

New Relic

QualityNet IT | New Relic



optimize their software. With real-time insights into application performance, infrastructure, and customer experience, New Relic enables proactive issue resolution and data-driven decision-making in support of the CCSQ QualityNet mission.

New Relic is a comprehensive observability platform designed to help organizations monitor, troubleshoot, and

What would you like to do?

Resources

- [AWS Getting Started Guide](#)
- ESS DevSecOps [New Relic Documentation](#)
- Complete vendor [New Relic Documentation](#)
- Searchable [New Relic Data Dictionary](#)
- New Relic [APM Best practice guide](#)
- New Relic [Browser Monitor best practice guide](#)
- New Relic [Infrastructure Monitor best practice guide](#)
- New Relic [Alert best practice guide](#)
- New Relic [Security policy](#)
- New Relic [Data retention policy](#) for Pro subscription
- New Relic University [to learn New Relic](#).

FAQ

New Relic is available to all ADOs who support a CMS application.

Each organization will be able to use all features within New Relic which include monitoring, troubleshooting, setting up, and receiving alerts as well as using and creating dashboards. Your organization may decide to use a subset of these features.

For new applications, review Getting Started tab above.

Yes. Your New Relic account will be pre-configured to send New Relic data to Splunk.

No. The current alert template contains sensitive data that cannot be sent to corporate email. Until the template is updated, accounts will be audited for adherence. The approved methods for receiving notifications are:

- Slack (It is recommended to use a dedicated Slack team channel for alert notifications)
- ServiceNow

Yes. This functionality will be pre-configured for each AWS account.

Yes. This feature is helpful for testing and finding issues with your software's business critical functionality before real users do.

Yes. There are two android and iPhone apps available in the respective app stores. One is for New Relic insights only and the other one is for monitoring.

Security Guidelines

- Refer to the [Security](#) page for the QualityNet CFE Data Management Policy and QualityNet Rules of Behavior
- [Ensure data is sent to an approved source](#) (Slack, Jira, Splunk).
- Ensure no PHI/PII data is sent to sources other than the approved one.
- Ensure no sensitive data is sent to corporate email.
- Ensure no incident alerts are sent to any public page or channel and limit the information to only the intended audience;
- Ensure no sensitive data is sent to another tool in a manner that violates the terms of that tool.

Need Help?

Please contact one of the following:

- **CCSQ Support Central:** Provides you with multi-program support to submit a new ticket, and track the status of an existing case, incident, or request. No login required. https://cmsqualitysupport.servicenowservices.com/ccsq_support_central
- **CCSQ Service Center:** For technical assistance with any account related issues, please contact the Service Center at:
Phone: (866) 288-8914 (TRS:711)
Slack: #help-service-center-sos
Email: ServiceCenterSOS@cms.hhs.gov
Hours of Operation: 24/7
- DevOps Slack channel at [#help-devsecops](#)
- Visit [ESS II DevSecOps Home](#)

