BOMGAR™

Bomgar Vault-PAM Integration Guide

TC:9/21/2016

Table of Contents

Bomgar Privileged Access Management and Bomgar Vault Integration Guide **3**

Workflow Summary 3

Privileged Access Management Prerequisites 3

Vault Prerequisites 3

Install and Configure the Endpoint Credential Manager **4**

System Requirements **5**

Configure a Connection to Bomgar Vault **7**

Configure the Vault Plugin **8**

Configure the Integration **8**

Troubleshooting the Integration **9**

Bomgar Privileged Access Management and Bomgar Vault Integration Guide

When Bomgar Vault is integrated with Bomgar Privileged Access Management (PAM), privileged access sessions become more secure due to Vault's seamless credential injection. This helps companies secure shared credentials for privileged users as well as manage and rotate passwords for privileged accounts to improve security and compliance.

Workflow Summary

- Confirm the location in which you will install the Endpoint Credential Manager (ECM).
    - Ensure the ECM can connect to the PAM server over port 443.
    - Ensure the ECM can connect to the Vault server over port 443.
    - Use a static IP for the machine where the ECM resides.

> ***Note:*** *Vault whitelists access based on IP address.*

- Set up the prerequisites.
    - Create an admin account in PAM as a service account.
    - Enable the API in Vault and add the IP address of the system where the ECM will be located.
- Install the ECM.
    - Set up the PAM information.
    - Install the Vault plugin in the ECM.
    - Configure the Vault connection information in the plugin.
- Test the connection and troubleshoot issues as necessary.

Privileged Access Management Prerequisites

- Vault integration requires PAM version 15.3.2 or higher.
- Create an API administrator account, if one does not already exist.

> ***Note:*** *This user must be a PAM system administrator.*

- Ensure domain authentication to PAM is functional. For more information, see Security Providers at https://www.bomgar.com/docs/privileged-access/getting-started/admin/security-providers.htm.
- Ensure that at least one endpointremote system is configured in PAM and that you can connect to it.

Vault Prerequisites

- Under the **Administration > Settings > API Configurations** tab, ensure that the API is enabled. For more information, see API Settings at https://www.bomgar.com/docs/vault/how-to/settings/api-settings.htm.
- Install the Bomgar Endpoint Credential Manager (ECM). For more information, see Install and Configure the Endpoint Credential Manager at https://bomgar.com/docs/vault/integrations/vault-integration/install-ecm-config.htm.

- Download the Bomgar Vault plugin at https://help.bomgar.com and load the Vault module.
- Configure the Vault plugin.

Install and Configure the Endpoint Credential Manager

The Bomgar Endpoint Credential Manager (ECM) allows you to quickly configure your connection. The Endpoint Credential Manager must be installed on your computer to enable the Bomgar ECM service.

System Requirements

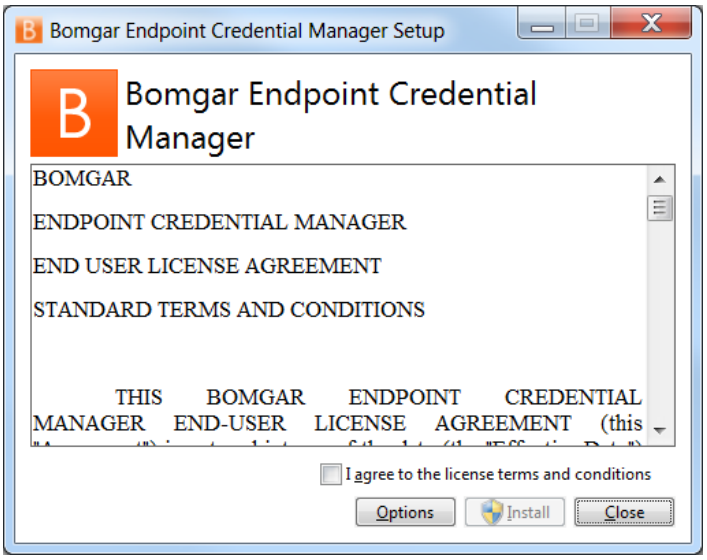
- **Windows Vista or newer, 64-bit only**
- **.NET 4.5 or newer**

Note: *When installing the Endpoint Credential Manager for use with Bomgar Vault, we recommend installing it on a machine with a static IP address to avoid potential issues with Vault's IP whitelisting for the API.*

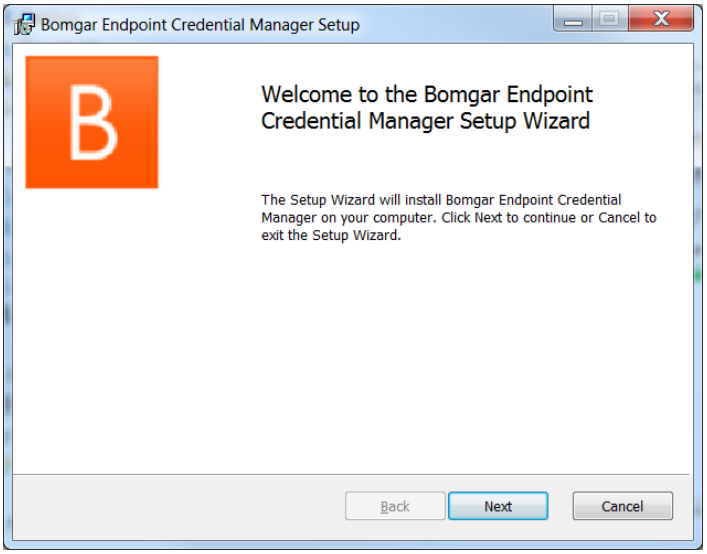
1. To begin, download the **Bomgar Endpoint Credential Manager** from Bomgar Support at https://help.bomgar.com/. Start the **Bomgar Endpoint Credential Manager Setup Wizard**.

2. Agree to the EULA terms and conditions. Mark the checkbox if you agree, and click **Install**.

Note: *You will not be allowed to proceed with the installation unless you agree to the EULA.*



3. Click **Next**.

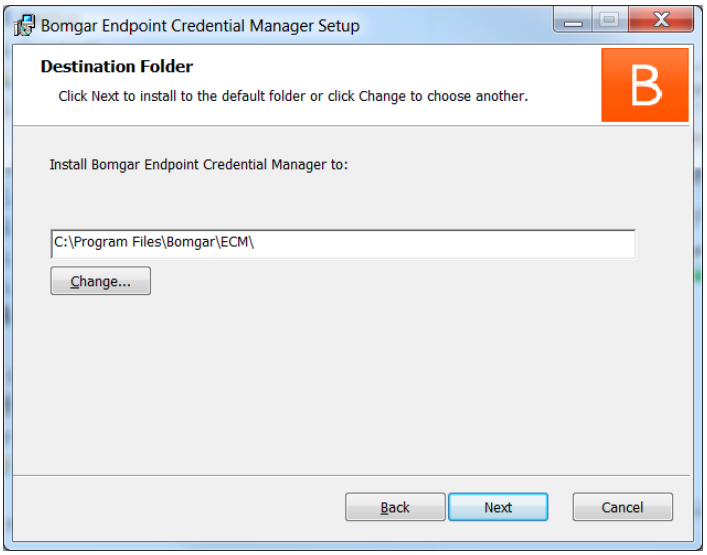


4. Choose a location for the Credential Manager and click **Next**.

5. On the next screen, you can begin the installation or review any previous step.

6. Click **Install** when you are ready to begin.

7. The installation will take a few moments. On the screen, Click **Finish**.



Configure a Connection to Bomgar Vault

Using the ECM Configurator, set up a connection to Bomgar Vault.

1. Locate the ECM Configurator you just installed using the Windows Search entry field or by viewing your Start menu programs list.
2. Run the program to begin establishing a connection.
3. When the ECM Configurator opens, complete the fields. All fields are required.

Enter the following values:

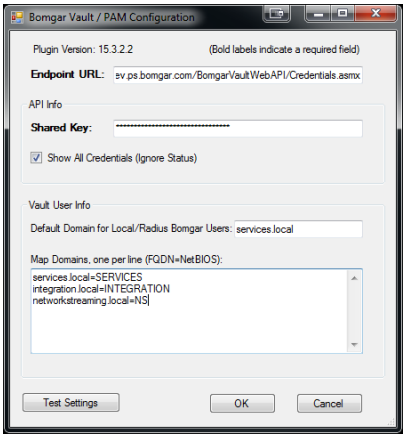
Field Label	Value
Username	The Admin username for Bomgar PAM.
Password	The Admin password for Bomgar PAM.
Site	The URL for your Bomgar PAM instance.
Port	The server port through which the ECM connects to your site.
Plugin	Click the **Choose Plugin...** button to locate the plugin.

4. When you click the **Choose Plugin...** button, the **ECM** location folder opens.
5. Paste your plugin files into the folder.
6. Open the plugin file to begin loading.
7. After the plugin for the ECM is loaded, open the plugin configuration dialog.

Configure the Vault Plugin

Now, you must configure the Vault Plugin to connect to your Vault instance.

1. The **Endpoint URL** should be the URL for your Vault instance: https://localhost/BomgarVaultWebAPI/Credentials.asmx.



> ***Note:*** *Change localhost to a name or IP address as necessary. Make sure SSL is enabled for your Vault server.*

2. Enter the **Shared Key**.
3. Select **Show All Credentials** to include credentials that are already checked out and unavailable for use.
4. Set up your default Vault domain. This must match the domain of your PAM installation. The default domain is used if you are logging into PAM with a local account, ensuring that there is always a domain used with the integration when retrieving credentials from Vault.
5. Next, map the domain(s), translating the fully qualified domain name (FQDN) to the NetBIOS name expected in Vault. Enter one domain per line.

> ***Note:*** *It is possible that you may see a certificate entry form or credentials prompt when you open the plugin, depending on the system to which you are connecting.*

IMPORTANT

To apply new settings in the configuration, restart the ECM service.

Configure the Integration

1. Ensure both products work separately.
   - In PAM, ensure that users are able to see the desired devices. Verify that you can Jump to the devices without any issues.

     > ***Note:*** *You need the ability to log into PAM using domain authentication.*

   - In Vault, ensure that users are able to see the desired credentials. Verify that your credentials can be checked out and that the passwords work.

     > ***Note:*** *You need the ability to log into Vault using domain authentication.*

2. Configure Vault to allow the desired users to access devices and credentials.
   - In Vault, create the same endpoints that exist in PAM.

IMPORTANT

The endpoint names must match exactly the endpoints listed in PAM. If your PAM endpoints show NetBIOS, use NetBIOS. If they exist as fully qualified names, use those. Usernames in PAM must match those in Vault (with the exception of local users), including the domain name.

3. In Vault, create an endpoint group(s).
4. Assign the desired endpoints, user groups, and credentials to the endpoint group; the PAM user may then be allowed to check out credentials. For more information, please see Bomgar Vault Endpoint Groups at https://www.bomgar.com/docs/vault/how-to/user-guide/endpoint-groups.htm.

For more information about the PAM Access Console , see the Access Console User Guide at https://www.bomgar.com/docs/privileged-access/getting-started/access-console/index.htm.

Ensure that the API is Enabled in Vault

1. In Bomgar Vault, go to **Credentials > Credentials** or **Credentials > Credential Group** and edit the credential or credential group.
2. Verify that the credential or credential group checkout policy is set to either **This credential can only be checked out by Privileged Access Management** or **Allow both**.

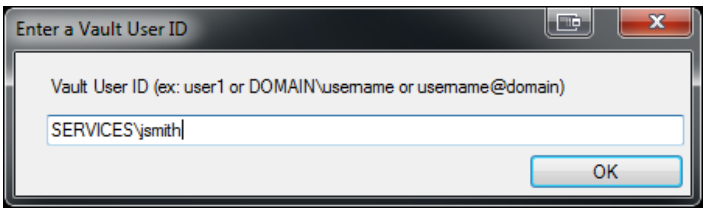
For more information about configuring the checkout policies in Vault, please see Add Credentials at https://www.bomgar.com/docs/vault/getting-started/getting-started/add-credentials.htm.

Troubleshooting the Integration

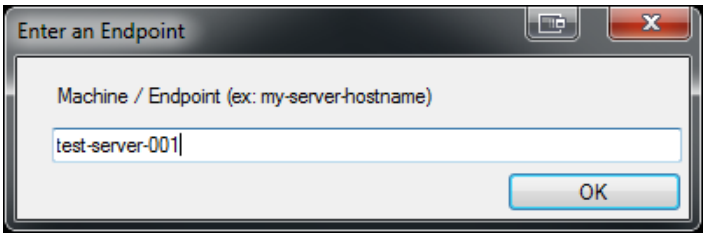
If you experience problems, you can quickly test the API that Vault uses, simulating the plugin request from the PAM Access Console when you connect to a specified endpoint. There are two useful test processes:

1. The API can be tested directly in Vault.
   - First, back up the **web.config**, then edit the **web.config**:
     - Go to **C:\Program Files\BomgarVault\WebSite\WebServices**
     - Open the webservice and comment out or remove the line:

       ```
       <remove name="Documentation"/>
       ```
   - Save the file, and restart IIS. Using the same URL you used in the ECM, open a browser and enter the URL.
2. The Endpoint Credential Manager includes a test function to ensure that the ECM is able to return results. This test simulates the Access Console Representative Console request to the plugin when connecting to endpoints.
   - Click the **Test Settings** button in the Vault configuration screen.
   - Enter the Vault user ID for the credential you wish to test. Click **OK**.



- Next, enter a Vault endpoint to test your connection (for example, **my-server-hostname**). Click **OK**.



- A dialog appears indicating if any credentials were or were not found. If credentials are found, the results appear in the dialog as well.