How to configure an External Ticketing Connection to ServiceNow (SNOW) for Remediation Projects

Prerequisites

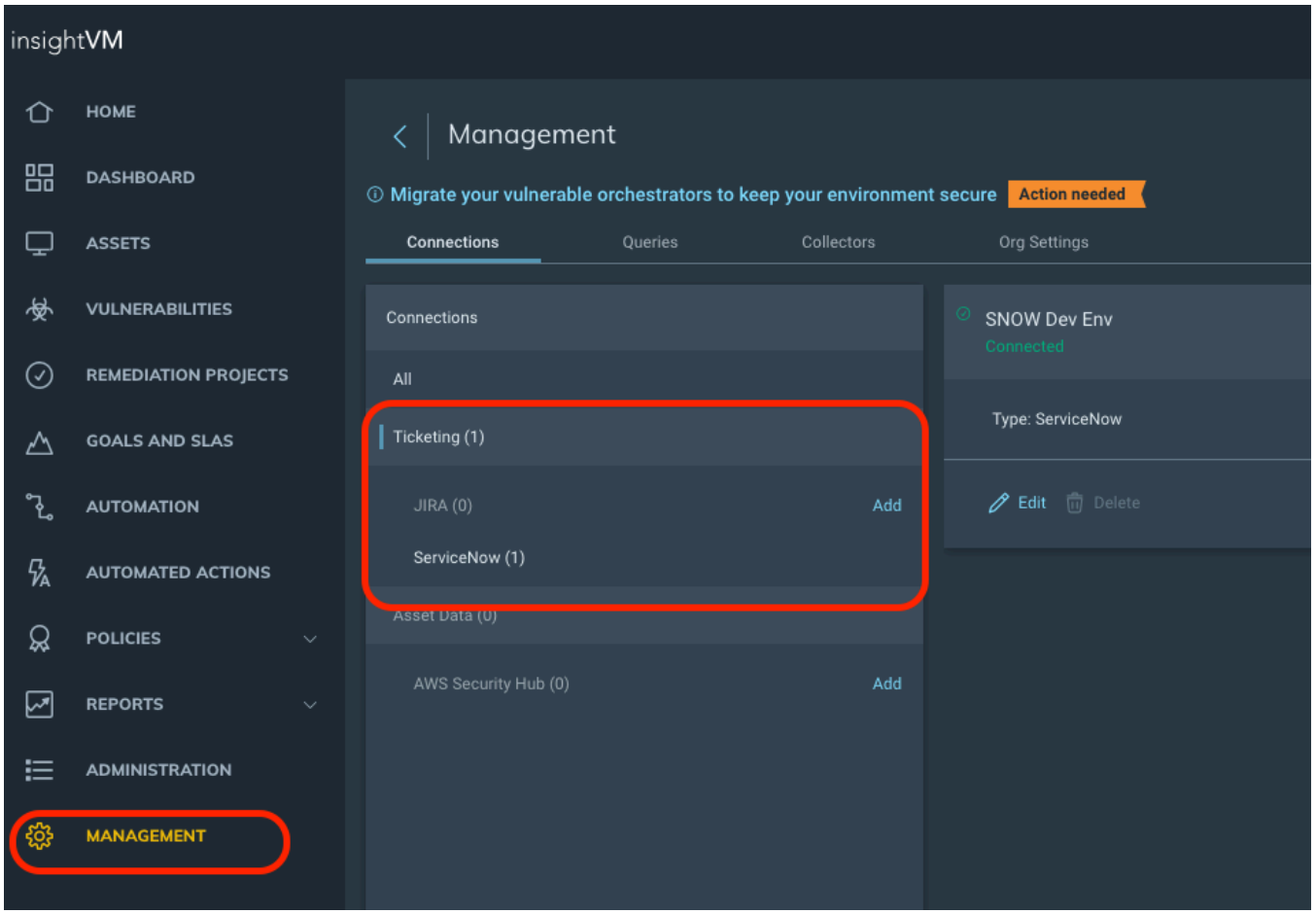
- ☐ **Ensure the ServiceNow instance (on-premise or cloud-based) is reachable from the Rapid7 Insight Platform IP addresses for your data region.** You may need to configure new firewall rules, if applicable. See Configure communications with the Insight Platform.
- ☐ **Ensure certain Access Controls have been enabled and properly configured.** Refer to Configuring Access Control rules in our documentation for the specific configuration parameters.

Please note that the *ServiceNow Vulnerability Response module* is not a requirement for this integration to work. Presently, only HTTP Basic authentication over TLS (HTTPS) is supported, and there are no options for Single-Sign-On (SSO) or Multi-factor Authentication (MFA) enforcement at this time.

InsightVM will initiate the connection and create ServiceNow Incident tickets (INCs) for each solution listed in a Remediation Project configured with the aforementioned ticketing connection. For multiple projects and **remediation teams, it is not necessary to create multiple ticketing connections to ServiceNow as a single connection can use assignment rules to properly delegate** tickets to the appropriate remediation teams (HelpDesk, Server Operations, Development, Security, etc.). Additionally, Remediation Projects that were created prior to setting up a ticketing connection can be modified to use a connection that has been created afterward.

Creating the Ticketing Connection

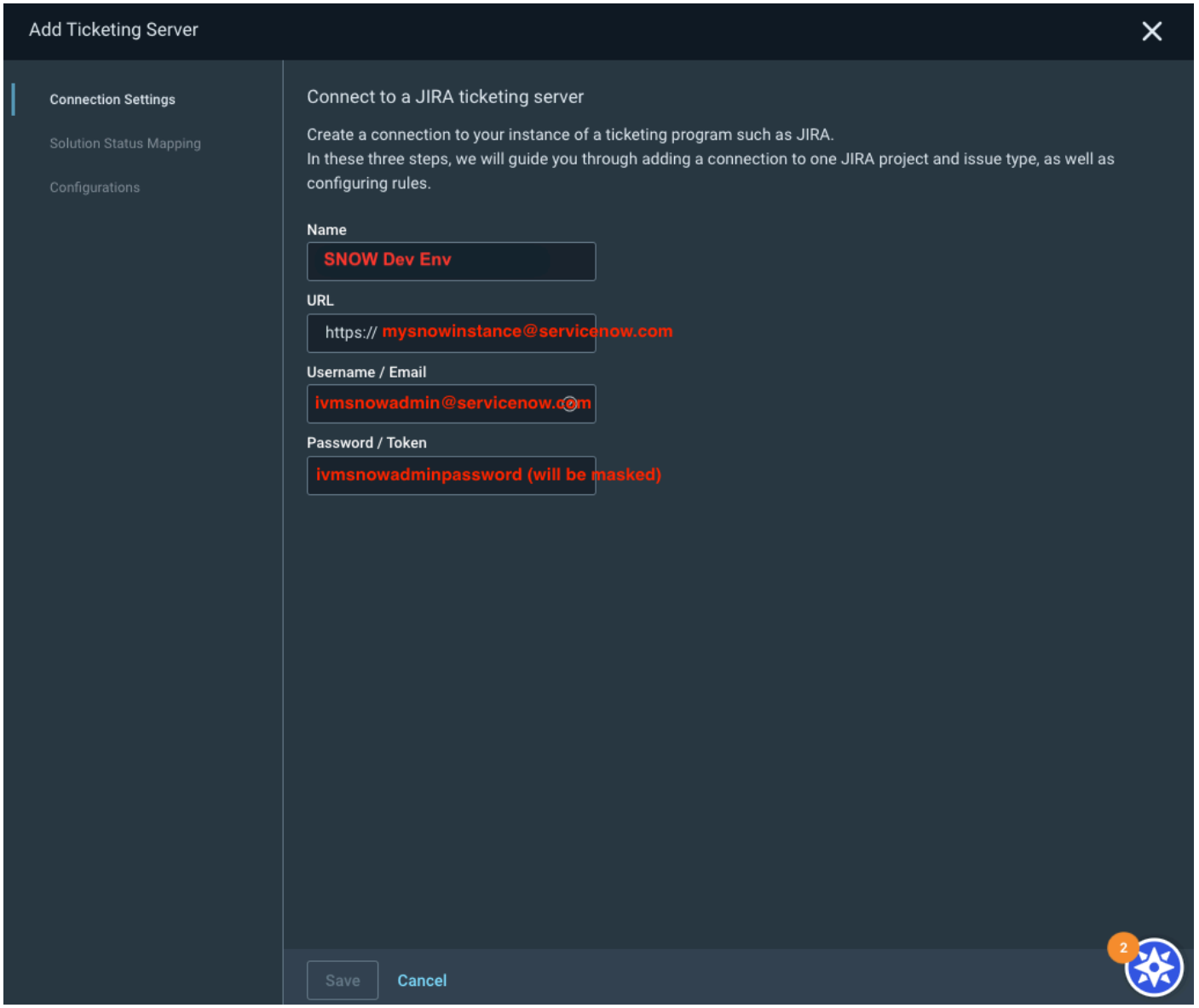
This can be done in either the *Management* page or the *Remediation Projects* page of InsightVM. For this document's purposes, we will be using the Management page.



1. Click Management.
2. Under Connections →Ticketing, click Add.
3. The Add Ticketing Server blade will appear. The first section will require:
    - a name for the connection (SNOW DEV, SNOW Prod, whatever makes contextual sense)
    - the ServiceNow instance's URL
    - the ServiceNow user account with the admin role that has been provisioned specifically for InsightVM to use (no other ServiceNow users should be using this account)
        i. If you have your ServiceNow instance configured such that user accounts must include an email address, ensure you use the full *local-part@domain.tld* formatted address in the username field.

- The password to the ServiceNow user account with the admin role is provisioned specifically for InsightVM to use.

4. Click Save.



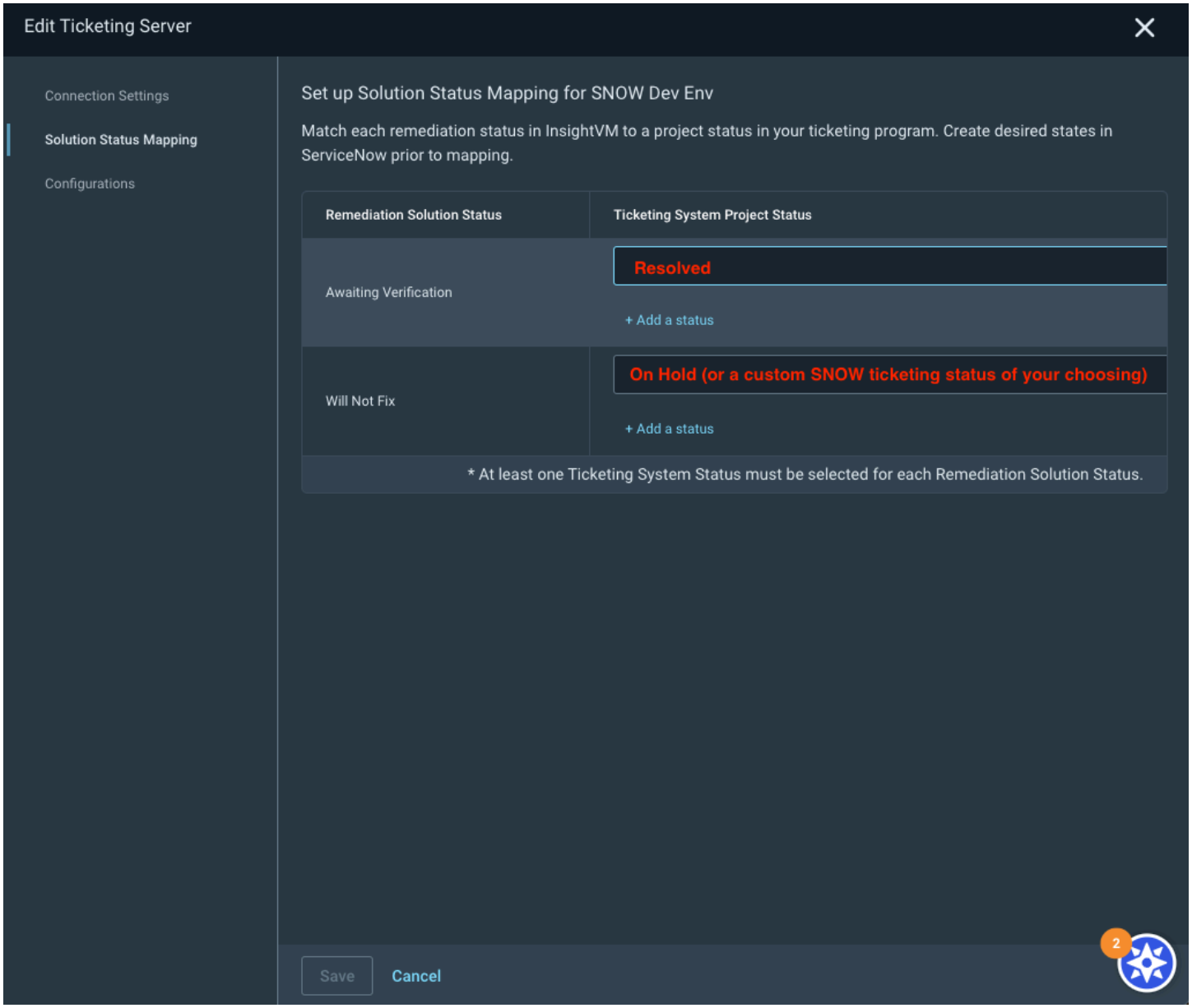
5. The second section will map the project solution's statuses to counterparts in ServiceNow. For both of InsightVM's solution statuses, under the Ticketing System Project Status dropdown, you will find the available ticket statuses retrieved from your ServiceNow instance. Recommended statuses are as follows:

   - **Awaiting Verification ↔ Resolved**

     i. This means when the assignee of the ServiceNow ticket sets the ticket status to Resolved, the solution in the Remediation Project will be set to Awaiting Verification thus the asset needs to be re-assessed by InsightVM either through an agent assessment or through an authenticated Scan Engine-based scan to confirm the remediation was successful.

- **Will Not Fix ↔ On Hold** (or some other meaningful ticketing status indicating it cannot be resolved or completed)
    i. This means that the project solution could not be applied to the assets in question for a reason the remediator team will have to explain and seek business approval.

6. Click Save.



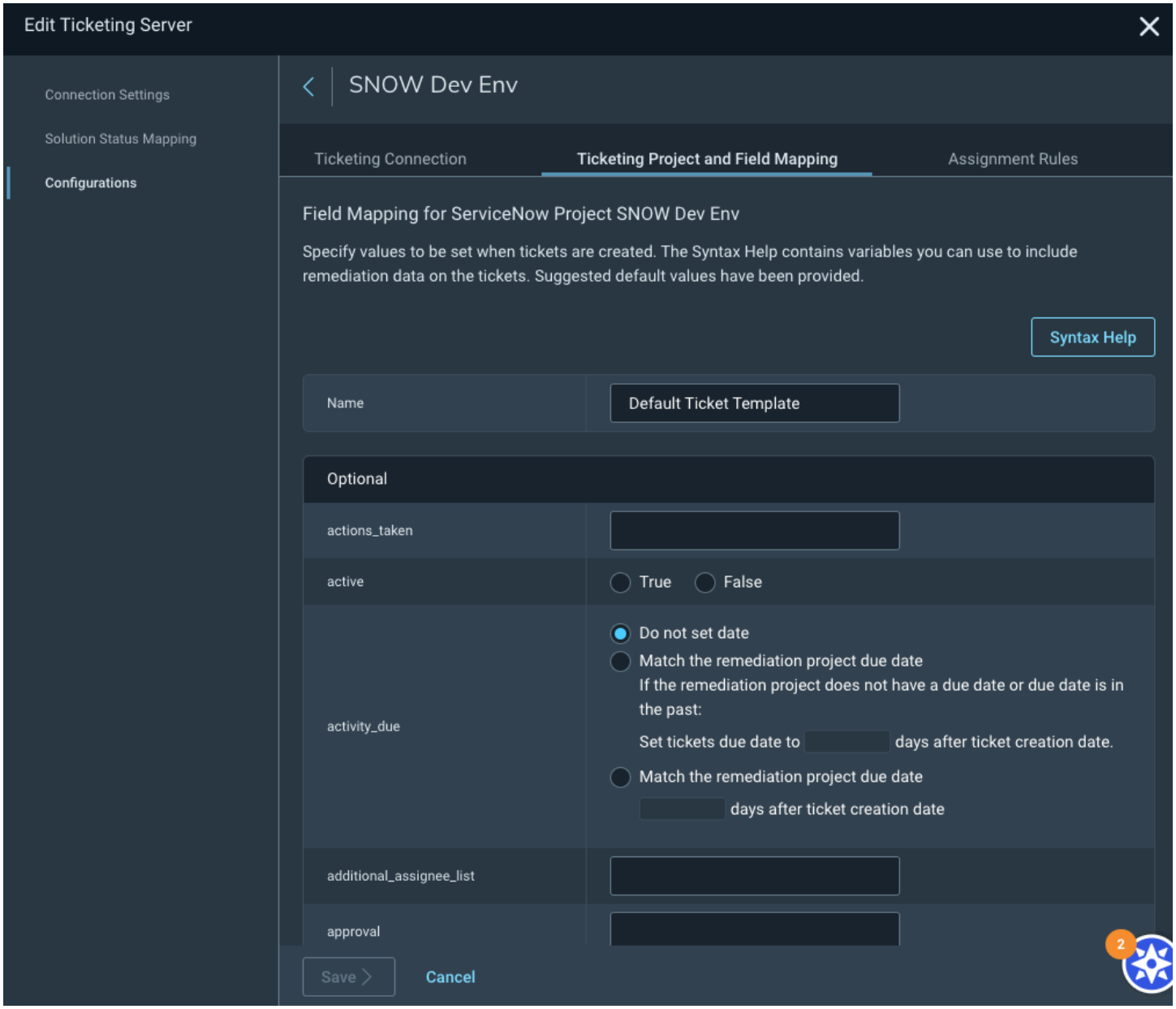
7. The third section will specify one or more connection configurations. This will determine what fields in a ServiceNow ticket will be populated by InsightVM and how the ticket will be assigned.
    - Click on the **Ticketing Connection heading** to select Incident in your ServiceNow instance.
    - Click Save.
    - Use the **Ticketing Project and Field Mapping heading** to specify which ticket fields to

populate.

i. This screen will be extensive as a ServiceNow ticket can have many fields. InsightVM provides some default values in specific fields, but you can adjust these as you see fit for your organization and processes.

ii. For variable data, such as asset names, IP addresses, vulnerability IDs, and solution text, InsightVM can use variable names to populate the fields accordingly. Refer to the following table to see the syntax available (this help is also available by clicking the Syntax Help button):

Remediation Ticket Integration	Field Description
$PROJ_UUID	The project uuid.
$PROJ_NAME	The project name.
$SOL_NAME	The solution name.
$SOL_ADDL_INFO	Solution Additional Information.
$SOL_FIX	Solution Fix Steps
$SOL_URL	Solution Reference URL
$ASSET_IP_LIST	A comma delimited list of asset IPs.
$ASSET_OS_LIST	A comma delimited list of asset OS's.
$ASSET_NAME_LIST	A comma delimited list of asset names.
$VULN_ID_LIST	A comma delimited list of vulnerability IDs.



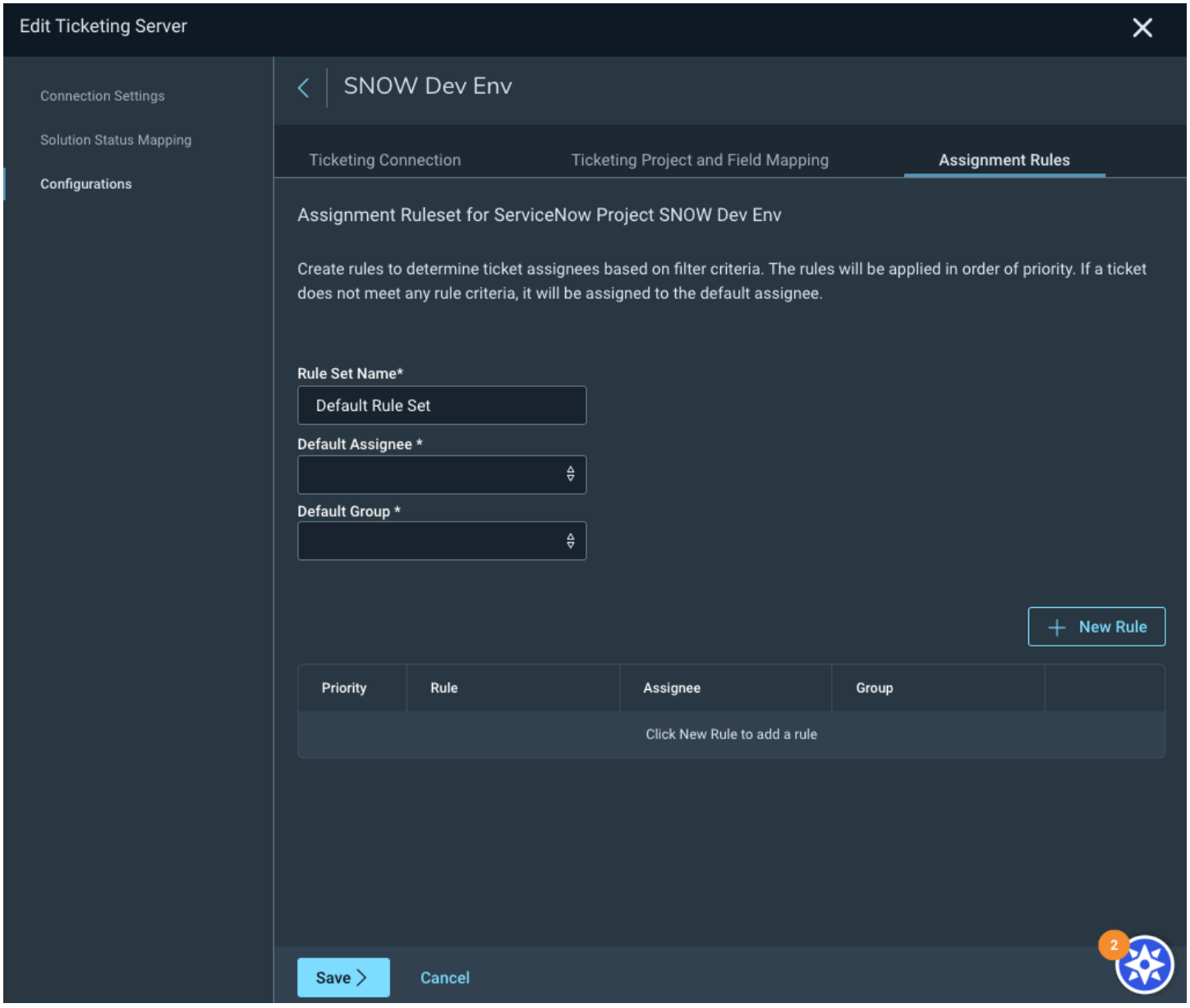
8. Click Save.
9. Use the **Assignment Rules heading** to create a ruleset defining how the tickets will be assigned to users and groups in ServiceNow.

    - There can be multiple rulesets that define different remediation teams (HelpDesk, Server Administrators, Developers, etc.). The available assignees and groups selected in the associated dropdown menus will come from ServiceNow.

        i. If the desired user and/or group is not seen, consult with your ServiceNow Administrator to ensure those user(s) and group(s) exist.

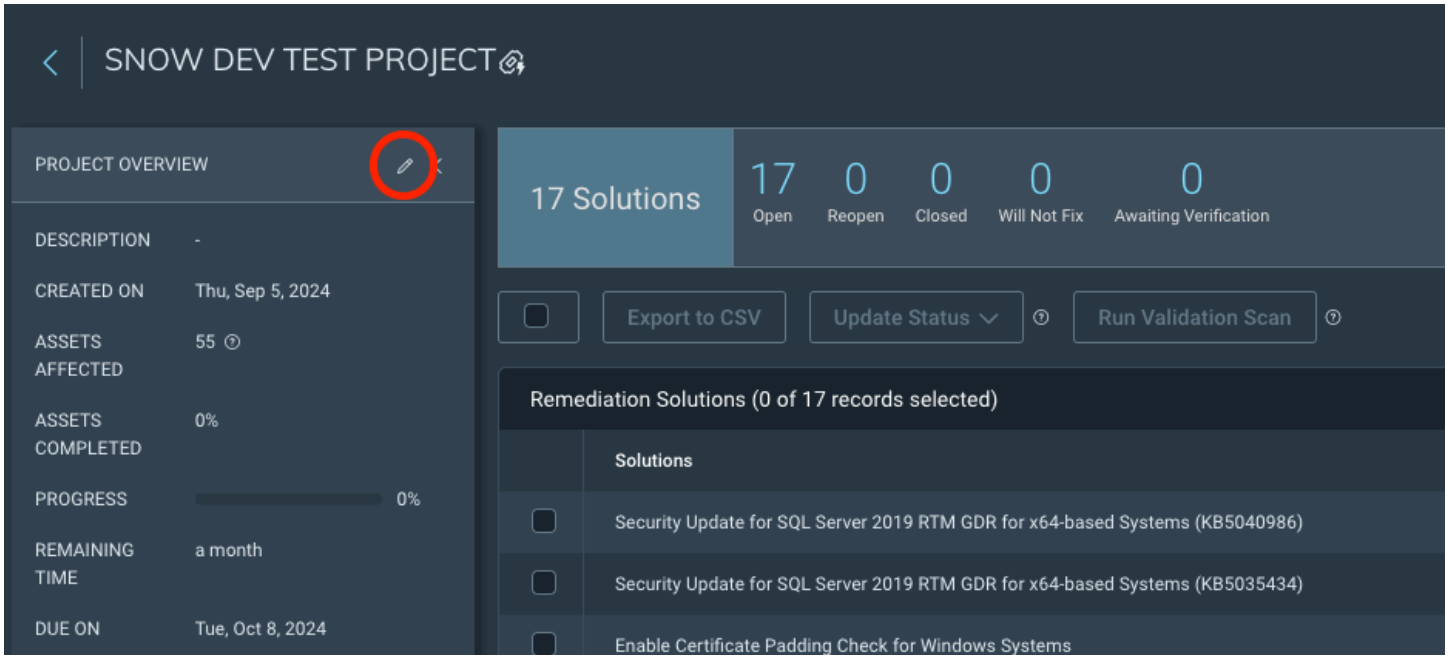
    - The ruleset priority determines in what order the rules are applied when the system determines who gets assigned the ServiceNow ticket.

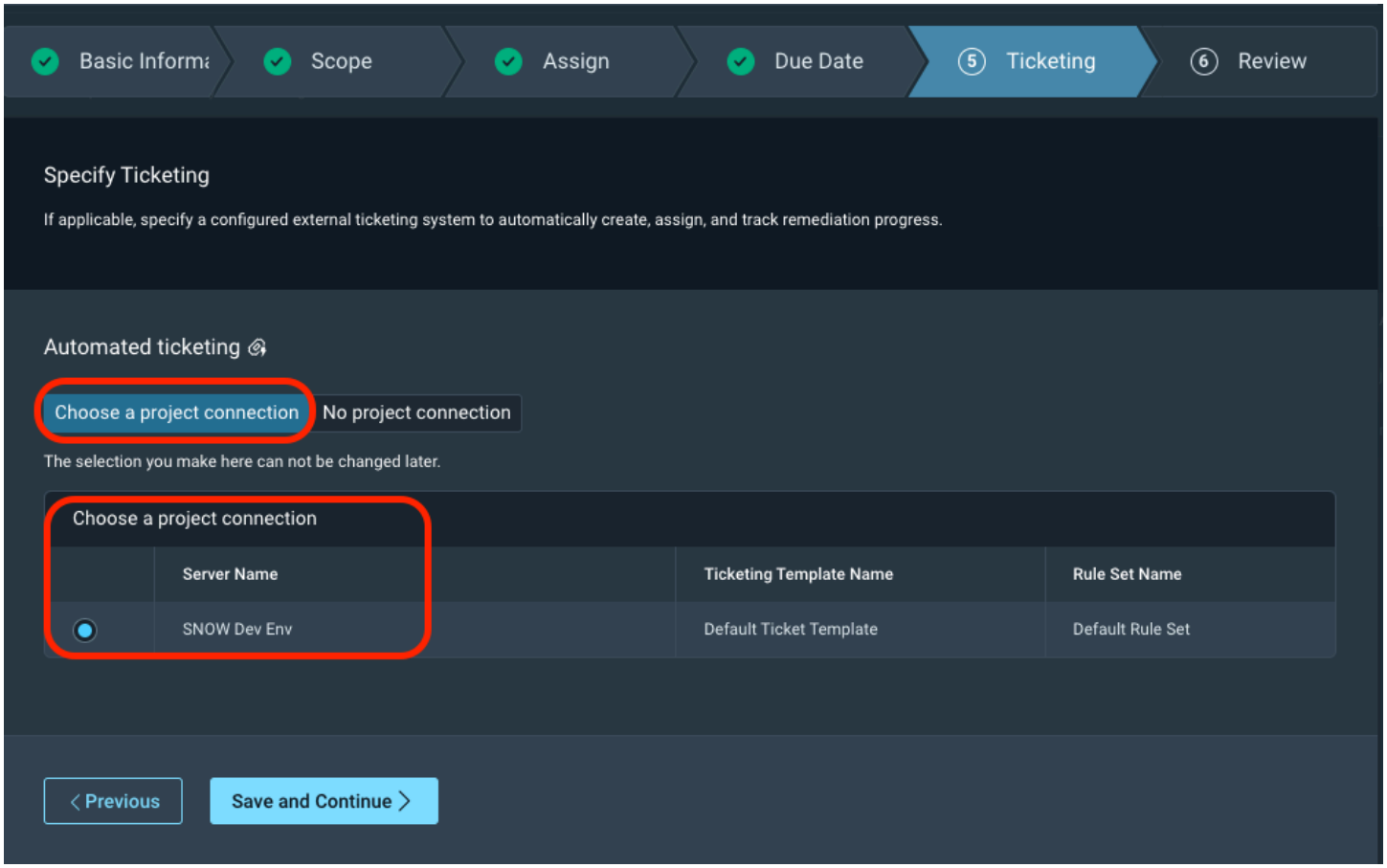
- The ruleset criteria is defined using InsightVM's Query Builder to filter down the assets. Please refer to our documentation for more details on Query Builder and its syntax.
- A **Default Assignee** and a **Default Group** must be defined as the user and group that will receive the ServiceNow tickets if none of the rulesets match. This could be described as the Security team so they can verify internally who the ticket should be assigned to.



10. Click Save.
11. Now that the ticketing connection has been configured, in step 5 of the *Remediation Projects wizard,* you can select a ticketing connection for the project to use. Once the project is created successfully, InsightVM will begin creating tickets based on the configuration of the ServiceNow ticketing connection.

12. For projects that existed prior to the ticketing connection setup, you can edit those projects to include the ticketing connection as well.
    - Be sure to choose the ticketing connection as well as the correct ticketing template/ruleset combination to ensure the created tickets are assigned to the correct remediators in ServiceNow:





If you run into issues configuring a ticketing connection, please speak with your Technical Account Manager (TAM), your Customer Success Manager (CSM), or your Customer Advisor (Managed VM (MVM) and Managed Threat Complete (MTC) customers) or simply open a case with Rapid7 Support.