

# Change Guardian 6.3.1.0 Release Notes

January 2024

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.

Change Guardian 6.3.1.0 release includes new features, security fixes, and usability improvements. Many of these improvements were made in direct response to suggestions from our customers. We hope you continue to help us to ensure that our product meets all your needs.

If you have suggestions for any documentation improvements, click [comment on this topic](#) at the bottom of any HTML page of [Change Guardian Documentation](#). To download Change Guardian and patches, see the [OpenText Downloads](#) website.

- ◆ “What is New?” on page 1
- ◆ “System Requirements” on page 2
- ◆ “Installing Change Guardian 6.3.1” on page 2
- ◆ “Upgrading to Change Guardian 6.3.1” on page 2
- ◆ “Software Fixes” on page 2
- ◆ “Known Issues” on page 3
- ◆ “Legal Notice” on page 4

## What is New?

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

### Manage Agents Dashboard

The [Manage Agents](#) dashboard is now integrated within Change Guardian main UI, enabling you to perform actions such as managing agents, installing agents on assets, applying agent packages, collecting agent logs, and more.

## Event Failover Destination Configuration

Change Guardian lets you configure an event failover destination for a steady flow of event data when the primary event destination is not available, thus minimizing the possibility of event loss.

## Manage Agent Grouping for Health Notifications

The [Manage Health Notification](#) dashboard now allows users to select and list agent group names to be notified for better usability.

## Management of Offline Agents

The agents that have missed a heartbeat due to system issues are listed as offline agents until the next heartbeat. When the system issue is resolved and the agent is back online, it no longer appears under [Offline Agents](#). You can manage the offline agents using [Manage Offline Agents Dashboard](#) under [Configuration](#).

## System Requirements

For more information about hardware requirements, supported operating systems, and browsers, see the [System Requirements for Change Guardian 6.3](#).

## Installing Change Guardian 6.3.1

You can install Change Guardian 6.3.1 on supported platforms. For more information about the installation procedure, see [Installing Change Guardian](#).

## Upgrading to Change Guardian 6.3.1

You can upgrade to Change Guardian 6.3.1 from Change Guardian 6.2.1.x and 6.3.0.x. For more information about upgrading Change Guardian, see [Change Guardian Installation and Administration Guide](#).

## Software Fixes

### Event Search Using Wildcard Fails to Retrieve Any Events

**Issue:** When you search for an event using wildcard, the search does not retrieve valid results. (Defect 520024)

**Fix:** The event search using wildcard works as expected.

### User Account Enable/ Disable Policy Does Not Send Events to Server

**Issue:** In a Windows 2019 OS, the [user account enable/ disable](#) policy does not send events to the Change Guardian server. (Defect 734001)

**Fix:** This issue has been resolved and the policy sends events to the server.

## Agent Health Dashboard Fails to Monitor Policy for Agents in Warning State

**Issue:** The Agent Health dashboard fails to display the policy details of agents that are in warning state with the error code as Missing auditing flags in ACE SACL. (Defect 580180)

**Fix:** The policy details of the agents in warning state shows as expected.

## Change Guardian Port Using an Inappropriate Validity Period

**Issue:** Change Guardian agent in port 2620 shows a certificate with 100 years validity. (Defect 696001)

**Fix:** The source code has been updated to generate self signed certificates with a maximum validity of 10 years.

## Change Guardian Server Contains Vulnerable Log4j and OpenJDK Packages

**Issue:** Post upgrade, Change Guardian server contains vulnerable Log4j and OpenJDK package files. (Defect 623030)

**Fix:** Change Guardian server has been updated with secured versions of Log4j and OpenJDK packages.

## SSL Certificate Using a Weak SHA1 algorithm

**Issue:** The SSL certificate signed by a server for Change Guardian agent is using a weak SHA1 hashing algorithm. (Defect 832012)

**Workaround:** The certificate has been replaced.

## Known Issues

OpenText 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](#).

## Agent Configurations Not Retained After Server Upgrade

**Issue:** When you create agent configurations for deployment, the configurations are lost after upgrading the server. (Defect 964001)

**Workaround:** Post upgrade, create new agent configurations, if necessary.

## Data Federation Fails to Add Data Sources from Specific Versions

**Issue:** In a data federated environment, when you try to add Change Guardian 6.3.0 or 6.2.1 data source servers to an authorized requester server (Change Guardian 6.3.1 server), the data source addition fails with an error message in the server log of the data source. (Defect 1012002)

**Workaround:** None.

# Legal Notice

For information about OpenText legal notices, see <https://www.opentext.com/about/legal/>

**Copyright © 2024 OpenText or one of its affiliates.**