



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.

Section	Title	Page
1	Purpose	1
2	Scope	1
3	Prerequisites	1
4	Procedure	1
4.1	Navigate to the Remediation Task Creation Page	1
4.2	Complete the Remediation Task Header Information	2
4.3	Complete the Vulnerability Details Section	3
4.4	Add Vulnerable Items (VITs) to the Policy Exception	3
4.4.1	Use Filters to Locate Specific VITs	4
4.4.2	Move VITs into the Exception List	4
4.4.3	Review and Save	4
4.5	Click the “Request Exception” Button	5
4.5.1	Complete the Exception Request Form	6
4.5.2	Complete the Risk Assessment Fields	7
4.5.3	List of Compensating Controls (Recommended)	7
4.5.4	Submit the Exception	7
4.6	PER Creation and Remediation Task Status Update	7
4.7	Review and Update the Policy Exception Record	8
4.8	Workflow Status Review	8
4.9	Requesting an Extension for an Existing Policy Exception	8
5	Requesting an Extension	8
5.1	Review Exception Schedule Details	8
5.2	Complete the Extension Request Form	9
5.3	Submit the Extension Request	10



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](#)

All > Active = true	Number	Short description	Deferral date	Until	% VIs remediated
	VUL0028829	Vulnerability - Internal, TEN-153388	2022-04-18 17:44:41		100%
	VUL0030054	Vulnerability - DMZ, TEN-57608: Signing is not required on the remote SMB server.	(empty)		100%



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., <i>Policy Exception Request – VMware Tools VMSA-2025-0015</i>).
Assignment Group	The team submitting the request (e.g., <i>Server Engineering, SCCM, App Support</i>).
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 .

Remediation Task
VUL3974551

Number: VUL3974551 State: In Review

Risk score: 81 Change Request State: -- None --

Risk rating: 2 - High Security request

Remediation target: 2026-01-29 03:35:33 Assignment group: Infrastructure - Cloud

Remediation status: In-flight Assigned to: (empty)

Short description: VMware Tools 11.x < 12.5.4 / 13.x < 13.0.5 Multiple Vulnerabilities (VMSA-2025-0015)

Description: The version of VMware Tools installed on the remote host is 11.x or 12.x prior to 12.5.4, or 13.x prior to 13.0.5. It is, therefore, affected by multiple vulnerabilities as disclosed in the VMSA-2025-0015 advisory.

- VMware Aria Operations and VMware Tools contain a local privilege escalation vulnerability. A malicious local actor with non-administrative privileges having access to a VM with VMware Tools installed and managed by Aria Operations with SDMP enabled may exploit this vulnerability to escalate privileges to root on the same VM. (CVE-2025-41244)

- VMware Tools for Windows contains an improper authorization vulnerability due to the way it handles user access controls. A malicious actor with non-administrative privileges on a guest VM, who is already authenticated through vCenter or ESX may exploit this issue to access other guest VMs. Successful exploitation requires knowledge of credentials of the targeted VMs and vCenter or ESX. (CVE-2025-41246)

Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number.



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.).

Screenshot of the Service Now Vulnerability Details tab. The tab is active, showing the following fields:

Vulnerability	TEN-166555	VPR Score	9
CVEs list		Vulnerability score	7.6
		Active exploit	Unknown

Below the fields, there is a Threat note: "The remote Windows host is potentially missing a mitigation for a remote code execution vulnerability." and a Remediation note: "Add and enable registry value EnableCertPaddingCheck: - HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck Additionally, on 64 Bit OS systems, Add and enable registry value EnableCertPaddingCheck: - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck".

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 Items (800)										
Task SLAs Preferred Solutions Change Requests Policy Exceptions										
Actions on selected rows... New Edit...										
Vulnerability group = VUL3974548										
	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
	VIT737911	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	mxl0393t2m.repsrv.com	1 - Critical	Open	false		0	2026-01-16 08:34:45	dimanal
	VIT7379080	10.142.55.39	mxl4193hw.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



Service Now Policy Exception Request

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.

The screenshot shows the 'Edit Members' interface for a 'Vulnerability Group Item'. At the top, there's a navigation bar with 'All', 'Favorites', 'History', and 'Workspaces'. The title bar says 'Vulnerability Group Item - Edit Members'. Below the title, there's a search bar with a magnifying glass icon and the word 'Search'. A 'Run filter' button is visible. On the left, there's a 'Collection' panel containing a search bar and a list of VIT numbers: VIT5274434, VIT5277968, and VIT7377327. On the right, there's a 'Vulnerable Items List' panel with a header 'VUL3974548' and a list of many VIT numbers, including VIT7378791 through VIT7378813. Between the two panels are 'Cancel' and 'Save' buttons. Above the panels, there's a filter configuration area with dropdowns for 'Number' and 'Is one of', and a list box containing 'VIT5277968', 'VIT5274434', and 'VIT7377327'. There are also 'AND' and 'OR' buttons and a clear 'X' button.

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 – VULxxxxxx) 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:



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

The screenshot shows the Service Now Remediation Task interface. At the top, there's a toolbar with various buttons like Save and Exit, Create Security Request, and Request Exception. The Request Exception button is highlighted with a large red arrow. Below the toolbar, there are several input fields: Number (VUL3974548), Risk score (67), Risk rating (3 - Medium), State (Open), Change Request State (None), Security request, and Assignment group. The Request Exception button is located in the top right corner of the main form area.

The screenshot shows the Request Exception modal window. It contains the following fields:

- Policy: Security Vulnerability Management Standard
- Control objective
- * Valid from: 2026-01-31 08:00:00
- * Valid until: 2026-03-31 17:00:00
- * Reason: Awaiting Maintenance Window
- * Justification: Exception Request: KB5048654 - Windows Server 2022 / Azure Stack HCI 22H2 Security Update (December 2024)
Exception ID: 212223
Requested By: MParuchuri@republicservices.com
- * Financial Damage: Minor Effect on Annual Profit
- * Reputation Damage: Minimal Damage
- * Regulatory non-compliance: Minor Violation
- * Privacy Violation: 20 - 500 Records
- * Loss of confidentiality: Minimal Critical Data or Extensive Non-Sensitive Data Disclosed
- * Loss of availability: Minimal Non-Critical Services Interrupted
- * Ease of exploit: Difficult
- * Exploit awareness: Public Knowledge
- * Skill level: Advanced Computer Skills
- * Compensating Controls Effectiveness: Good Compensating Controls
- * List of compensating controls: Endpoint Protection Deployed: We utilize advanced endpoint protection solutions equipped with features to detect and block malicious software and unauthorized code execution attempts.

At the bottom right are Cancel and Submit buttons.



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)



Service Now Policy Exception Request

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

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

The figure consists of two side-by-side screenshots of the ServiceNow Remediation Task interface. Both screenshots show a confirmation message at the top: "Policy Exception has been created. PER0002697".

Screenshot 1 (Left): Shows the Remediation Task screen for VUL4013007. It displays fields like Number (VUL4013007), Risk score (83), and Risk rating (2 - High). Below these are sections for Short description (Temporary Policy Exception for VUL1834482 - WinVerifyTrust Signature) and Description. At the bottom, there are tabs for Vulnerability Details, Group Configuration, Notes, and Remediation Status, with the Vulnerability tab currently selected.

Screenshot 2 (Right): Shows the same Remediation Task screen for VUL4013007. It also displays the same confirmation message. To the right of the screen, a context menu is open with several options: Open link in new tab, Open link in new window, Open link in InPrivate window, and Open link in split screen window.



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.

The screenshot shows the 'Policy exception' screen with PER0002697. The workflow status is 'Analyze'. Key fields include:

- Number: PER0002697
- Requester: Alaric Diman
- Approver: Kenneth Winkler
- State: Analyze
- Substate: ... None ...
- Watch list: (empty)
- Executive Approval Group: (empty)
- Executive Approver: (empty)
- Owner: Alaric Diman (circled in red)
- Exception Type: Exception for Reservation Task: VUL4013007
- Reason: Awaiting Maintenance Window
- Temporary Policy Exception Details:
 - Vulnerability Name: WinVerifyTrust Signature Validation CVE-2013-3900 Mitigation (EnableCertPaddingCheck)
 - Exception Requested by: Delta - APujari@republicservices.com and MParuchuri@republicservices.com
 - Validity of PER: 60 days
 - Known Solution:
 - Add and enable the registry value EnableCertPaddingCheck at the following locations:
 - For all systems: HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck
 - For 64 Bit OS systems: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck

Buttons at the top right: Save and Exit, Save (circled in red), Cancel request.

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

The screenshot shows the Service Now interface for a policy exception. The top navigation bar includes 'All', 'Favorites', 'History', and 'Workspaces'. The title bar says 'Policy exception - PER0002677'. Below the title, a message states 'Restart servers during approved maintenance windows to apply the updated VMware Tools version.' The main content area has tabs for 'Source', 'Risk assessment', 'Schedule' (which is selected), 'Comments', and 'Settings'. Under 'Schedule', there are fields for 'Valid from' (2025-12-18 13:29:31), 'Valid to' (2026-02-23 13:29:34), 'Duration' (67 Days), 'Approved extensions' (0), and 'Remaining extensions' (2). To the right, there are fields for 'Created' (2025-12-18 13:32:29), 'Date approved' (2025-12-18 13:51:31), 'Extension date' (with a calendar icon), and 'Extension reason' (None). At the bottom of the schedule section are buttons for 'Save and Exit', 'Save', 'Request Extension' (which is highlighted with a red box), and 'Close exception'.

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.

<p>5.2.1 Review Existing Validity Dates The top section of the modal displays the current exception period:</p> <ul style="list-style-type: none">• Valid from – The start date of the original exception• Valid to – The current expiration date <p>These fields are read-only, confirming the context of the extension request.</p>	<p>The modal has a header 'Policy exception - PER0002677'. It contains a section titled 'Request extension' with the instruction 'Select an exception extension date beyond the current validity dates.' Below this are fields for 'Valid from' (2025-12-18 13:29:31) and 'Valid to' (2026-02-23 13:29:34). A large input field for 'Extension date*' contains the value '2026-04-30 17:00:00'. A dropdown for 'Extension reason*' is set to 'Awaiting Maintenance Window'. A large text area for 'Justification*' contains the following text: 7 Active (Open) VITs remaining. The extension is required because remediation is still pending due to several factors. Some systems are awaiting action from specialized teams such as Citrix and EPM, which have been assigned responsibility for handling the updates. Certain devices are not enrolled in SCCM, requiring onsite assistance to complete remediation. Additionally, there are systems where access is currently unavailable, and onsite support is needed to proceed. For others, remediation scripts have already been applied, but confirmation through a Tenable vulnerability scan is still pending. These dependencies and access limitations have delayed full compliance, necessitating additional time to complete remediation process.</p>
<p>5.2.2 Enter the New Extension Date (Required) In the Extension date field, select the new <i>proposed</i> expiration date for the exception. Ensure the date reflects the true remediation timeline, including:</p> <ul style="list-style-type: none">• Pending patching• Dependency issues• Required maintenance windows• Vendor delays <p>The extension date must be beyond the current Valid To value.</p>	
<p>5.2.3 Select an Extension Reason (Required) Choose the most accurate reason from the Extension reason dropdown. Examples include:</p> <ul style="list-style-type: none">• Awaiting Maintenance Window• Fix Unavailable• Mitigating Control in Place• Resource Constraints• Others <p>In the screenshot, the selected option is Awaiting Maintenance Window, indicating scheduling limitations.</p>	



Service Now Policy Exception Request

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-