Service Now Policy Exception Request

Version Log

Version	Date	Author	Description of Changes
1.0	2025-12-22	Alaric Diman	Initial draft created; full documentation of Policy Exception Request process added.
1.1	2026-01-05	Alaric Diman	Added Sections 4.6–4.9 with screenshots and explanations (PER creation, "In Review" state change, Owner field, Save action, Request Extension workflow).
1.2	2026-01-19	Alaric Diman	Added Section 5.2 detailing the Request Extension form fields (Extension date, Extension reason, Justification).
1.3	2026-01-30	Alaric Diman	Updated formatting, clarified steps, added emphasis callouts, and incorporated additional screenshots.

Service Now Policy Exception Request

1. Purpose

This Work Instruction provides the step-by-step process for creating a **Policy Exception Request** in ServiceNow's **Vulnerability Response (VR)** module. Once a policy exception is fully approved, the system will automatically update all covered **Vulnerability Items (VITs)** to the **Deferred** state for the duration of the exception.

2. Scope

This procedure applies to:

- System Engineers
- Application & Server Owners
- Infrastructure Owners
- Any group responsible for vulnerability remediation or exception submission

Applies to:

- Tenable Security Center vulnerabilities
- Patch-related delays
- Vendor dependent fixes
- Maintenance window limitations

3. Prerequisites

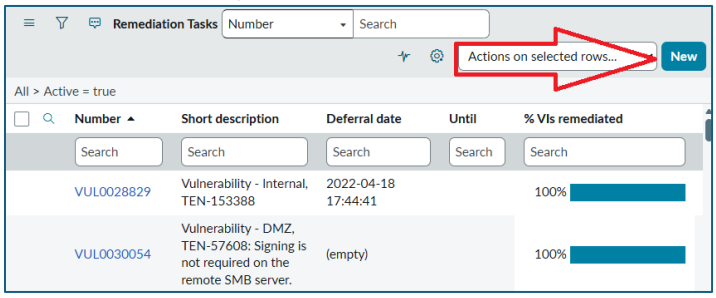
Before submitting a policy exception request, ensure the following:

- You have identified the specific **Vulnerability Items (VITs)** requiring an exception.
- A valid business justification is prepared (e.g., dependency issues, maintenance window constraints, vendor limitations, operational risk).
- You understand the required **exception duration** (temporary exceptions typically have a defined limit such as 30, 60, or 90 days based on policy).
- You have any necessary documentation ready (emails, risk approvals, or implementation plans).

4. Procedure

4.1 Navigate to the Remediation Task Creation Page

- Access ServiceNow instance using SSO.
- Use the application navigator and go to:
  - **Vulnerability Response > Remediation Tasks > New**
  - Link: Remediation Tasks | ServiceNow



Service Now Policy Exception Request

4.2 Complete the Remediation Task Header Information

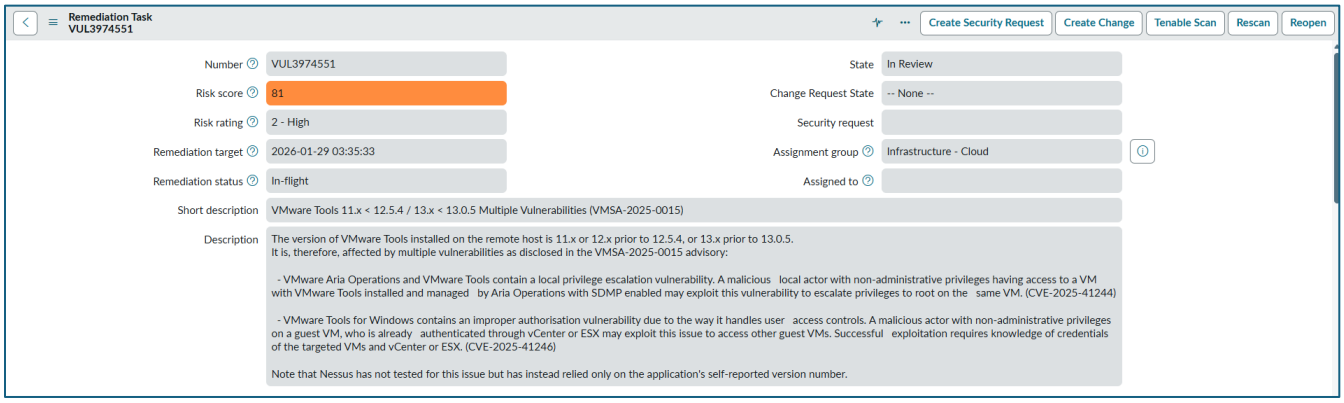
- You will see the Remediation Task New Record form.

Fill out the following fields:

Tip: The more detailed the justification, the faster Security and Risk approve the request.

[Header Section]

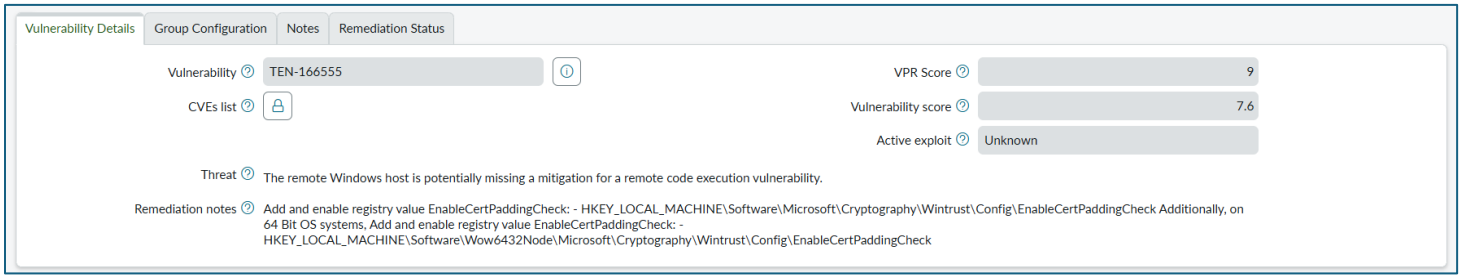
Field	What to Enter
Short Description	A clear title (e.g., *Policy Exception Request – VMware Tools VMSA-2025-0015*).
Assignment Group	The team submitting the request (e.g., *Server Engineering*, *SCCM*, *App Support*).
Assigned To	Optional; assign if a primary engineer owns the work.
Description	Provide detailed justification: reason for exception, impact, timeline, dependency, vendor info, etc.
State	Leave as **Open**.



Service Now Policy Exception Request

4.3 Complete the Vulnerability Details Section (Scroll to the middle of the form and open the Vulnerability Details tab.)

Field	Purpose / What to Enter
Vulnerability	This field is pre-populated when the task is created from a Vulnerability Group. If blank, click the search icon and select the correct Vulnerability record (e.g., TEN-266420 for VMware Tools).
CVEs List	Auto-populated based on the vulnerability definition. No manual entry required.
Threat	A read-only description summarizing the threat narrative from Tenable/Qualys.
Remediation Notes	Provides remediation guidance (e.g., "Upgrade VMware Tools to version 12.5.4 or later"). No update needed unless additional internal notes are helpful.
VPR Score	Read-only. Tenable's Vulnerability Priority Rating.
Vulnerability Score	Read-only. Overall severity (often CVSS-based).
Active Exploit	Read-only. Shows exploit availability (Known, Unknown, Weaponized, etc.).

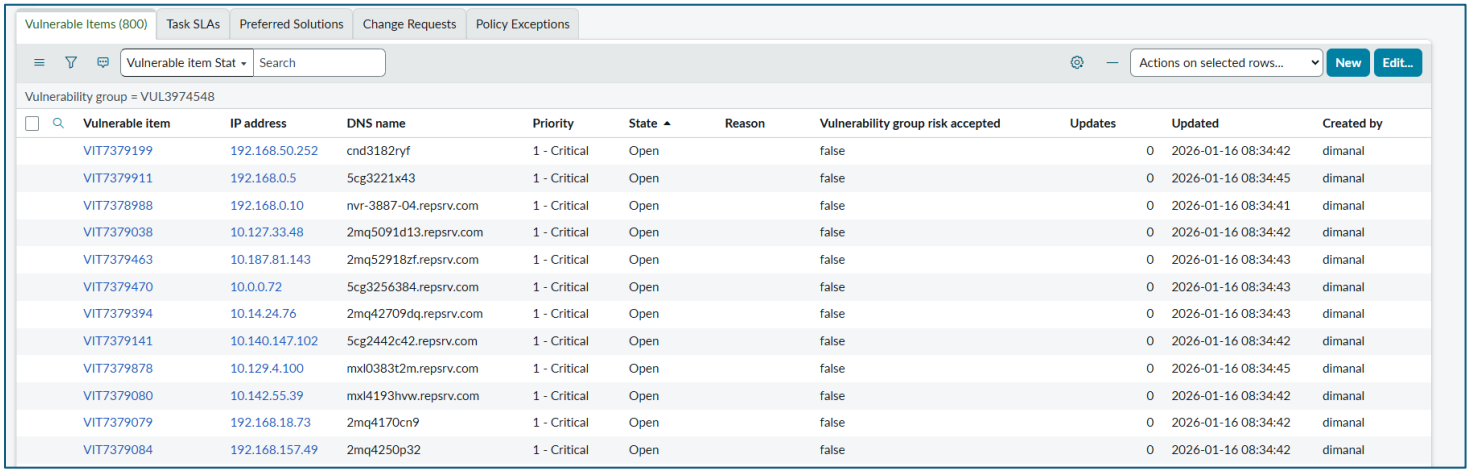


4.4 Add Vulnerable Items (VITs) to the Policy Exception

Scroll to the bottom of the Remediation Task and locate the Vulnerable Items related list.

- Click the "**Edit**..." Button

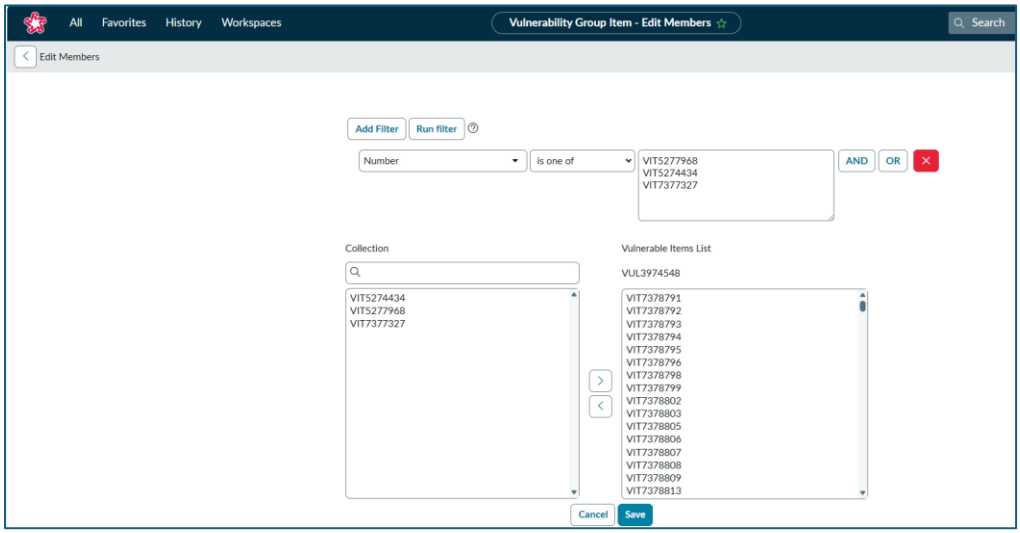
This opens the Edit Members window.



Vulnerable item	IP address	DNS name	Priority	State	Reason	Vulnerability group risk accepted	Updates	Updated	Created by
VIT7379199	192.168.50.252	cnd3182ryf	1 - Critical	Open		false	0	2026-01-16 08:34:42	dimanal
VIT7379911	192.168.0.5	5cg3221x43	1 - Critical	Open		false	0	2026-01-16 08:34:45	dimanal
VIT7378988	192.168.0.10	nvr-3887-04.repsrv.com	1 - Critical	Open		false	0	2026-01-16 08:34:41	dimanal
VIT7379038	10.127.33.48	2mq5091d13.repsrv.com	1 - Critical	Open		false	0	2026-01-16 08:34:42	dimanal
VIT7379463	10.187.81.143	2mq52918zf.repsrv.com	1 - Critical	Open		false	0	2026-01-16 08:34:43	dimanal
VIT7379470	10.0.0.72	5cg3256384.repsrv.com	1 - Critical	Open		false	0	2026-01-16 08:34:43	dimanal
VIT7379394	10.14.24.76	2mq42709dq.repsrv.com	1 - Critical	Open		false	0	2026-01-16 08:34:43	dimanal
VIT7379141	10.140.147.102	5cg2442c42.repsrv.com	1 - Critical	Open		false	0	2026-01-16 08:34:42	dimanal
VIT7379878	10.129.4.100	mxl0383t2m.repsrv.com	1 - Critical	Open		false	0	2026-01-16 08:34:45	dimanal
VIT7379080	10.142.55.39	mxl4193hvw.repsrv.com	1 - Critical	Open		false	0	2026-01-16 08:34:42	dimanal
VIT7379079	192.168.18.73	2mq4170cn9	1 - Critical	Open		false	0	2026-01-16 08:34:42	dimanal
VIT7379084	192.168.157.49	2mq4250p32	1 - Critical	Open		false	0	2026-01-16 08:34:42	dimanal

4.4.1 Use Filters to Locate Specific VITs

- At the top of the Edit Members window, click Add Filter.
- Set the filter as follows (as shown in the screenshot):
  - Field: **Number**
  - Operator: **is one of**
  - Value: Enter one or more **VIT numbers** (e.g., VIT5277968, VIT5274434, etc.)
- Click Run filter.
  - The Collection panel (left side) now shows only the VITs matching your filter.
  - This is the fastest way to locate specific servers in large vulnerability groups.



4.4.2 Move VITs into the Exception List

Once the filtered results appear in the Collection list:

- Select the desired VITs on the left side.
  - Use Ctrl+Click for multiple selections
  - Or use Shift+Click for ranges
- Click the **>** button to move them into the Vulnerable Items List on the right.
  - The right-side list (Vulnerable Items List – VULxxxxxxx) represents the VITs that will be included in the Policy Exception request.

4.4.3 Review and Save

Before saving:

✓ Ensure all intended VITs appear in the **right panel**

✓ Remove any incorrect VITs using the **<** arrow

✓ Verify that the list corresponds to the systems that require the exception

Once confirmed:

- Click **Save** to commit the changes.
- You will be returned to the Remediation Task, and the selected VITs now appear under the Vulnerable Items list.

Service Now Policy Exception Request

4.5 Click the “Request Exception” Button

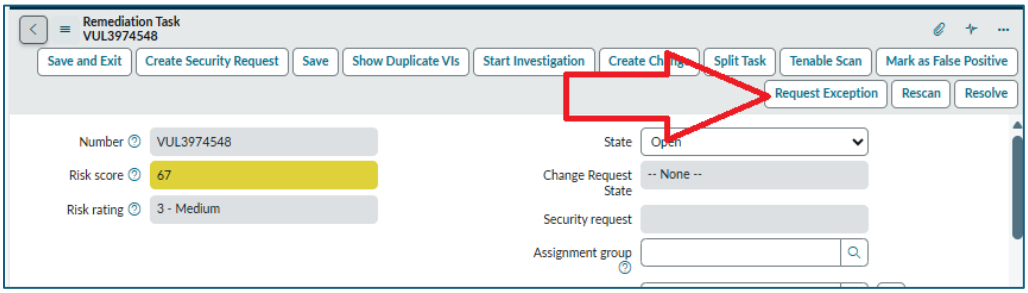
At the top of the Remediation Task form, locate the action bar and click:

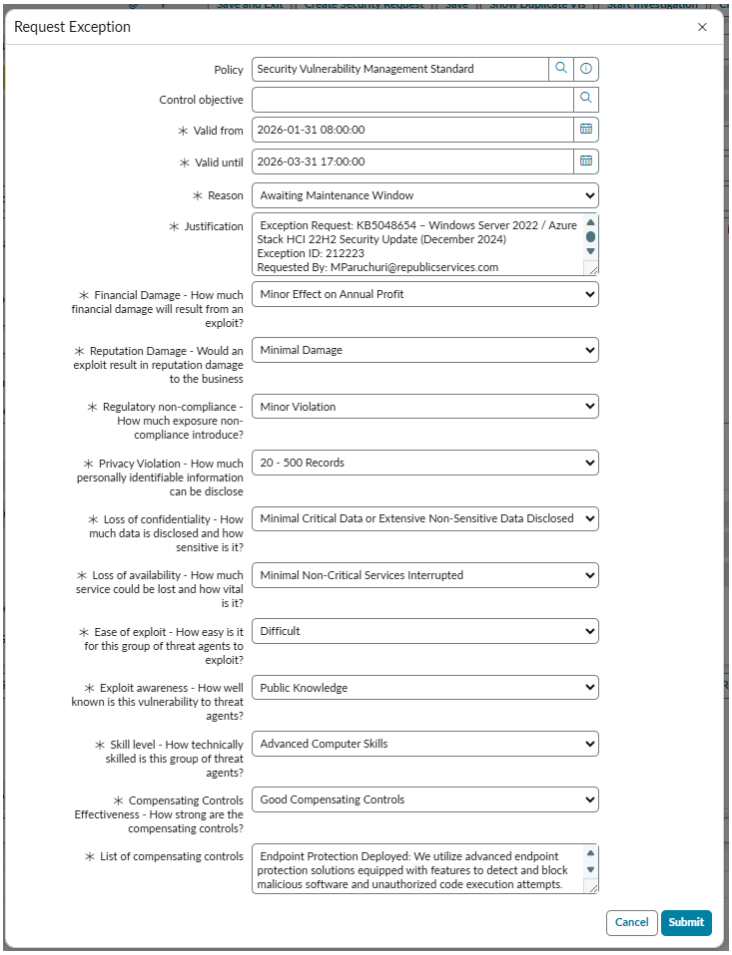
➡️ **Request Exception**

This opens the **Request Exception** modal window.

Your screen will look like this:

- A popup titled **Request Exception**
- Multiple required fields marked with a red asterisk
- “Valid from” automatically populated
- “Valid until” requiring user input





Service Now Policy Exception Request

4.5.1 Complete the Exception Request Form
Below is a field-by-field guide tailored to Republic Services' configuration.

- **Policy**
  Input: Security Vulnerability Management Standard
  This links the exception to the appropriate Republic Services governance standard.

- **Control Objective**
  Leave blank unless instructed by Security Governance.

- **Valid From (Required)**
  Auto-populated with the current date/time.
  Feel free to modify.

- **Valid Until (Required)**
  Enter the date when the exception expires.
  Typical durations: **30–90 days**, depending on policy and justification.

- **Reason (Required)**
  Select the reason why the system cannot be remediated in time.
  Example from your screenshot: **Awaiting Maintenance Window**

  - If the patch **exists but cannot be applied now**, choose:
    ✓ Awaiting Maintenance Window
  - If the vendor patch **does not exist** or is not supported yet, choose:
    ✓ Fix Unavailable
  - If alternate protections reduce the risk during deferral, choose:
    ✓ Mitigating Control in Place
  - If leadership has explicitly approved permanent or long-term risk acceptance, choose:
    ✓ Risk Accepted

- **Justification (Required)**
  Provide a clear and detailed explanation, including:
  - Patch / KB number
  - Business impact
  - Why remediation cannot occur before SLA
  - Who requested the exception
  - Relevant exception ID (if continuing or extending)

4.5.2 Complete the Risk Assessment Fields

Each dropdown must be completed. The fields evaluate the potential risk if the vulnerability remains unpatched.

Field	Meaning	Example Selection
Financial Damage	Estimated financial impact if exploited	*Minor Effect on Annual Profit*
Reputation Damage	Potential harm to public trust	*Minimal Damage*
Regulatory Non-Compliance	Legal/regulatory consequence	*Minor Violation*
Privacy Violation	Number of PII records exposed	*20–500 Records*
Loss of Confidentiality	Sensitivity of data exposed	*Minimal Critical Data or Extensive Non-Sensitive Data Disclosed*
Loss of Availability	Service downtime and impact	*Minimal Non-Critical Services Interrupted*
Ease of Exploit	Difficulty level for threat actors	*Difficult*
Exploit Awareness	Public awareness of the vulnerability	*Public Knowledge*
Skill Level	Threat actor skill required	*Advanced Computer Skills*
Compensating Controls Effectiveness	Strength of existing safeguards	*Good Compensating Controls*

4.5.3 List of Compensating Controls (Recommended)

Provide a description of protection that reduces risk while vulnerability remains unpatched.

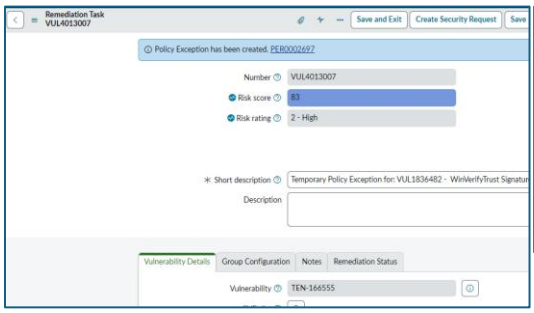
4.5.4 Submit the Exception

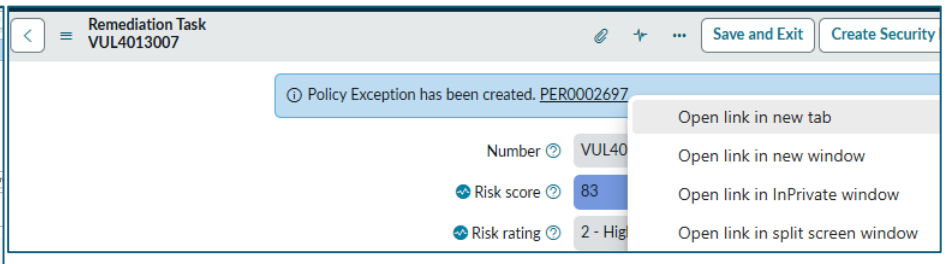
Click **Submit** to finalize the request.

4.6 PER Creation and Remediation Task Status Update

After submitting the Request Exception, ServiceNow automatically updates the Remediation Task and generates a new exception record. The following changes occur immediately:

- A confirmation banner appears at the top of the screen, stating:
  - "Policy Exception has been created. PER00XXXX."
- This PER# is the unique identifier for the newly created policy exception request.
- Clicking the PER link opens the exception record, where you can view:
  - Approval workflow
  - Exception details
  - Current status
  - Approvers and timestamps

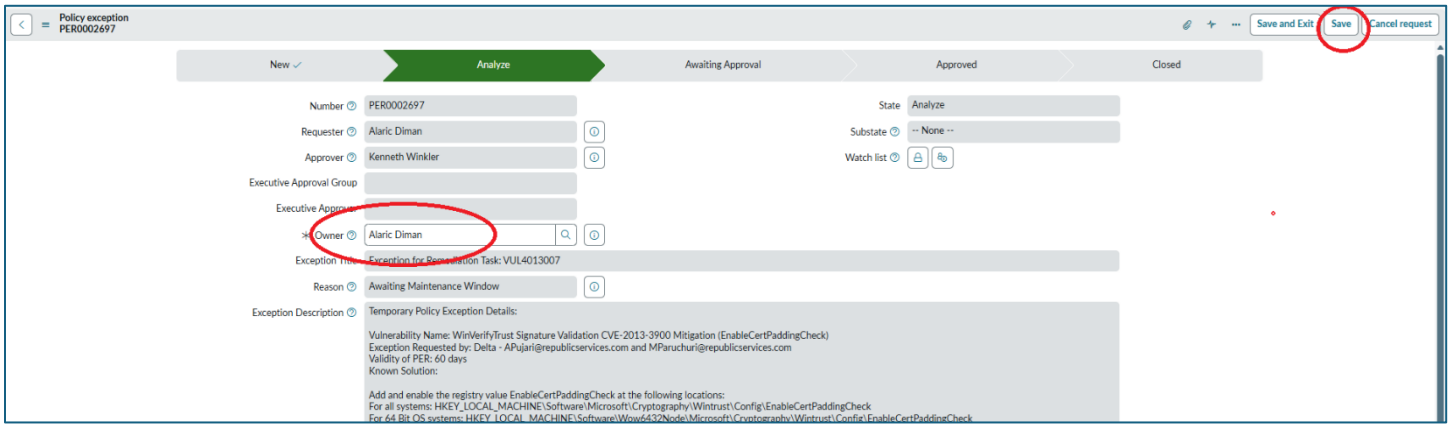




Service Now Policy Exception Request

4.7 Review and Update the Policy Exception Record (Final Verification Step)

After the Policy Exception (PER#) is created, you can open the exception record to validate and finalize its details. The last screen displays key fields that may require your attention. The circled items in the screenshot represent two important actions: verifying the Owner and saving the record.



4.8 Workflow Status Review

At this stage, the exception will typically be in the Analyze phase of the workflow:
New → Analyze → Approved → Closed

This confirms:

- The exception has been successfully created
- Ownership is assigned
- The record is now under evaluation by Security Governance
- No further action is required unless additional information is requested

5. Requesting an Extension for an Existing Policy Exception

The **Schedule** tab in the Policy Exception record provides key lifecycle information about the exception, including its validity period, duration, and the number of extensions allowed. The primary action in this section is the **Request Extension** feature, highlighted in the screenshot.

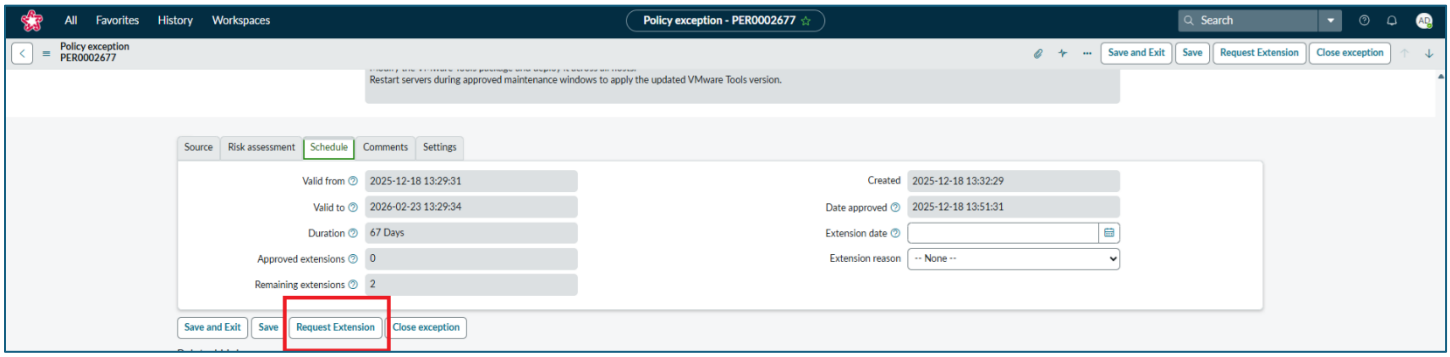
5.1 Review Exception Schedule Details

In the **Schedule** tab, verify the following system-generated fields:

- **Valid from** – The date/time the exception began
- **Valid to** – The current expiration date of the exception
- **Duration** – Total length of the exception in days
- **Approved extensions** – Number of previously approved extensions
- **Remaining extensions** – How many more extensions may be requested under policy
- **Created / Date approved** – System timestamps showing when the exception was created and approved

These fields help determine whether an extension is justified and still permissible.

Service Now Policy Exception Request



5.2 Complete the Extension Request Form

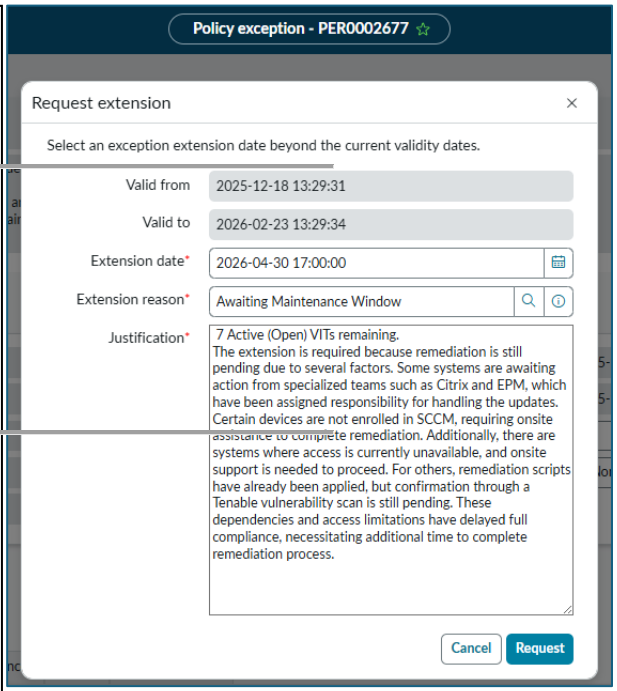
When the **Request Extension** button is clicked, the *Request extension* window opens. This modal allows you to specify the new exception end date and provide the justification required for approval. Each field in this window is important for Security Governance evaluation.

5.2.1 Review Existing Validity Dates

The top section of the modal displays the current exception period:

- Valid from – The start date of the original exception
- Valid to – The current expiration date

These fields are read-only, confirming the context of the extension request.



5.2.2 Enter the New Extension Date (Required)

In the Extension date field, select the new *proposed* expiration date for the exception.

Ensure the date reflects the true remediation timeline, including:

- Pending patching
- Dependency issues
- Required maintenance windows
- Vendor delays

The extension date must be beyond the current Valid To value.

5.2.3 Select an Extension Reason (Required)

Choose the most accurate reason from the Extension reason dropdown.

Examples include:

- Awaiting Maintenance Window
- Fix Unavailable
- Mitigating Control in Place
- Resource Constraints
- Others

In the screenshot, the selected option is Awaiting Maintenance Window, indicating scheduling limitations.

5.2.4 Provide a Detailed Justification (Required)

Use the Justification field to clearly explain why the extension is necessary.

A strong justification should include:

- Number of Active (Open) VITs remaining
- Dependencies impacting remediation (e.g., Citrix, EPM, SCCM enrollment)
- Access issues or systems needing onsite support
- Pending Tenable scan confirmation
- Any compensating controls in place
- Operational or scheduling factors delaying remediation

5.3 Submit the Extension Request

Once all required fields are complete:

- Review your entries
- Click **Request** to submit the extension

The extension will enter the approval workflow.

Security Governance must approve the request before the existing exception expires.

- END OF DOCUMENT-