BOMGAR™

Lieberman ERPM Integration with Bomgar Privileged Access

TC:5/3/2017

Table of Contents

Bomgar Privileged Access Integration with Lieberman Enterprise Random Password Manager

Bomgar's Privileged Access plugin integration to Lieberman Enterprise Random Password Manager (ERPM) enables automatic password injection to authorized systems through encrypted Bomgar connections, removing the need to share and expose credentials to privileged accounts. In addition to the retrieval and automatic rotation of standard credentials, the integration also has the ability to retrieve shared credential lists, giving domain admins and other privileged users access to those credentials for use on the targeted systems.

> ***Note:*** *Auto-rotation occurs only if configured.*

The integration between Bomgar and Lieberman ERPM enables:

- One-click password injection and session spawning
- Credentials never exposed to authorized users of Bomgar
- Access to systems on or off the network with no pre-configured VPN or other routing in place
- Passwords always stored securely in the Lieberman ERPM server

The Bomgar Endpoint Credential Manager (ECM) enables the communication between Lieberman ERPM and Bomgar Privileged Access. The ECM is deployed to a hardened Windows Server inside the firewall, typically in the same network as Lieberman. Once the ECM is deployed, Bomgar users see a list of administrator-defined credentials for the endpoints they are authorized to access. A set of these credentials can be selected when challenged with a login screen during an access session, and the user is automatically logged in, having never seen the username/password combination.

Lieberman ERPM handles all elements of securing and managing the passwords, so policies that require the password to be rotated after use are supported with additional configuration provided by the plugin. Bomgar Privileged Access handles creating and managing access to the endpoint and then recording the session and controlling the level of access granted to the user, including what the user can see and do on that endpoint.

Prerequisites for the Bomgar Privileged Access Integration with Lieberman ERPM

To complete this integration, please ensure that you have the necessary software installed and configured as indicated in this guide, accounting for any network considerations. The integration is provided in the form of a plugin (ZIP archive containing the necessary DLL files and other supporting files) for use within Bomgar's Endpoint Credential Manager (ECM). Please ensure you have acquired the proper version of the ECM to be compliant with the version of Bomgar Privileged Access in use, and install the ECM according to the instructions in "Configure the Lieberman ERPM Plugin for Integration with Bomgar Privileged Access" on page 7.

Applicable Versions

- Bomgar Privileged Access: 15.x and newer
- Lieberman ERPM: 5.4.0 and newer

Network Considerations

The following network communication channels must be open for the integration to work properly.

Outbound From	Inbound To	TCP Port #	Purpose
ECM Server	Bomgar Appliance	443	ECM calls to the Bomgar API.
ECM Server	Lieberman ERPM	443	ECM calls to Lieberman ERPM.

Configure Lieberman ERPM for Integration with Bomgar Privileged Access

The integration requires minimal setup within Lieberman ERPM and should work with your existing data as it stands. The two main requirements are a delegation identity that can impersonate ERPM web users and the installation of the ERPM SDK Web Services.

Delegation Identity

1. Under **Delegation > Web Application Identity Impersonation Mappings**, select **Create Mapping**.
2. If an identity already exists that you would like to use for the integration, select it and skip to step 3 below. Otherwise, continue with the following steps:
    a. Click **Add Identity** and select **Explicit Identity**.
    b. Enter the desired username and password, and then click **OK**.
3. Select the desired identity and click **OK**.
4. Select the identities or roles the above user should be able to impersonate, and then click **OK**.
5. Verify the new mappings, and then click **OK** to close the dialog.

ERPM SDK Web Services

Please consult the Lieberman ERPM Admin Guide for instructions on installing and enabling the SDK Web Services.

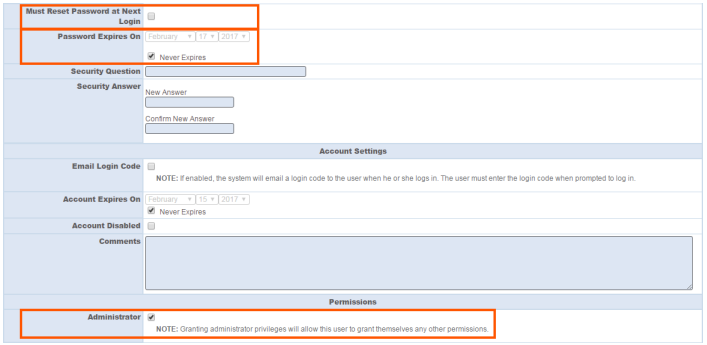
Configure Bomgar Privileged Access for Integration with Lieberman ERPM

Several configuration changes are necessary on the Bomgar Appliance to integrate with Lieberman ERPM.

All of the steps in this section take place in the Bomgar **/login** administrative interface. Access your Bomgar interface by going to the hostname of your Bomgar Appliance followed by /login (e.g., **https://access.example.com/login**).

Create an API User Account

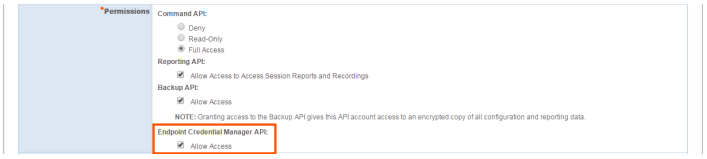
The API user account is used from within the integration to make Bomgar Command API calls to Bomgar.



1. Go to **/login > Users & Security > Users**.
2. Click **Create New User** and name it **Integration** or something similar.
3. Leave **Must Reset Password at Next Login** unchecked.
4. Set **Password Expires On** to **Never Expires**.
5. Check **Administrator**.
6. Scroll to the bottom and save the account.

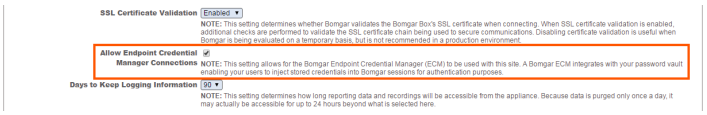
Allow ECM Connections

PA 17.1 and Later



1. Go to **/login > Management > API Configuration**.
2. Add or edit an API account.
3. For **Endpoint Credential Manager API**, check **Allow Access**.

Prior to PA 17.1



1. Go to **Management > Security**.
2. Ensure the box **Allow Endpoint Credential Manager Connections** is checked.

Configure the Lieberman ERPM Plugin for Integration with Bomgar Privileged Access

Install the Endpoint Credential Manager

The Endpoint Credential Manager (ECM) must be installed on a system with the following requirements:

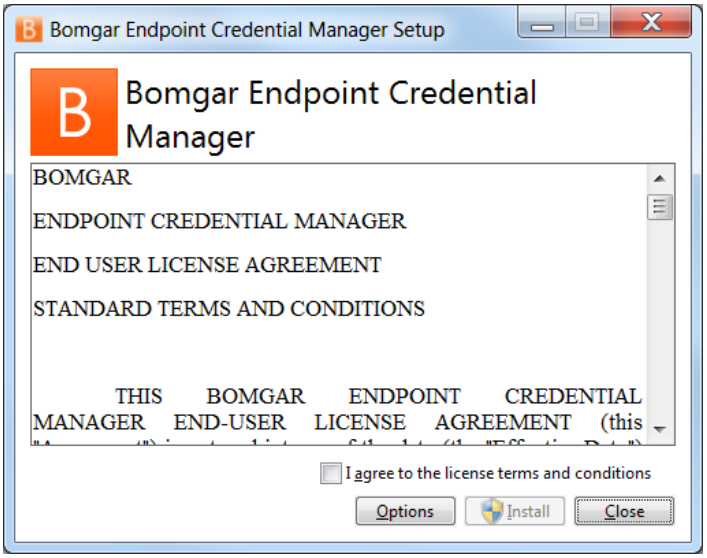
- **Windows Vista or newer, 64-bit only**
- **.NET 4.5 or newer**

1. To begin, download the Bomgar Endpoint Credential Manager (ECM) 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**.

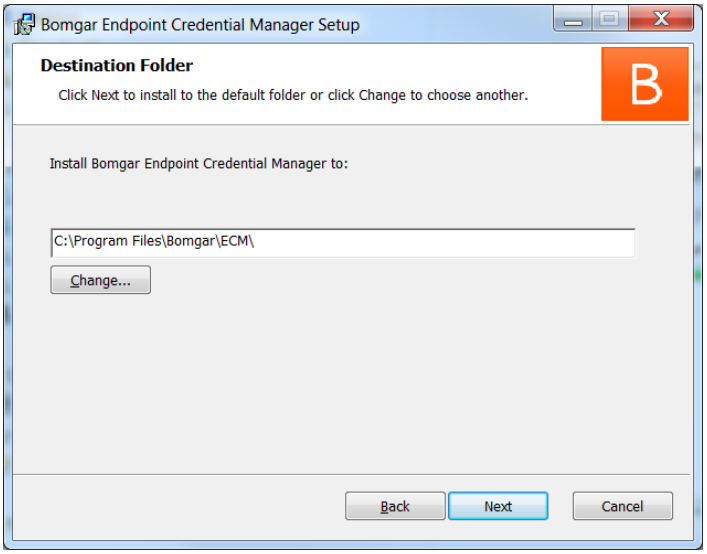
   > ***Note:*** *You are not allowed to proceed with the installation unless you agree to the EULA.*

   If you need modify the ECM installation path, click the **Options** button to customize the installation location.

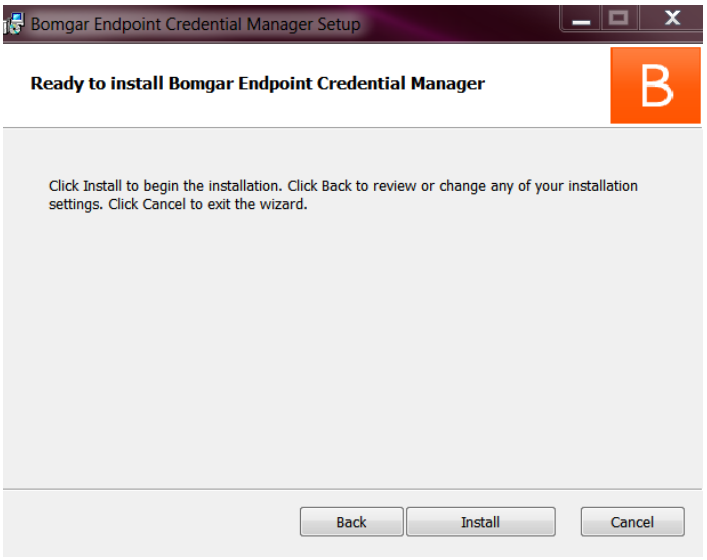
3. Click **Install**.



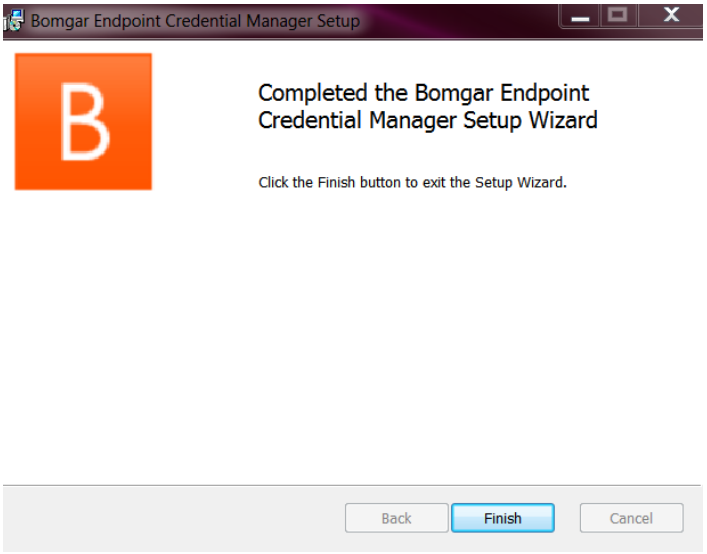
4. Choose a location for the credential manager and click **Next**.
5. On the next screen, you can begin the installation or review any previous step.



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



7. The installation takes a few moments. On the screen, click **Finish**.



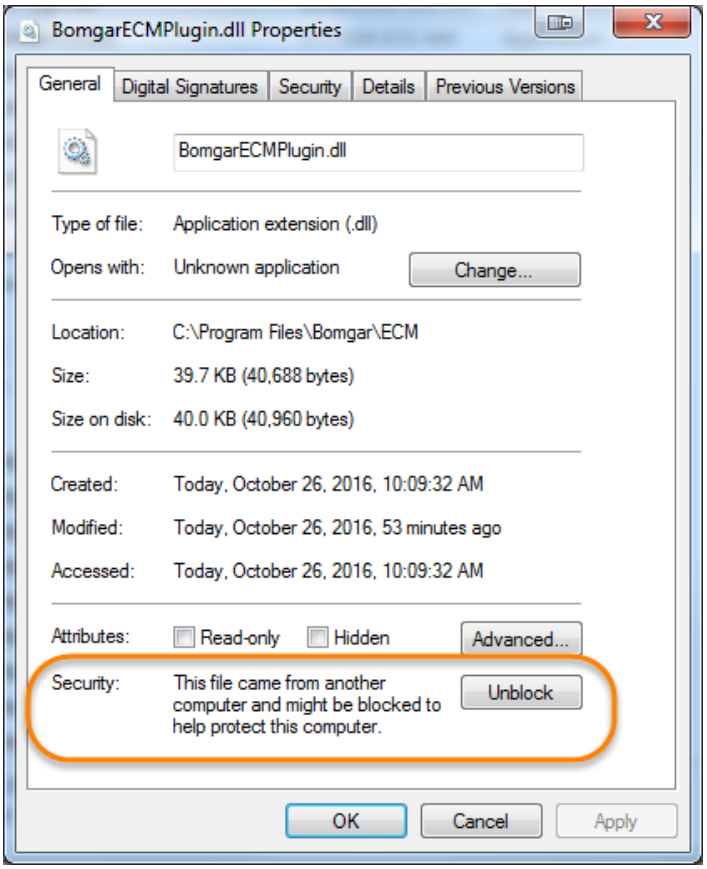
Note: *To ensure optimal up-time, administrators can install up to five ECMs on different Windows machines to communicate with the same site on the Bomgar Appliance. A list of the ECMs connected to the appliance site can be found at* ***/login > Status > Information > ECM Clients****.*

Note: *When multiple ECMs are connected to a Bomgar site, the Bomgar Appliance routes requests to the ECM that has been connected to the appliance the longest.*

Install and Configure the Plugin

1. Once the Bomgar ECM is installed, extract and copy the plugin files to the installation directory (typically **C:\Program Files\Bomgar\ECM**).
2. Run the **ECM Configurator** to install the plugin.

3. The Configurator should automatically detect the plugin and load it. If so, skip to step 4 below. Otherwise, follow these steps:
    a. First, ensure that the DLL is not blocked. Right-click on the DLL and select **Properties**.
    b. On the **General** tab, look at the bottom of the pane. If there is a **Security** section with an **Unblock** button, click the button.
    c. Repeat these steps for any other DLLs packaged with the plugin.
    d. In the Configurator, click the **Choose Plugin** button and browse to the location of the plugin DLL **LiebermanERPMPlugin.dll**.
4. After selecting the DLL, click the gear icon in the Configurator window to configure plugin settings.



5. The following settings are available:

Setting Name	Description	Notes	Required
Endpoint URL	The full URL to the ERPM SDK Web Services	e.g., https://<lieberman-server-hostname>/ERPMWebService/AuthService.svc	Yes
API User	Delegation identity created and assigned impersonate permissions for various other ERPM identities and/or roles		Yes
API Password	Password of the above delegation identity		Yes
Authenticator	The authenticator associated with the delegation identity	Leave this blank if using an explicit account.	No

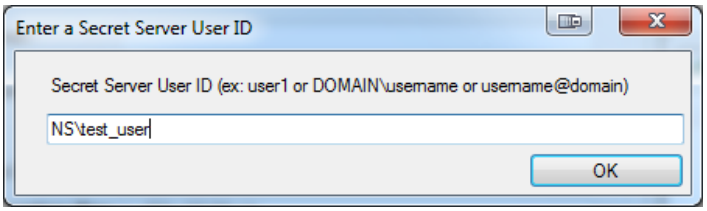
Setting Name	Description	Notes	Required
Default Domain for Local Bomgar Users	When a value is supplied, the plugin initially attempts to retrieve credentials for the user with the username from Bomgar and the configured default domain	This setting is necessary if some or all Bomgar users are local users but the corresponding accounts in ERPM are domain accounts with the same username portion.	No
Enable fall-back to local account if domain account not found	When checked, the plugin first attempts to retrieve credentials for the user as a domain user and then, if no match is found, makes a second attempt without the domain	This setting is necessary if some or all Bomgar users are domain users but the corresponding accounts in ERPM are domain accounts with the same username portion.	No
Map Domains	Allows for the mapping of fully qualified domain names to their shorter NetBIOS names	This setting is necessary to match domain users in Bomgar to domain users in ERPM. Bomgar reports the logged-in user with the fully qualified domain name (FQDN), while ERPM may expect the NetBIOS name of the domain. These mappings must be done manually and can be entered one per line as FQDN=NetBIOS (e.g., Example.local=EX).	No
Enable creation of password spin jobs	When checked, the plugin creates password spin jobs for credentials checked out via the integration	Checking out credentials via the ERPM SDK Web Services does NOT result in a spin job for managed passwords that would normally rotate when checked in via the web interface. To compensate for this, the plugin can examine the credential to see if it is set to auto-spin and then create a job to do so. No spin job is created for credentials that do not have random passwords or that are not configured to auto-spin.	No
Manually schedule jobs	When checked, the spin job is created immediately upon checkout but is scheduled to run at a later time based on the check-out duration setting	If password rotation is desired (i.e., the creation of password spin jobs is enabled), this setting should ALWAYS be used for Bomgar Privileged Access versions 16.1.1 or earlier and NEVER used for versions 16.1.2 or later.	No
Check-out duration in minutes	The number of minutes for which a check-out is valid if not checked back in manually	This value is used in determining the time the password spin job is scheduled to run.	No
Password Change Template Job ID	The numeric ID of the template job shown in the Jobs list in ERPM	Lieberman recommends creating a password change job that can be used as a template for future jobs submitted by the integration. The basic settings of this job are used for each subsequent job with only the password, endpoint-specific information, and scheduling being overridden.	No

Setting Name	Description	Notes	Required
Job Comment	A custom job comment that can be configured to help distinguish jobs that were submitted as part of the integration	The string `<username>` is replaced with the username of the ERPM identity performing the check-out. It can be placed anywhere in the string or removed if desired.	No
Include credentials from Shared Credential Lists	When checked, the plugin includes credentials from a Shared Credential List	In addition to retrieval of normal managed credentials, the integration can also retrieve endpoint-specific credentials from a Shared Credential List.	No

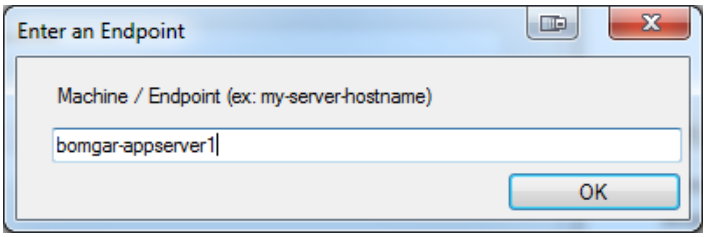
Test Settings

The settings specific to Lieberman ERPM can be tested directly from the plugin configuration screen using the **Test Settings** button.

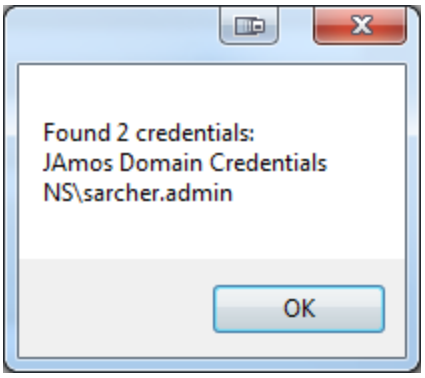
1. Enter a user account from which to retrieve credentials.



2. Enter an endpoint for which the user account has one or more credentials.



3. View the resulting list.



> ***Note:*** *No actual passwords are retrieved or displayed, only the list of credentials.*

> ***Note:*** *The settings used for the test are the ones currently entered on the screen, not necessarily what is saved.*

Clear Token Cache

To avoid excessive authentication calls to Lieberman, the plugin caches (in an encrypted form) authentication tokens for users as they attempt to retrieve secrets through the integration. Subsequent calls use the cached token until it expires. At that point, a new authentication token is retrieved and cached. The **Clear Token Cache** button allows an admin to clear all cached authentication tokens if such action becomes necessary for maintenance, testing, etc.