Netskope Integration Guide

Utilize Netskope's industry leading v1 API to integrate Netskope with GreyMatter. This integration prevents sensitive data from being exfiltrated from your environment by risky insiders or malicious cybercriminals who have breached your perimeter.

Important: The Netskope v1 integration uses the v1 API permission control, which is slated for deprecation in the near future. We strongly recommend customers use Netskope's new v2 API by integrating the Netskope v2 CASB integration instead. Learn more about the Netskope v2 CASB integration.

1. **Determine the architecture structure of your environment:**

This integration requires your environment to support vendor cloud deployments through **port 3443**.

If you already know that your architecture supports vendor cloud deployments, continue to step 2. If you are unsure whether your organization can use this deployment type, please ensure compatibility before continuing.

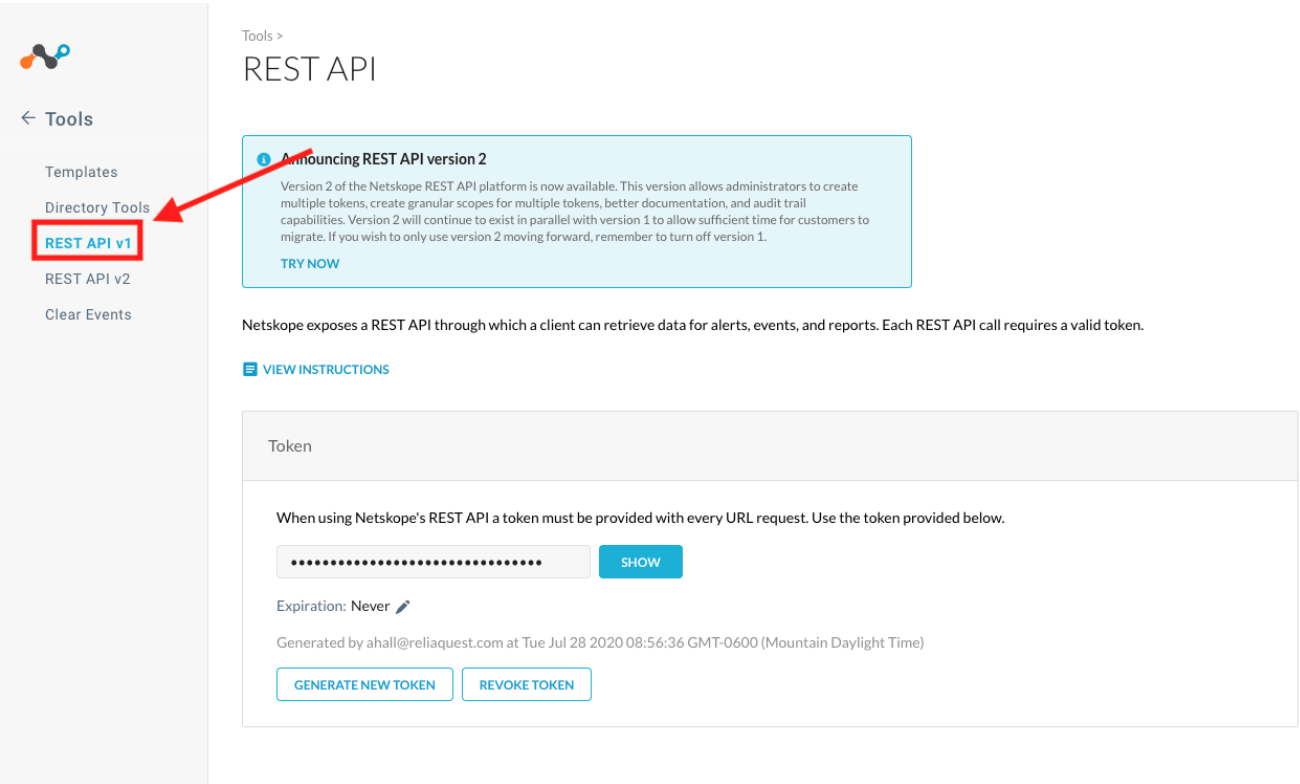
2. **Generate an API v2 Token within the Netskope console**

For this integration, you will need the following information:

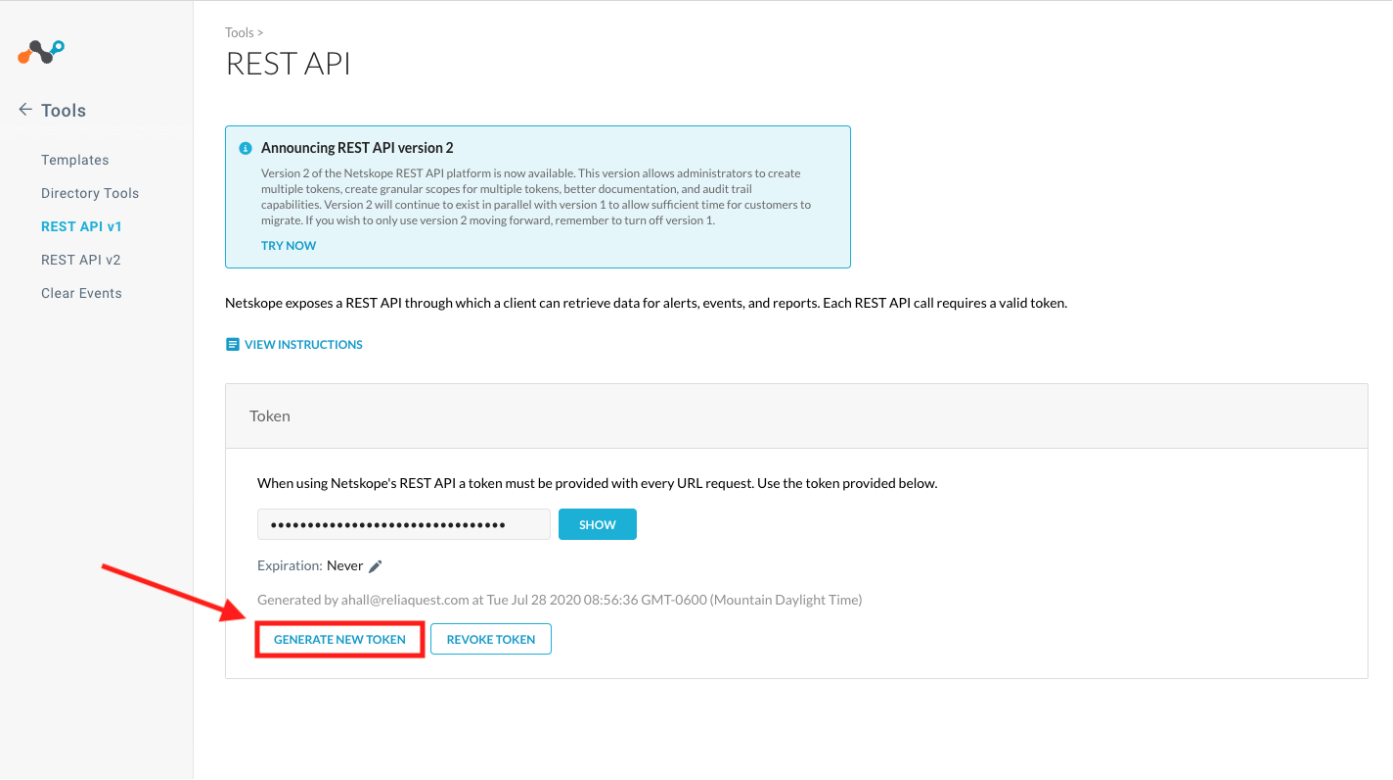
- URL: https://<tenant>.goskope.com
- API token

Generate an API token by following the steps below:

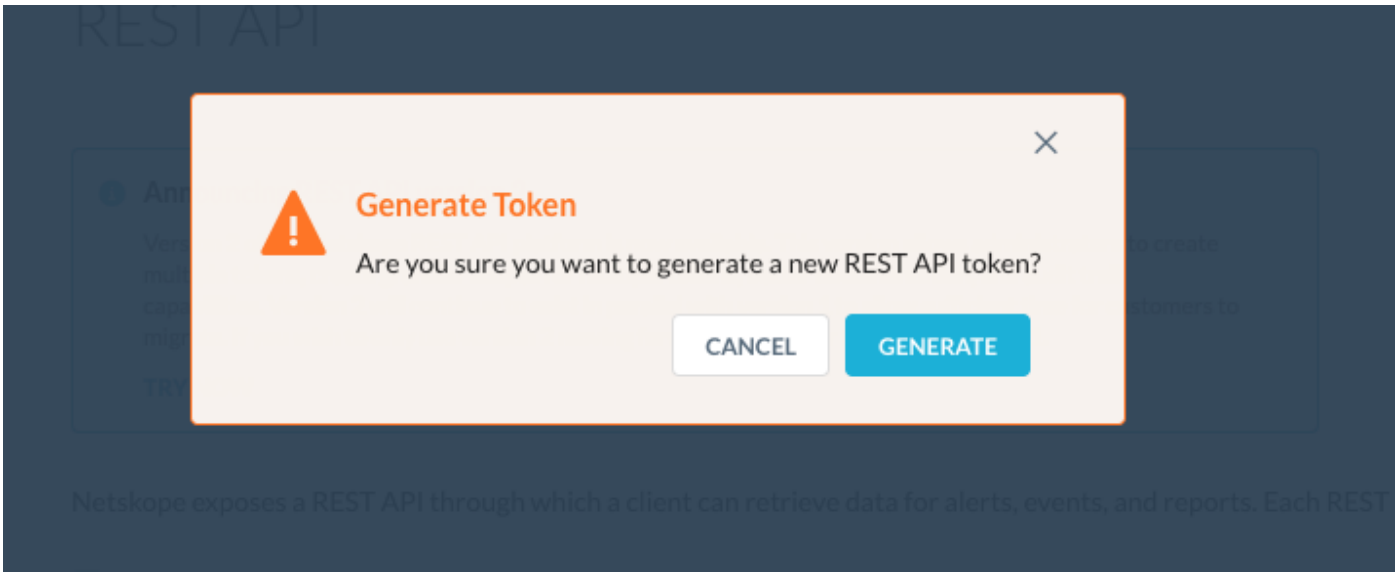
1. Go to **Settings > Tools** and then click the REST API v2 link.



2. Click the **Generate New Token** button.



3. In the confirmation dialogue box, click the **Generate** button to confirm you want to generate a new REST token.



4. Copy the token and have it ready to send to your CSM.

Important: There are no restrictive permissions required to generate a new v1 API Token. When you supply the token to our team, you will have access to the Playbooks once the integration is complete.

3. Fill Out the ServiceNow Form

Once you've collected the URL and the API token listed in Step 2, notify your CSM/Implementation Specialist and they will send you a small digital form. Complete this form and our team will finish the process. Keep in mind, your integration cannot be constructed until you have completed this form.

4. Collect Variables and Test Playbooks

Once your integration is complete, go to the Respond tab in GreyMatter and use the variables below to test the various playbooks.

Collect the following variables:

- Quarantine Profile ID
- File ID

PLAYBOOK NAME	DESCRIPTION	REQUIRED INPUT VARIABLE(S)	MULTI-VALUE SUPPORT FOR INPUT VARIABLE(S)	EXPECTED OUTPUT RESULTS
Get Quarantine List	Get a list of all files and/or hashes currently blocked from network execution within the specified technology.	*No inputs needed*	Yes	Receive list of blocked files and/or hashes.
Add File to Quarantine List	Adds the specified file to a quarantine list to prevent execution on the network. Can only be executed if Quarantine Profile ID is set in Integration configuration.	Quarantine Profile ID* **The user profile associated with Netskope*. File ID* (MD5 or SHA256) **The Netskope Hash version.*	N/A	Confirmation of specified file being added to ban list.
Remove File From Quarantine List	Removes the specified file from a quarantine list to allow execution on the network. Can only be executed if Quarantine Profile ID is set in Integration configuration.	Quarantine Profile ID* **The user profile associated with Netskope*. File ID* (MD5 or SHA256) **The Netskope Hash version.*	N/A	Confirmation of specified file being removed from ban list.

ReliaQuest Team Instructions*

**Only accessible to ReliaQuest employees*

Netskope Integration Guide

Disclaimer: All customer data is classified and handled as 'Confidential' (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.