instance Alarm

In an AWS console, when any of the regional or master server instances cross the threshold of a predefined parameter limit, the AWS users are alerted.

OpenSSL Fix

This release resolves an issue where a vulnerability in OpenSSL certificate parsing leaves systems open to denial-of-service attacks. (`CVE-2022-0778`)

Enabled TLS 1.2

With the installation of Change Guardian Agent for Windows or Change Guardian Agent for UNIX, the server and agent communications will happen through TLS 1.2 protocol.

System Requirements

For more information about hardware requirements, supported operating systems, and browsers, see the System Requirements for Change Guardian 6.2.1.1.

Installing Change Guardian 6.2.1.1

The Change Guardian server components are deployed in the SaaS environment and the Change Guardian server is configured to work as a forwarder. For information on installing the forwarder, see Installing Change Guardian Forwarder.

Known Issues

Micro Focus strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

Change Guardian Server Does Not Connect to AWS in an Authentication-Enabled Proxy Environment

Issue: In an authentication-enabled proxy server, the S Link integrator fails to connect to an Internet URL and shows the following error:

```
java.io.IOException: Unable to tunnel through proxy. Proxy returns "HTTP/1.1 407
Proxy Authentication Required.(Defect 559014)
```

Workaround: None

Unable to Export More Than 50k Federated Events in a Multi-Region SaaS Environment

Issue: Change Guardian federated event reports of more than 50k fail to export in a SaaS deployment with master nodes federation enabled. (`Defect 565175`)

Workaround: None

Legal Notice