Security Agent for UNIX 7.5 Service Pack 1 Release Notes

September 2017

Security Agent for UNIX includes new features, improves usability, and resolves several previous issues. 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 ensure that our products meet all your needs. You can post feedback on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

For the latest version of these release notes, see Security Agent for UNIX 7.5 SP1 Release Notes.

The documentation for this product is available on the NetIQ 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 Security Agent for UNIX NetIQ Documentation (https://ww.netiq.com/documentation/change-guardian/) page. To download this product, see the Security Agent for UNIX Product Upgrade (http://www.netiq.com/products) website.

1 What’s New?

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

1.1 Updates to Certified Platforms

There are several updates to the Change Guardian certified platforms:

1.1.1 New Certified Platforms

Security Agent for UNIX is now certified on the following platforms:

- SUSE Linux Enterprise Server (SLES) 12 SP2 64-bit
- Red Hat Enterprise Linux Server (RHEL) 7.3 64-bit

- Red Hat Enterprise Linux Server (RHEL) 6.8 64-bit
- Oracle Linux 7.3 64-bit
- Oracle Linux 6.8 64-bit
- Cent OS 7 (1611) 64-bit
- Cent OS 6.9 64-bit

1.1.2 Deprecated Platforms

Security Agent for UNIX is deprecated on the following platforms:

- SUSE Linux Enterprise Server 11 SP3 64-bit
- SUSE Linux Enterprise Server 12 SP1 64-bit
- SUSE Linux Enterprise Server 12 64-bit
- Red Hat Enterprise Linux Server 7.0 64-bit
- Red Hat Enterprise Linux Server 7.1 64-bit
- Oracle Linux 7.1 64-bit
- Oracle Linux 7.0 64-bit
- Cent OS 7.2 64-bit
- Cent OS 6.8 64-bit

For more information see, Technical Information page.

1.2 Simplified Packaging for Change Guardian for UNIX Installations

Change Guardian for UNIX users only need to download one installer from Micro Focus that includes everything needed for Change Guardian for UNIX 5.0. Change Guardian 5.0 bundles the Security Agent for UNIX 7.5 SP1 installer and makes it easy to install through the Agent Manager interface. The packaging and deployment model is similar to the model for the Windows agent that was introduced in Change Guardian 4.2.

In addition, for new, independent Change Guardian for UNIX 5.0 deployments, the UNIX Agent Manager has been replaced by the Change Guardian 5.0 Agent Manager. For more information, see Security Agent for UNIX Installation and Configuration Guide.

The UNIX Agent Manager still plays an important role in upgraded systems and systems where the Security Agent for UNIX is also used for Sentinel or Secure Configuration Manager.

1.3 Software Fixes

Security Agent for UNIX includes enhancements and software fixes that resolve several previous issues.

1.3.1 Disk Space Filling Up with Error Messages After Security Agent For UNIX Installation

Issue: The disk space is getting filled with the following error messages after installing Security Agent for UNIX because of the *BadPath* errors captured by the agent:

```
NetIQ::CGU::realPath()[line 2942] - ERROR: bad path
```

```
NetIQ::CGU::realPath()[line 2957] - ERROR: path . is not an absolute path.
```

Fix: There are no *BadPath* errors found in the log files and hence disk space is no more getting filled up with the log messages. `(Bug 1030546)`

1.3.2 Parsing Errors Received From the Agent for Oracle Endpoints

Issue: In Oracle Database 11g R2 versions and later, a null character is added to the query for the following SQL actions:

- `alter session set`
- `select distinct sid`

Because of null character in query, the Security Agent for UNIX sends events to Sentinel in invalid JSON format.

Fix: Security Agent for UNIX will now remove the null character from the events, before sending events to Sentinel. It now send the events to Sentinel in the correct JSON format. `(Bug 983686)`

1.3.3 Security Agent for UNIX Does Not Populate RealUserName Event Field For BSM Events

Issue: In Solaris, when a user switches between multiple accounts, Security Agent for UNIX does not populate RealUserName event field for BSM events.

Fix: Security Agent for UNIX now populates the RealUserName event field appropriately. (Bug 1031690)

1.3.4 Security Agent for UNIX Does Not Populate EffectiveUserName Event Field For BSM Events

Issue: In Solaris and Linux, when a file is modified by a non-root user, Sentinel event indicates that the file was modified by a root user.

Fix: Security Agent for UNIX now populates the EffectiveUserName event field to capture the actual user name that modified the file. `(Bug 1022116)`

1.3.5 Unable to Modify Security Agent for UNIX Properties Using UAM

Issue: When you try to update log level properties of Vigilent or detectd using UAM, the update fails with following error:

```
ERROR: Configuration failed - Operation timeout
```

Fix: You can now update the Security Agent for UNIX properties using UAM. `(Bug 1016530)`

1.3.6 Security Agent for UNIX Delays Sending Events to Change Guardian While Monitoring Large Number of Files

Issue: Security Agent for UNIX for Change Guardian shows inefficient scanning and indexing while monitoring large number of files (more that 50000 files), because scanning large number of files and indexing them takes lot of time which stops the agent from forwarding events to Change Guardian server.

Fix: Security Agent for UNIX now sends events while monitoring large number of files without any delay. `(Bug 1031757)`

2 System Requirements

For detailed information on hardware requirements and supported operating systems and browsers, see Technical Information page.

3 Installing Security Agent for UNIX

You can deploy and manage Security Agent for UNIX using the following:

- NetIQ UNIX Agent Manager (UAM)
- Change Guardian Agent Manager (CG AM)

Both UAM and CG AM allow you to remotely install one or more Agents. They also allow you to install and reconfigure the selected Agent components directly on the assets you need to monitor without having to interact with the Agents individually. However, there are certain specific functionalities available only on UAM or CG AM. Depending on your requirements, you can decide whether you need to install UAM, CG AM, or both. UAM and CG AM can coexist. For more information, see Understanding Security Agent for UNIX.

Review the deployment considerations to understand how you can install and manage agents. For more information, see Deployment Considerations.

For more information about installing these components, see the Security Agent for UNIX Installation and Configuration Guide, on the Security Agent for UNIX Documentation Web site.

4 Upgrading Security Agent for UNIX

To upgrade Security Agent for UNIX prior to 7.5 versions, you must use UAM only.

To upgrade Security Agent for UNIX 7.5 and later, in addition to UAM, you can now use CG AM. However, if you do not plan to enable the agent for Change Guardian, you can use only UAM. In deployments where you have agents enabled for Sentinel or SCM along with Change Guardian, review the deployment considerations to understand how you can upgrade and manage agents. For more information, see Deployment Considerations.

For Change Guardian 4.2.1, if you want to upgrade your agents only to 7.5.1 version, you must perform the procedure in the following section: Section 5.18, “Upgrading Security Agent for UNIX from 7.5 to 7.5.1 Fails To Authenticate With Change Guardian 4.2.1,” on page 8.

For more information about upgrading Security Agent for UNIX, see the Security Agent for UNIX Installation and Configuration Guide, on the Security Agent for UNIX Documentation Web site.

5 Known Issues

NetIQ Corporation 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 (http://www.netiq.com/support).

5.1 Cannot Install Security Agent for UNIX as Non-root User

The installation process does not support installing the Security Agent for UNIX as a non-root user. `(Bug 1052123)`

5.2 Touch Command Does Not Generate Events for File Modification

The HP-UX 11iv3 auditing subsystem does not provide information for the `utimes`, `utime`, `dup`, or `dup2` system calls. This limitation means that Change Guardian is not able to report events for the `utimes` access type in the CGU `FileMod` object and cannot report events when the contents of a file changes.

When you monitor changes to the attributes of a file on a HP-UX computer, Change Guardian does not generate events when the time attribute changes. `(Bug 969023)`

5.3 Cannot Generate Events for File Handling on RHEL7.2

The Security Agent for UNIX on RHEL 7.2 does not generate file handling events while using the Vi command, because the auditing system cannot generate utime events. `(Bug 968824)`

5.4 Exception in Agent When You Forward Events from the Agent for Change Guardian to the Standalone Sentinel Server

Issue: When you forward File Integrity Changed events from the agent for Change Guardian to the Standalone Sentinel server, file integrity attachments might display the following exception: `Error parsing JSON: ReferenceError: changed is not defined.(Bug 971624)`

Note: This issue is not found in Sentinel 7.4 or later versions.

Workaround: Ignore the exception. There is no impact to the performance because of this exception.

5.5 Events Generated for File Deletion Using rm –rf Command Display Incorrect Information

Issue: When you enable the **Including Subdirectories** or **Excluding Subdirectories** filter for monitoring file deletion, the events generated for file deletion do not display correct path information for the deleted files. The events are generated as file deletion events when you delete directories and sub-directories, even though the policy applied is for monitoring **file** deletion only.

When you enable **Excluding Subdirectories** filter, events are generated when you delete files under subdirectories also.`(Bug 975953)`

5.6 Directory Delete and Rename Events Might Not Appear For Linux

When you delete or rename directories on Linux platforms, the audit logs show null value for the directory name. Change Guardian might not capture the correct directory name in the audit logs. `(Bug 974273)`

5.7 Unable to Deploy Agents Remotely via UAM in FIPS mode

Issue: When the UNIX Agent Manager is running in FIPS mode, it does not support the remote deployment of the agents. `(Bug 989710)`

Workaround: You should manually install the agents, and then add them to UAM using **Add Host**.

5.8 Manual Configuration Required to Use UNIX File System Browser

To enable the UNIX file system browser in Change Guardian, you must set the `repositoryEnabled` flag (under `HKLM\Software\NetIQ\ChangeGuardianAgent\repositoryEnabled`) to `1`, and then restart the agent.

If you do not manually set the flag to `1`, when you use the Registry Browser, you will receive a `Could not connect to UNIX Data Source error`. `(Bug 981826)`

NOTE: To enable browsing for UNIX data sources while creating a policy, the computer where you install the Policy Editor must have a Windows agent. If you do not install an agent on the Policy Editor computer, you must manually enter the data source paths while creating a policy.

5.9 UNIX Agent Manager 7.5 Cannot Deploy Agent on FIPS Enabled Linux or UNIX Computers

When the operating system is running in FIPS mode, UNIX Agent Manager 7.5 (Linux and Windows) cannot deploy the Security Agent for UNIX. It displays the following error:

```
SSH Install Failed - Session.connect: java.io.IOException: End of IO Stream Read
```

```
Installation Failed - Session.connect: java.io.IOException: End of IO Stream
Read.(Bug 999496)
```

5.10 UNIX Agent Manager 7.5.1 Cannot Monitor Security Agent for UNIX 7.4

Issue: The communication between UNIX Agent Manager 7.5.1 and Security Agent for UNIX 7.4 fails due to protocol mismatch.

Workaround: Upgrade Security Agent for UNIX 7.4 to 7.5 and then to 7.5.1 version. For more information about upgrading to Security Agent for UNIX 7.5, see Upgrading Agent Using UNIX Agent Manager `(Bug 989481)`.

5.11 Event Diagnostics Not Supported for Security Agent for UNIX

The **Assets Monitoring Failures** report contains Windows assets only. It does not contain data related to the UNIX assets `(Bug 906282)`.

5.12 Events Not Generated When Soft Link for File is Deleted

Issue: `File was deleted` events are not generated when soft link for file is deleted `(Bug 975575)`.

5.13 Sentinel Agent Manager Connector Not Working in FIPS Mode

Issue: Sentinel Agent Manager Connector does not work in FIPS mode.

Workaround: For the Sentinel Agent Manager Connector to work in FIPS mode, perform the steps mentioned in NetIQ Knowledge Base Article 7018187. `(Bug 997589)`

5.14 UNIX Agent Manager 7.5 Cannot Manage AppManager Agent for UNIX

Issue: UAM 7.4 is packaged and is compatible with AppManager Agent for UNIX 8.1. When the Security Agent for UNIX 7.5 is installed on the same host as the AppManager Agent for UNIX, it becomes incompatible with UAM 7.4 due to secure communication incompatibilities. Therefore, UAM 7.5 must be used to manage the Security Agent for UNIX 7.5 on the host.

NOTE: UAM 7.5 is not compatible with AppManager Agent for UNIX.

Workaround: For instructions on managing the AppManager Agent for UNIX installations on the hosts where Security Agent for UNIX 7.5 is also installed, use the procedure, Installing Locally on a UNIX or Linux Computer in *NetIQ AppManager for UNIX and Linux Servers Management Guide*. `(Bug 1001277)`

5.15 Error Occurs When Adding Asset to UAM

Issue: When you add an asset to one UAM the following error message is displayed because the same asset is already registered with a different UAM:

`invalid credential`

Workaround: You have to delete the asset from the previous UAM asset list.

NOTE: You can also manually go to `/usr/netiq/cmnagent/config` location and delete the `acctToken` file.

`(Bug 1048907)`

5.16 Security Agent for UNIX 7.5 SP1 With Change Guardian 5.0 and Secure Configuration Manager Cannot Coexist

When you install Security Agent for UNIX 7.5 SP1 using CG AM for new installation of Change Guardian 5.0 and SCM 6.x on the same computer, SCM registration fails because of the dynamic certificate changes.`(Bug 1045613)`

5.17 SCM Registration Fails While Upgrading Security Agent for UNIX from 7.5 to 7.5.1 Using CG AM 5.0

Issue: SCM Registration Fails While Upgrading Security Agent for UNIX from 7.5 to 7.5.1 using CG AM where SCM and Change Guardian are enabled. `(Bug 1056447)`

Workaround: Perform the following steps from UAM to re-register Security Agent for UNIX with SCM server:

1. Go to **Configure** > **SCM Options**.
2. Click **Configure** button.
3. In the **SCM Configuration** window, ensure that the **Core Services Address** is same as SCM Core IP Address and click **Save**.
4. Restart the agent service by selecting **Stop** and **Start** buttons in the **Agent Controls** panel.

OR

You can perform the following manual registration steps on Security Agent for UNIX:

1. Navigate to the following location: `/usr/netiq/bin`
2. Run the following command: `#./wcRegister`
3. Run the following command to restart SCM services: `#/etc/init.d/uvserv restart`

5.18 Upgrading Security Agent for UNIX from 7.5 to 7.5.1 Fails To Authenticate With Change Guardian 4.2.1

Issue: Upgrading Security Agent for UNIX from 7.5 to 7.5.1 using UAM or manually fails to authenticate with the Change Guardian 4.2.1.

Workaround:

Perform the following steps:

1. On CG server 4.2.1, navigate to '/opt/netiq/cg/javos' and open 'javos.yml'
2. Comment out the existing `excludedCipherSuites` list by prefixing with `#`.
3. Add the following line (including the two spaces at the beginning) under the line commented out in Step 2:

   ```
     excludedCipherSuites:
   [SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA,SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_RSA_W
   ITH_3DES_EDE_CBC_SHA,TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_
   3DES_EDE_CBC_SHA,TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDH_RSA_WITH_3DES_E
   DE_CBC_SHA,TLS_ECDHE_RSA_WITH_RC4_128_SHA, SSL_RSA_WITH_RC4_128_MD5,
   SSL_RSA_WITH_RC4_128_SHA]
   ```

4. Run the following command to restart javos:

   ```
   /etc/init.d/nq_javos restart
   ```

NOTE: If you want to manage Security Agent for UNIX 7.4 or earlier versions, perform the following steps:

1. Uncomment the following entry (including the two spaces at the beginning) from `javos.yml` file:

   ```
     # supportedCipherSuites: [SSL_RSA_WITH_RC4_128_SHA]
   ```

2. Remove the following cipher from the list of *excludedCipherSuites*:

   ```
   SSL_RSA_WITH_RC4_128_SHA
   ```

3. Run the following command to restart javos:

   `/etc/init.d/nq_javos restart`.

---

6 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website (http://www.netiq.com/support/process.asp#phone).

For general corporate and product information, see the NetIQ Corporate website (http://www.netiq.com/).

For interactive conversations with your peers and NetIQ experts, become an active member of our community (https://www.netiq.com/communities/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

7 Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.