

RadiantOne v7.3.27

Release Notes

November 29, 2022

These release notes contain important information about improvements and bug fixes for RadiantOne v7.3.27.

These release notes contain the following sections:

[Improvements](#)

[Supported Platforms](#)

[Bug Fixes](#)

[Known Issues](#)

[How to Report Problems and Provide Feedback](#)

Improvements

- [VSTS40052]: Improved the custom limits settings to avoid confusion by removing the Time Limit and Look Through Limit properties.
- [VSTS43382]: Improvement for the RadiantOne audit report generation process so that it prints the progress of processing the entries and generating the report.
- [VSTS43873]: Improvement to enforce granular precedence among specific locations within the same naming context for custom limits. The deepest level in the tree will take precedence over parent custom limits.
- [VSTS44003]: Added an option to vdsconfig execfile command to continue executing commands despite errors. Use: vdsconfig execfile <file> -ignoreError
- [VSTS44253/44203]: Added Kafka capture connector as an option for persistent cache refreshes for views from Oracle databases.
- [VSTS44382]: Added a query timeout property for the database timestamp capture connector for persistent cache refresh to avoid the connector waiting indefinitely when the database server isn't responding quickly.
- [VSTS44451]: OpenJDK Update for jdk8u352-b08.
- [VSTS44511]: Improved the password policy dictionary check process to support a "contains" match instead of just an exact match. Set "enablePwdPolicyDictionarySubstringCheck" : true either in the ZooKeeper vds_server.conf settings or using vdsconfig command line utility, if you want the password policy to enforce a "contains" match. **Note that the value "true" must be in all lowercase.**
- [VSTS44520]: Improvement to the graphapi custom data source so that entries returned from Azure AD will have a memberOfDisplayName attribute which mirrors the contents of the memberOf attribute, but will contain the displayName of the group instead of the guid.

Supported Platforms

RadiantOne is supported on the following 64-bit platforms:

- Microsoft Windows Server 2008 R2, 2012 R2, 2016, 2019
- Windows Servers Core
- Red Hat Enterprise Linux v5+
- Fedora v24+
- CentOS v7+
- SUSE Linux Enterprise v11+
- Ubuntu 16+

For specific hardware requirements of each, please see the RadiantOne System Requirements located in the Radiant Logic online knowledge base.

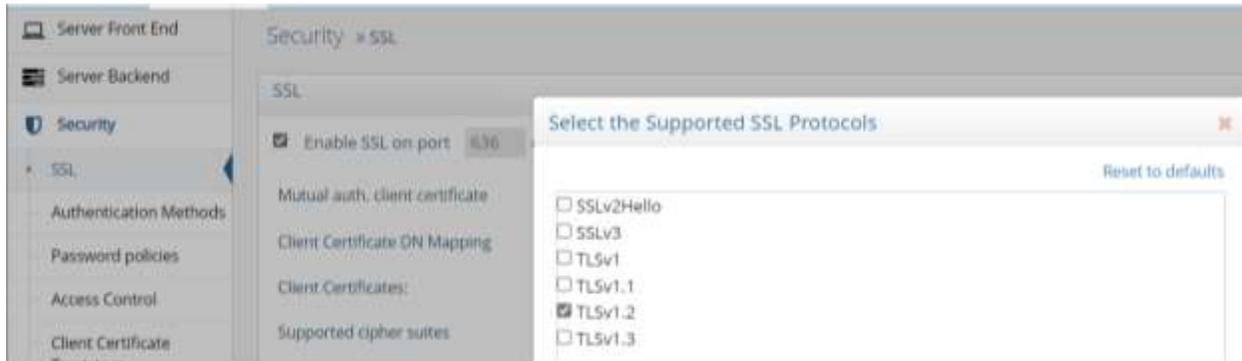
Bug Fixes

- [VSTS38634]: Fixed an issue with persistent cache configuration (requested attributes and refresh dependencies) when unauthorized characters are part of the backend table's metadata.
- [VSTS42860]: Reduced security risks by adding missing security headers and removing deprecated ones.
- [VSTS43967]: Fixed LDAP object class syntax parsing during schema extraction, so that it accepts situations when there is no space between the OID and the opening parenthesis, and properly parses it.
- [VSTS44049]: Fixed an issue where meta-prefixed attributes from SCIMv2 backends were returned in the virtual entries whether they were configured/mapped in the ORX/DVX or not.
- [VSTS44115]: Fixed an issue with the "Keep track of user's last successful logon time every" setting in password policy not getting saved or loaded properly.
- [VSTS44147]: Fixed an issue with backlink computation causing a loop when dynamic and nested (cyclic) groups are involved which was causing stability issues in the RadiantOne FID service.
- [VSTS44148]: Fixed an issue where the attribute uniqueness constraint during a move/modRDN was preventing the new RDN value from being enforced.
- [VSTS44228]: Fixed an issue where the user-defined binary attributes specified in a custom schema might experience incorrect binary values within the exported LDIF file for replication.
- [VSTS44234]: Fixed an issue with dynamic groups not being calculated properly when the memberURL attribute contains unsupported characters.

- [VSTS44261]: Fixed an issue with non-string attribute types not being correctly translated or updated for SCIMv2 backends.
- [VSTS44262]: Fixed an issue with connection pooling causing RadiantOne to send anonymous binds through the RLI Router to Active Directory backends for modify requests when pass-through authorization was enabled.
- [VSTS44278]: Fixed an issue where the RadiantOne license expiration date was not being honored and the control panel was still accessible and functional. Now redirection to an error page is now implemented if the RadiantOne license is expired.
- [VSTS44292]: Fixed an issue where the RadiantOne SCIM server did not report totalResults counts correctly in its responses.
- [VSTS44293]: Fixed an issue with enable/disable referral chasing not working.
- [VSTS44314]: Fixed an issue where inter-cluster replication did not function properly when the operational attributes were configured to be hidden.
- [VSTS44330]: Fixed issues seen when defining a new password policy where the “Accounts may be locked out due to login failures” was automatically enabled and the interface was displaying negative values for the account activity properties.
- [VSTS44394]: Fixed an issue with the backlink attribute optimization options not being saved correctly on the Main Control Panel -> Directory Namespace tab
- [VSTS44412]: Upgraded to org.apache.commons:commons-text:1.10.0 to address CVE-2022-42889.
- [VSTS44439]: Fixed an issue with Main Control Panel -> Directory Browser search result page not properly displaying the options to modify and delete attributes.
- [VSTS44591]: Fixed an issue with the dictionary check settings not being saved properly for password policies configured from the RadiantOne Main Control Panel.
- [VSTS44606]: Fixed an issue with the scimclient2 custom object that was preventing it from working with SCIM attributes containing hyphenated names.
- [VSTS44616]: Fixed an issue where the Main Control Panel > Settings tab was not displaying properly on follower cluster nodes.

Known Issues

Related to [VSTS44451]: OpenJDK Update for jdk8u352 included in this patch release, there is a known issue when RadiantOne is configured for FIPS-mode. To avoid the issue, you must disable TLS 1.3 and enable TLS 1.2. This can be done from RadiantOne Main Control Panel > Settings > Security > SSL. Click CHANGE next to Enabled SSL Protocols. Uncheck TLS 1.3 and check at a minimum TLS v1.2. Save and restart the RadiantOne service.



For known issues reported after the release, please see the Radiant Logic Knowledge Base:
<https://support.radiantlogic.com/hc/en-us/categories/4412501931540-Known-Issues>

How to Report Problems and Provide Feedback

Feedback and problems can be reported from the Support Center/Knowledge Base accessible from: <https://support.radiantlogic.com>

If you do not have a user ID and password to access the site, please contact support@radiantlogic.com.