In Rapid7, you can submit a request to exclude vulnerabilities pertaining to a specific asset or vulnerabilities across all assets in an asset group.

This guide will demonstrate how to submit an exclusion request for an asset and how to view your vulnerability exclusions.

**Step 1. IMPORTANT**
At this time, you will submit a Team Dynamix Ticket via the Team Dynamix Portal using the link: [https://ecu.teamdynamix.com/TDClient/Requests/ServiceDet?ID=31591](https://ecu.teamdynamix.com/TDClient/Requests/ServiceDet?ID=31591). The following Template should be copied/Pasted within the ticket, filled out and forwarded to Cyber Security Operations Center for review by the VMC committee. All attributes in Bold should be met with an explanation. **NOTE: When submitting vulnerabilities for exceptions/risk acceptance; it is ONE asset per ticket listing all vulnerabilities for that ONE asset.**

---

**Vulnerability Management Team Dynamix Exception Ticket Template**

**Vulnerability:**
Description Field: What is the vulnerability that Rapid7 is reporting?
Free Text Field

**Asset:**
Description Field: What is the name of the Asset in Rapid7?
Free Text Field

**Reason:**
Drop down option with the following:
1) Acceptable use
2) Compensating control

**Business Need:**
Description Field: What is the purpose of the server/application/service in regards to University operations? (e.g. in support of processing, storing, maintaining or any use of financial information/student information/employee information/alumni information/patient information etc.)
Free Text Field

**Technical Justification:**
Description Field: What is the reason(s) you are unable to apply the recommended remediation to the reported vulnerability? What compensating security controls are you employing to address the potential risk to the server/application/service?
Free Text Field

**Sensitive Data:**
Description Field: Does the server/application/service contain or use any information designated sensitive by the University, State, Federal, or International authorities (e.g. Social security numbers (SSN), Payment Card Industry Information (PCI), Driver’s license number, Personally identifiable patient information (PHI), Personally identifiable student information (FERPA), Personnel identifiable information (PII), Proprietary research data, Legal data)
Drop down option with the following:
1) Yes
2) No
**Step 2.**
Navigate to one of your assets.

Under the **Vulnerabilities** section, you’ll see all detected vulnerabilities listed for your asset.

---

**Step 3.**

To the right of your listed vulnerabilities is a column titled **Exceptions**.

To submit an exclusion request, click the **Exclude** button next to one of the vulnerabilities. This will bring up the **Vulnerability Exception** menu.
Step 4.
In the Vulnerability Exception menu, select the drop-down menu for Scope to apply the exclusion to just this specific asset or all assets in an asset group.

Click the drop-down menu for Reason to specify a reason for the exclusion.

**Key:**

- **Compensating controls:** Network managers may mitigate the security risks of certain vulnerabilities, which, technically, could prevent their organization from being PCI compliant. It may be acceptable to exclude these vulnerabilities from the report under certain circumstances. For example, the application may discover a vulnerable service on an asset behind a firewall because it has authorized access through the firewall. While this vulnerability could result in the asset or site failing the audit, the merchant could argue that the firewall reduces any real risk under normal circumstances. Additionally, the network may have host- or network-based intrusion prevention systems in place, further reducing risk.

- **Acceptable use:** Organizations may have legitimate uses for certain practices that the application would interpret as vulnerabilities. For example, anonymous FTP access may be a deliberate practice and not a vulnerability.

- **Acceptable risk:** In certain situations, it may be preferable not to remediate a vulnerability if the vulnerability poses a low security risk and if remediation would be too expensive or require too much effort. For example, applying a specific patch for a vulnerability may prevent an application from functioning. Re-engineering the application to work on the patched system may require too much time, money, or other resources to be justified, especially if the vulnerability poses minimal risk.

- **False positives:** According to PCI criteria, a merchant should be able to report a false positive, which can then be verified and accepted by a Qualified Security Assessor (QSA) or Approved Scanning Vendor (ASV) in a PCI audit. Below are scenarios in which it would be appropriate to exclude a false positive from an audit report. In all cases, a QSA or ASV would need to approve the exception.

In the Additional comments section, you must provide a detailed explanation for your exclusion.

Beside Expires on, provide a date for which you would like your exclusion to expire. It is not recommended to put Never, unless you can provide enough evidence to support your reasoning.

Click Submit.
Step 5.
Upon submitting your exclusion request, your exception will display as **Under Review**.

*If your request is approved*, it will be removed from the listed vulnerabilities under your asset. *If the request is rejected*, then a “Resubmit” icon will appear beside the vulnerability.

**NOTE:**
Our VMC committee will determine the validity of the vulnerability exclusion request and will approve or deny based on their decision. If an explanation for an exclusion is deemed unsatisfactory, or if the user is persistent after multiple denials and resubmissions, a user and their manager may be requested to attend a meeting in which they will discuss the exclusion with members of the VMC committee.

**Step 6.**
At the time of writing this document, the only method of viewing your current exclusion requests is by individual asset.

To view the status of the exclusion requests that you have submitted, navigate to the specific asset. The status of the vulnerability exclusion request is listed under the **Vulnerabilities** section.