Defining ServiceNow Instances

Connecting ServiceNow with QualityClouds · https://community-staging.qualityclouds.com/qcdocs/qc/connecting-servicenow-qualityclouds/defining-servicenow-instances/

Prerequisites:

Before performing these steps, make sure you have the following information:

- Login credentials to the Admin Quality Clouds portal - https://portal.qualityclouds.com/

Setting up your instances

In order to be able to scan your instances, you need to point Quality Clouds to them.

→ To create an instance in Quality Clouds

If using Certificate-Based Authentication

Enforce security using Certificate-based authentication for ServiceNow.

- **What is Certificate-based authentication?**

Certificate-based authentication verifies user logins or API requests using trusted certificates issued by a Certificate Authority (CA). This authentication method can be used to authenticate requests to ServiceNow SOAP and REST APIs. Since the interaction between Quality Clouds and ServiceNow instances is implemented via the REST API, it is possible to support Certificate Based authentication for this interaction, as an alternative to the Basic authentication mechanism.

- **Why use a certification-based authentication?**

To provide enhanced security in the connection between Quality Clouds and your ServiceNow instance.

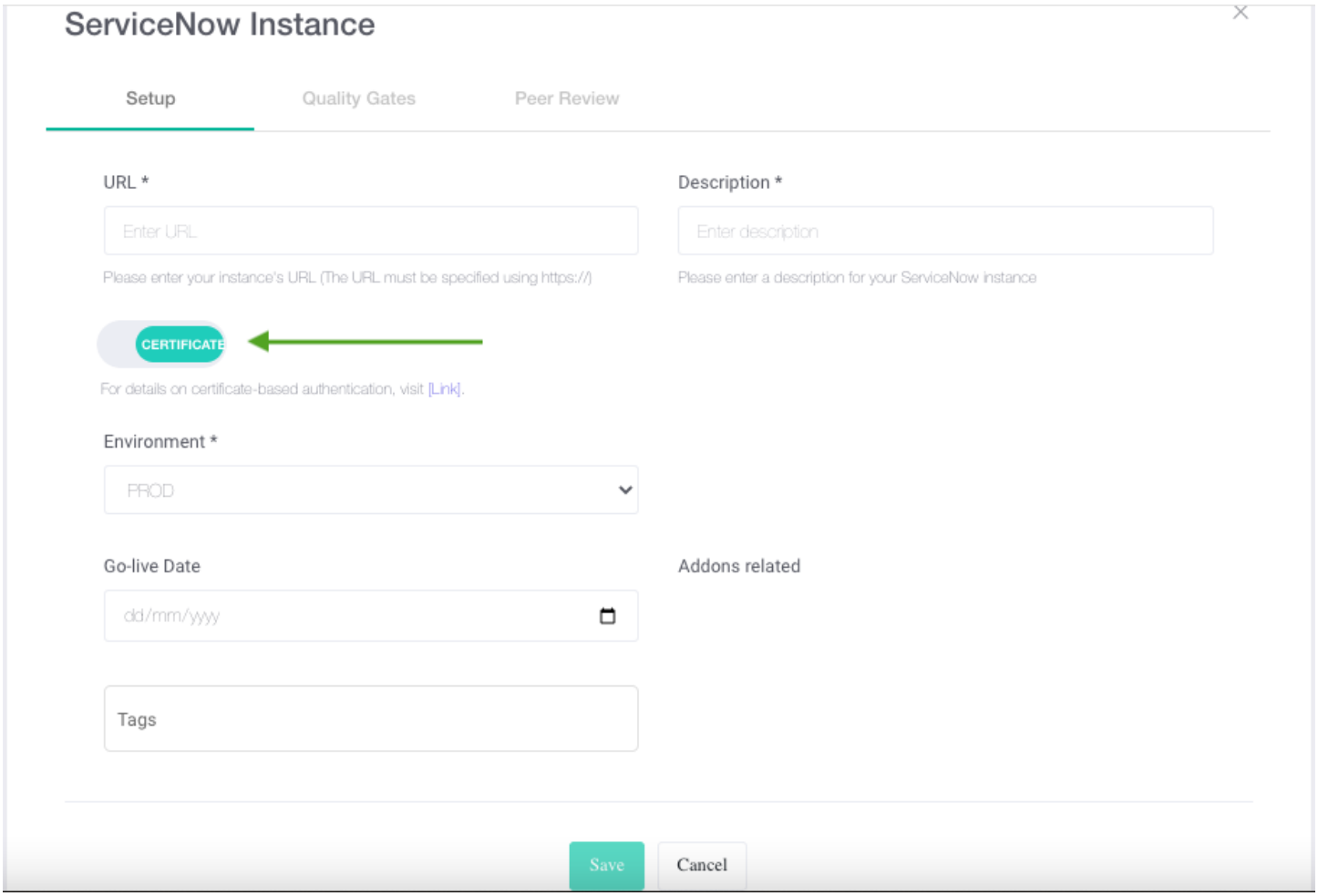
- **How does the certificate-based authentication work in Quality Clouds?**

1. Verify your instance supports Certificate-based authentification by following this step:
   - Append **/adcv2/supports_tls** to your instance URL and open it in a browser.
   If the response is "**True**" it means your instance supports it. However, if the response is a **402 error**, you will need to contact ServiceNow and ask to enable ADCv2 and ADC-to-APP mTls
2. Download the public certificate from Quality Clouds
   - Certificate valid **until** April 4th, 2025 11 am CEST here
   - Certificate valid **from** April 4th, 2025 11 am CEST here
3. Install the certificate in ServiceNow instance. Follow the ServiceNow instructions on how to install the Quality Clouds certificate in your instance.
4. Make sure that the installed Quality Clouds certificate is mapped to a user with the required permissions to enable a Quality Clouds scan.
5. Activate the 'Certificate' toggle in the Quality Clouds Admin portal, ServiceNow instance section.
6. Verify the connectivity by clicking the 'Test connection' icon.

1. Login to the Quality Clouds Admin portal at https://portal.qualityclouds.com/.
2. Go to **Account**.
3. Go to the **Instances** section.
4. Select the ServiceNow tab (if you use several SaaS with Quality Clouds).
5. Click **+** (Add button).
6. Enable the '**CERTIFICATE**' toggle.
7. Fill in the following information:
   - **URL** – URL of the ServiceNow instance. If your ServiceNow instance uses SSO or any other external authentication method, make sure that the account you provide has local authentication in ServiceNow (does not need to be authenticated by external providers) and is able to use the REST API.
   - **Description** -Short and meaningful description of the instance. For example: MyCompany UAT
   - **Environment** – Environment type of the instance. This is used to add descriptive context to your instance.NoteServiceNow production (PROD) instances are subject to an extra check: *Debugging properties enabled in production environments.*

- **Go-live Date** – Date on which the instance was first started, serves as a baseline for instance changes.
- **Tags** – Use tags to add specific information for better instance recognition.

8. Click **Save**.

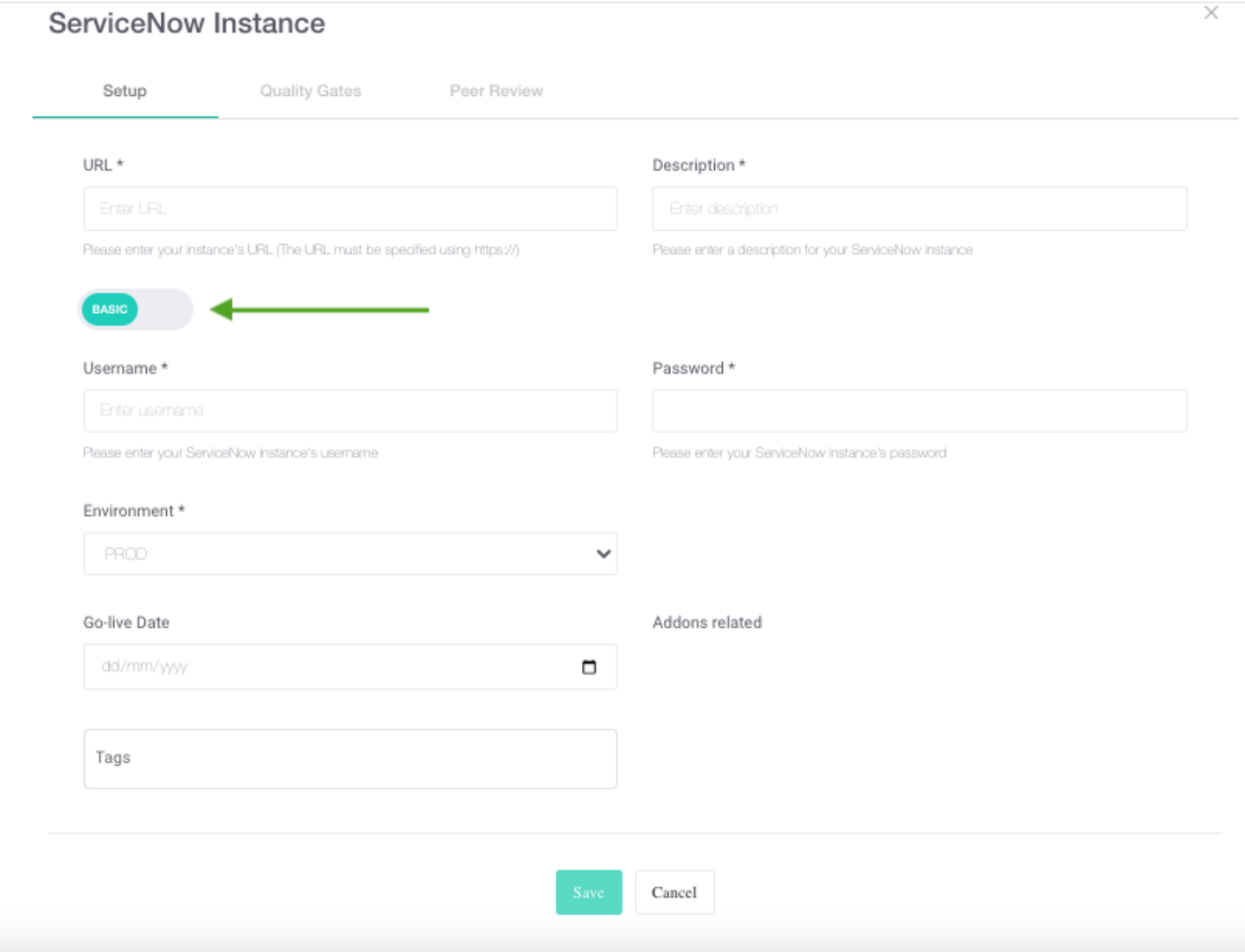


If using Basic Authentication

1. Login to the Quality Clouds Admin portal at https://portal.qualityclouds.com/.
2. Go to **Account**.
3. Go to the **Instances** section.
4. Select the ServiceNow tab (if you use several SaaS with Quality Clouds).
5. Click **+** (Add button).
6. Fill in the following information:

- **URL** - URL of the ServiceNow instance. If your ServiceNow instance uses SSO or any other external authentication method, make sure that the account you provide has local authentication in ServiceNow (does not need to be authenticated by external providers) and is able to use the REST API.
- **Description** -Short and meaningful description of the instance. For example: MyCompany UAT
- **Username** and **Password** - ServiceNow access credentials to the instance.
- **Environment** - Environment type of the instance. This is used to add descriptive context to your instance.NoteServiceNow production (PROD) instances are subject to an extra check: *Debugging properties enabled in production environments.*
- **Go-live Date** - Date on which the instance was first started, serves as a baseline for Org changes.
- **Tags** - Use tags to add specific information for better instance recognition.
- **Addons related** - These are the add-ons included in your contract.

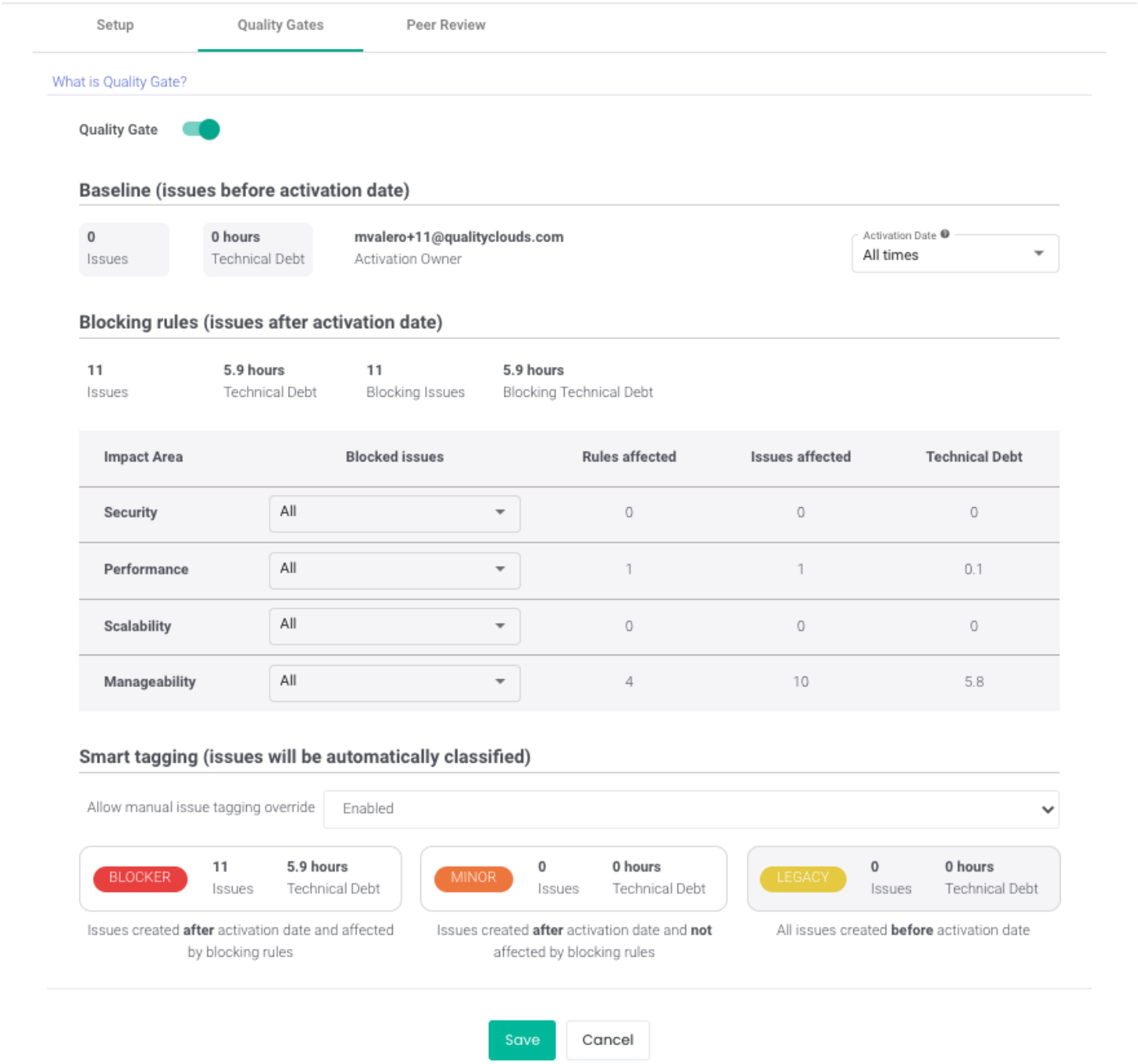
7. Click **Save**.



→ Configure the Quality Gates

1. When setting or editing an instance, click on the 'Quality Gates' tab.
2. Enable the Quality Gates toggle.
3. Add the Activation Date.
4. Configure the Blocking rules table and smart tagging.
5. Click '**Save**'.

Click **here** to learn how Quality Gates work.



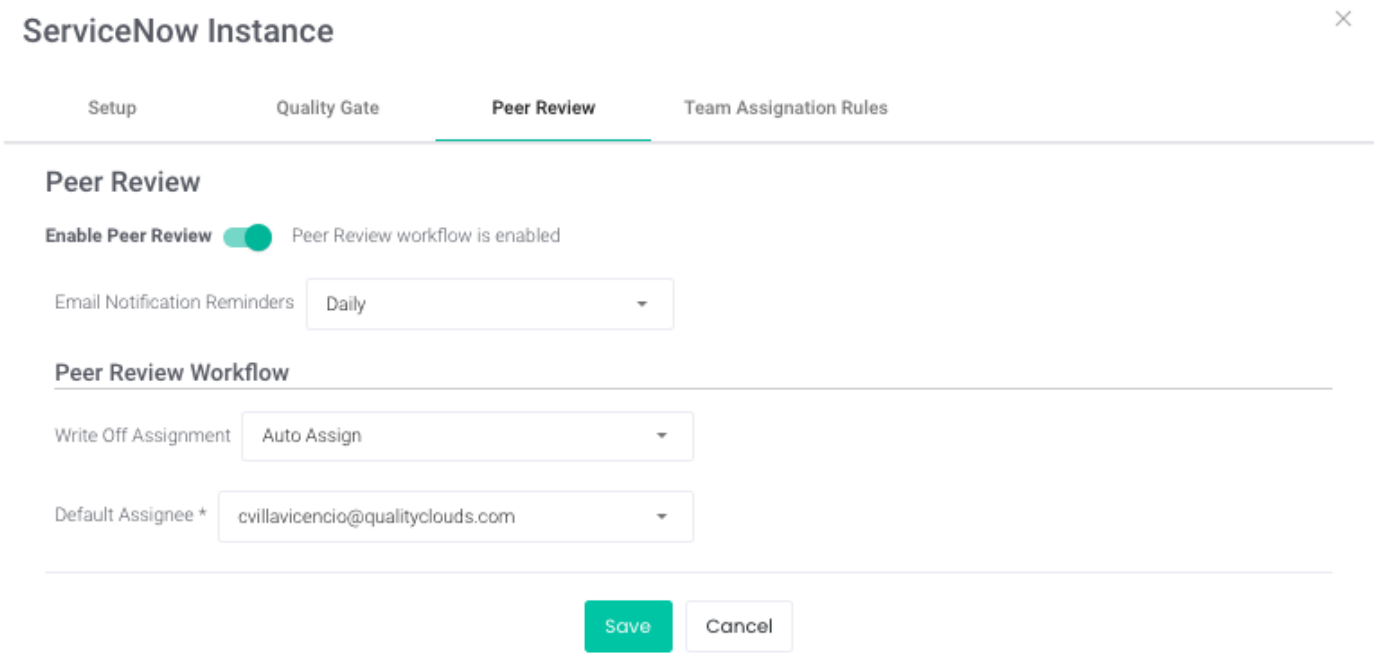
→ Configure the Peer Review

1. When setting or editing an instance, click on the 'Peer Review' tab.
2. Enable the Peer Review toggle.
3. Select when to get notified when Peer Reviews are pending: None, Daily, Weekly or Monthly.
4. In the Peer Review Workflow section select '**Write Off assignation**':

- Manual Assign: Requests are unassigned, requiring the customer to select an approver manually from the Peer Review dashboard | *It will hide the Default Assignee drop-down menu.*
- Auto Assign: All requests are automatically assigned to a predetermined approver | *It will show the Default Assignee and there won't be any other option than to select one person from the list.*

5. Select the Default assignee email on the dropdown menu. Enable it if you want the default assignee to be notified when a write-off is assigned.
6. Click '**Save**'.

- Manual Assign will hide the Default Assignee drop-down menu.
- Auto Assign will show the Default Assignee and there won't be any other option than to select one person from the list.



You can now continue with the following steps:

1. Test connectivity.
2. Schedule scans or Run scans manually.