

Proofpoint Threat Response v3.6.0 Release Notes

June 2018

Release Summary:

Threat Response 3.6.0 adds support for email quarantine in IBM Domino environments.

Only customers running IBM Domino should upgrade to this version.

Please refer to the following for more detailed information:

1. [Threat Response Auto-Pull \(TRAP\) Enhancements](#)
2. [Download Instructions](#)

Recommendations:

As with any software upgrade it is recommended that a full system backup be created prior to starting the upgrade. Backups can be initiated in the Appliance Management Console. This backup, as well as an export of the Master Secret, should be downloaded and stored in a secure location.

If any issues are encountered during or after upgrading please open a support ticket at: <https://proofpointcommunities.force.com/>.

Threat Response Auto Pull (TRAP) Enhancements

The following improvements have been made to the Threat Response Auto Pull (TRAP) capabilities:

- IBM Domino Support

This release adds support for integration with IBM Domino mail servers to enable email quarantine capability. Threat Response provides the ability to manually or automatically remove malicious emails from a user's mailbox.

Feature set:

Supported

- Basic auto and manual quarantine
- Undo quarantine
- Distribution list expansion

Not Supported

- Forward following
- Search & Quarantine (when message-ID is missing in TAP alert)
- Abuse mailbox

NOTE: Threat Response only supports distribution list expansion for members of distribution lists that have SMTP addresses

Supported Domino versions include:

Platform	Version
Domino Server	Supported: 9.0.1 (Fix-Pack 10) running on Windows Server

Download instructions

NOTE: Starting in Threat Response v3.2.0, the minimum specification of the virtual appliance has been updated. Please review the [Virtual Machine requirements](#) section for updated minimum specification.

Installation files are available upon request.