BOMGAR™

Bomgar Vault 17.2.1
Discovery Tool Guide

TC:11/27/2017

Table of Contents

Overview of the Bomgar Vault Discovery Tool

Discovery is an essential part of keeping your environment secure. With the Bomgar Vault Discovery Tool, you can identify vulnerable privileged accounts and learn important information about those accounts, including:

- **Platform:** The platform type of endpoints associated with the scanned accounts.
- **Location:** The location of the accounts within your network.
- **Credentials:** Information about the credentials associated with the accounts.

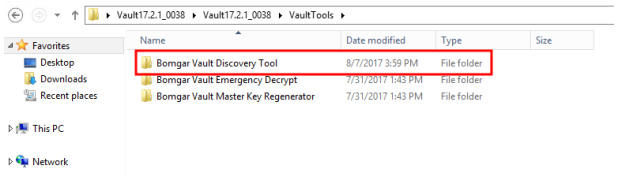
Once the discovery tool has uncovered these accounts, you can import them into the Bomgar Vault application, where the accounts can be properly validated, rotated, and managed. Using the Bomgar Vault Discovery Tool gives you key insight into the most vulnerable areas of your network and helps you prevent security breaches within your organization.

This guide walks you through how to use the Bomgar Vault Discovery Tool to scan your privileged accounts and how to export this information.

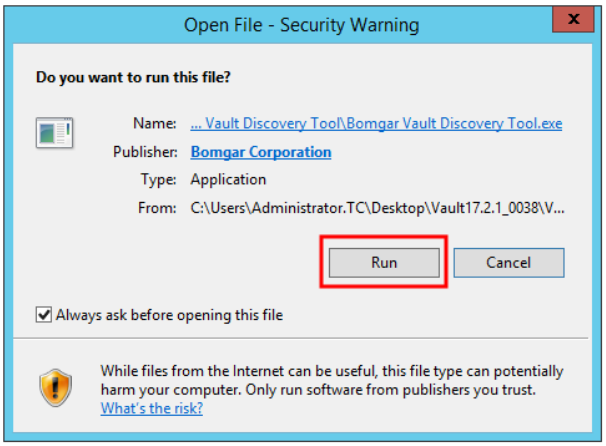
Start the Bomgar Vault Discovery Tool

After you receive your Bomgar Vault installer and extract the files to your Vault server, you can use the Bomgar Vault Discovery Tool to uncover privileged accounts within your network. To access and start the discovery tool, follow the steps below.

1. Locate the **Vault x.x** installation folder on your Vault server and go to **Vault x.x > VaultTools > Bomgar Vault Discovery Tool**.



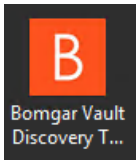
2. In the **Bomgar Vault Discovery Tool** folder, double-click **Bomgar Vault Discovery Tool Setup x.x.xxx.exe.**
3. If you see an **Open File - Security Warning** prompt, click **Run**, and the discovery tool starts.



Discover Privileged Accounts on the Network

Start the Bomgar Vault Discovery Tool Application

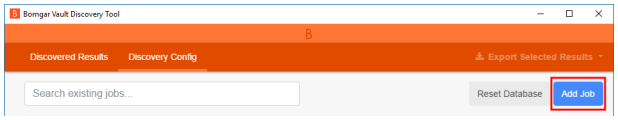
After you have installed the Bomgar Vault Discovery Tool, a Bomgar Vault Discovery Tool shortcut appears on your machine. Double-click the shortcut to start the application.



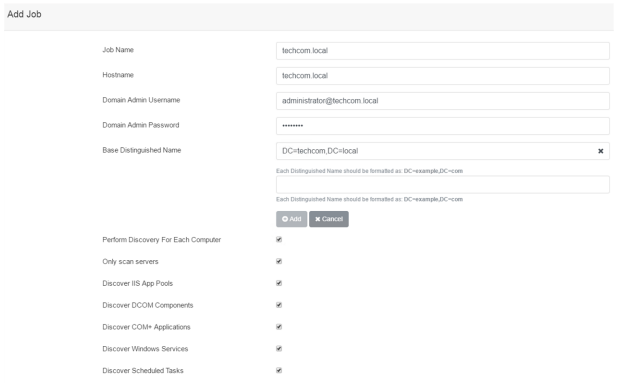
Configure a New Discovery Job

When opening the discovery tool for the first time, you are automatically taken to the **Discovery Config** section to configure your first discovery job.

1. Click **Add Job**.



2. From the **Add Job** page, enter the following information:



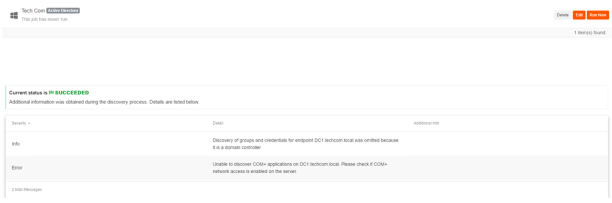
   - **Job Name:** A friendly name for the discovery job, which can be used to search for the job later.
   - **Hostname:** The hostname of the domain you wish to scan for accounts.
   - **Domain Admin Username:** The username associated with the administrator account for the domain.
   - **Domain Admin Password:** The password associated with the administrator account used for the domain.
   - **Base Distinguished Name:** Add the **Base Distinguished Name** for the domain. "DC=example, DC=com."
   - **Perform Discovery for Each Computer:** Choose this option if you want the discovery tool to scan each computer discovered in your domain. You can also choose to restrict or to expand the parameters of your scan further by selecting the options below:
     - **Only scan servers**
     - **Discover IIS App Pools**
     - **Discover DCOM Components**
     - **Discover COM+ Applications**
     - **Discover Windows Services**
     - **Discover Scheduled Tasks**

3. Once you have configured your discovery job, click **Validate**. Then the discovery tool checks to see if it can connect to the domain using the information provided. If the validation is successful, a green box appears stating the job has been tested. If the validation is unsuccessful, a red box appears with details about why it was unable to test the job.

4. After a successful validation, click **Save**.

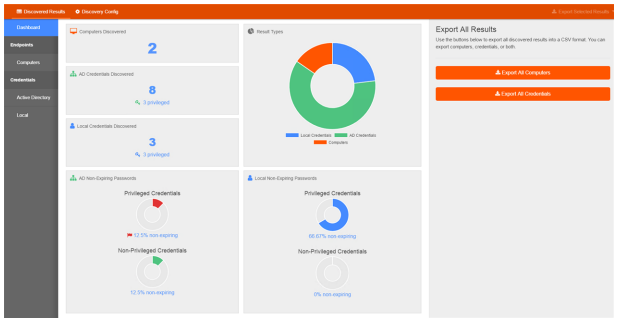
Start a Scan

1. After the job has been created, the **Run Now** button becomes available beside the job. Click **Run Now** to start a scan.
2. While a scan is in progress, a status of **Currently running** is present. When the scan has successfully completed, the status changes to **Succeeded**. Click on the job for more information or to view errors that occurred during the scan.



Review and Export All Results

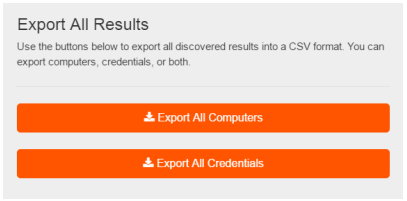
1. To review the results of a scan and to export information, click on the **Discovered Results** tab.
2. Review the **Dashboard** to see a total number of all endpoint systems and accounts found.



Note: *The dashboard keeps a running total of systems and accounts discovered from all jobs performed. Once you have performed many discovery jobs, a total is tallied for all jobs on the dashboard.*

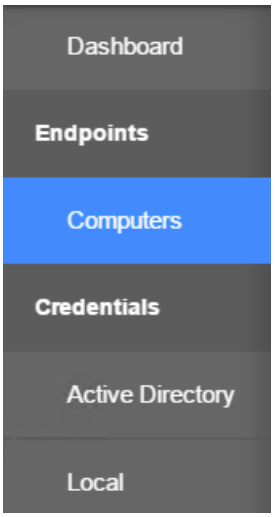
- **Computers Discovered**
- **Groups Discovered**
- **Domain Groups Discovered**
- **Credentials Discovered**

3. From the **Dashboard**, you can choose to **Export All Computers** or **Export All Credentials.** These actions generate a CSV file, which you can save to your machine.

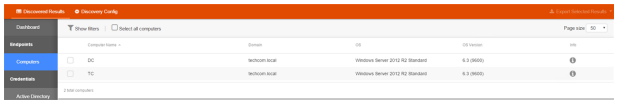


Select and Export Specific Endpoint Results

If you wish to see a list of endpoints discovered, click the **Computers** option located on the left side menu. A list of all discovered computers appears.



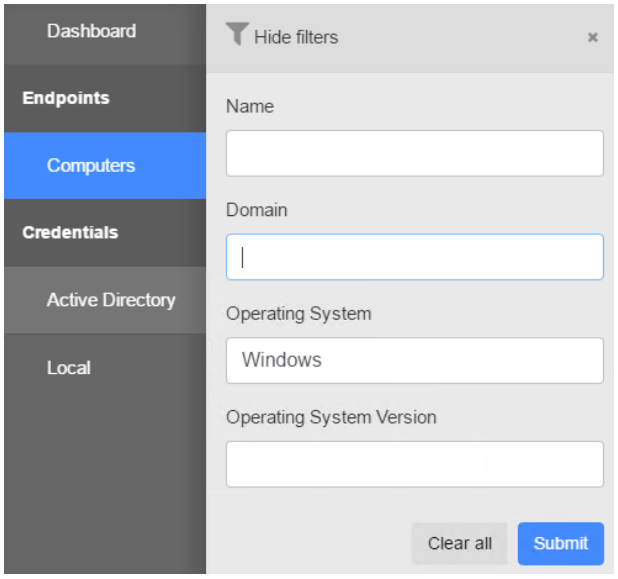
To select individual results, check the box beside the list item. You may select multiple computers from the list. Or, you can check **Select all computers** to check all items.



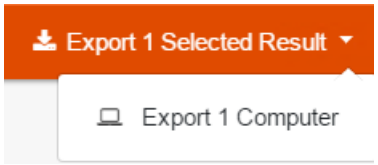
You can also filter the results by clicking **Show Filters** at the top of the page. When selected, the following fields appear:

- **Name**
- **Domain**
- **Operating System**
- **Operating System Version**

You can filter the results based on this information. Type in your criteria and click **Submit**.

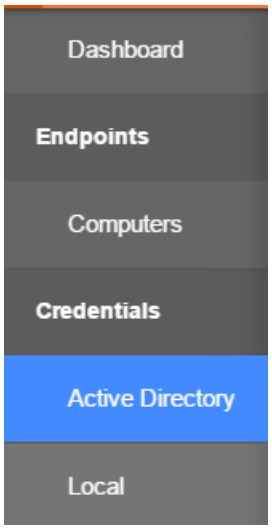


The results update to match the criteria you entered. After filtering the results, you can export the results to CSV by clicking **Export Selected Results** located in the top right.

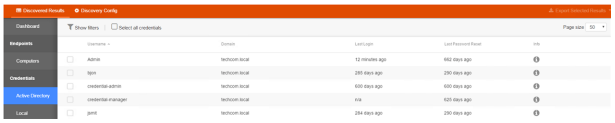


Select and Export Specific Active Directory Account Results

If you wish to see discovered Active Directory accounts, click the **Active Directory** option on the left side menu. A list of all discovered accounts appears.



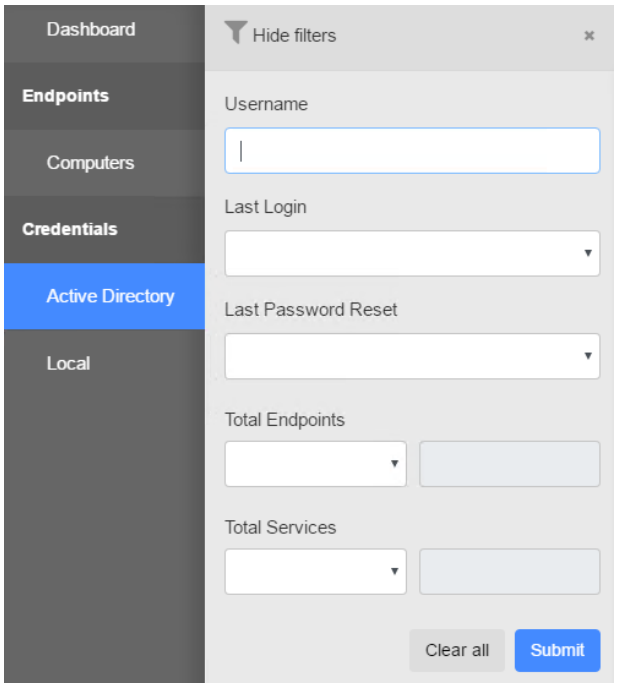
To select individual results, check the box beside the list item. You may select multiple accounts from the list.



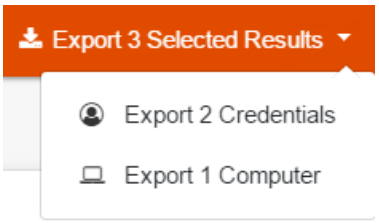
You can also filter the results by clicking **Show Filters** at the top of the page. When selected, the following fields appear:

- **Username**
- **Last Login**
- **Last Password Reset**
- **Total Endpoints**
- **Total Services**

You can filter the results based on this information. Type in your criteria and click **Submit**.

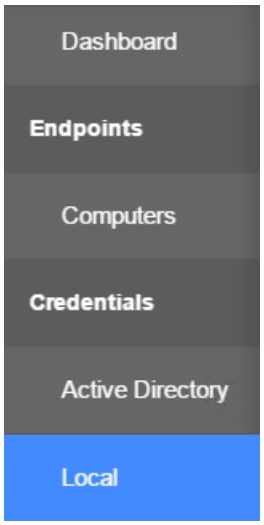


The results update to match the criteria you entered. After filtering the results, you can export the results to CSV by clicking **Export Selected Results** located in the top right.

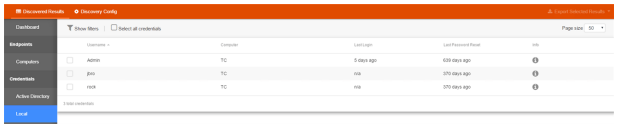


Select and Export Specific Local Account Results

If you wish to see discovered Local accounts, click the **Local** option on the left side menu. A list of all discovered accounts appears.



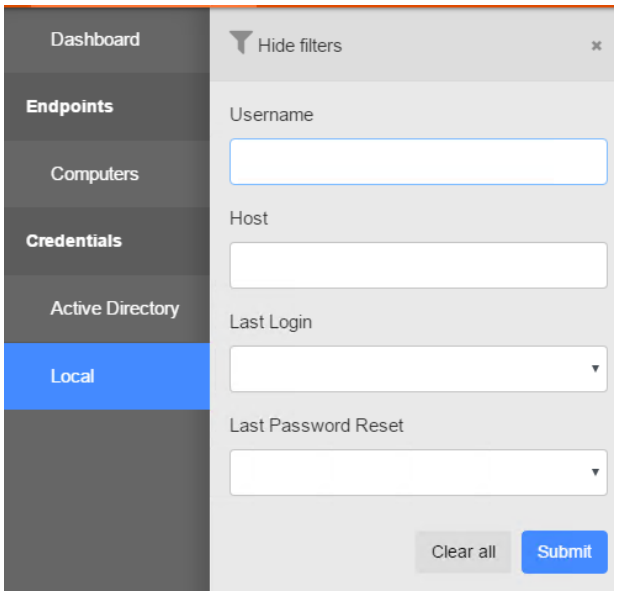
To select individual results, check the box beside the list item. You may select multiple accounts from the list.



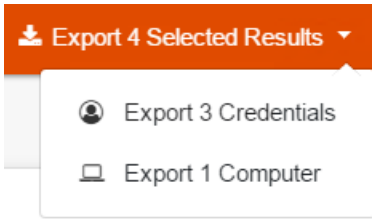
You can also filter the results by clicking **Show Filters** at the top of the page. When selected, the following fields appear:

- **Username**
- **Host**
- **Last Login**
- **Last Password Reset**

You can filter the results based on this information. Type in your criteria and click **Submit**.



The results update to match the criteria you entered. After filtering the results, you can export the results to CSV by clicking **Export Selected Results** located in the top right.



Import Results into Bomgar Vault

Once you have exported your findings to a CSV file and saved it to your machine, you can import the endpoints and credentials discovered into Bomgar Vault. This allows you to start mananging and rotating the credentials discovered in your network. Before import, make sure the following are in place:

- **Configuration:** Make sure you have configured all settings in Bomgar Vault. You can review the settings by logging into your Bomgar Vault site and going to **Administration > Settings**.
- **Version:** Check to make sure you are using a version of the Discovery Tool that is compatible with your Vault site. Bomgar Vault 17.2.1 and later requires Bomgar Vault Discvoery Tool version 1.0 or later.
- **Order:** When starting the import process, you must import endpoints before credentials.

Follow the steps below:

1. Log into your Vault site. Go to **Endpoints > Endpoints**.
2. Click the **Bulk Insert** button.
3. Click the **Upload File** button.
4. Locate the CSV file you saved from the discovery tool export. Select it.
5. Click **Open**.
6. Click the **Validate File** button.

7. Once validated, click the **Import Endpoints** button.
8. When import is complete, click the **Close** button.

The endpoints should then be available in the **Endpoints** section. Then, repeat the same steps for your credentials by going to **Credentials > Credentials** and clicking the **Bulk Insert** action.

Notes:

- Once importing is complete, credentials and endpoints should be associated without further configuration.
- While the discovery tool does scan information like scheduled tasks and services, this information does not import into Bomgar Vault.

Frequently Asked Questions about the Bomgar Vault Discovery Tool

How does the Bomgar Vault Discovery Tool scan my network for privileged accounts?

The discovery tool uses native .NET 4.5 libraries to perform ping scans to detect endpoints on the network. It is important to note that Nmap is not used to determine if endpoints are responsive.

Can I customize what parts of my network are scanned?

Yes. From the **Add/Edit Job** pages, you can choose which components of your network you would like scanned.

What platform types are scanned using the Bomgar Vault Discovery Tool?

Windows and Linux endpoints can be scanned using the tool.

How does the Bomgar Vault Discovery Tool know which ports are available for scanning Windows endpoints?

NetStat is used to determine which TCP connections are active and available.

Does the Bomgar Vault Discovery tool attempt binding?

Yes. When using Active Directory credentials, the tool performs enumeration over port 389.