BOMGAR™

# Bomgar Vault 17.2.1
# Settings Reference



TC:11/21/2017

# Table of Contents

# Configure Bomgar Vault Settings

In Bomgar Vault, you can control many administrative system settings on a global level. These settings are accessed by navigating to **Administration > Settings**. The topics below describe the settings for configuring Vault.

# General Settings for Vault

### Time to inactivate unused user

Set the global inactivity expiration threshold (days) for Vault users. For example, if a user has not logged into Vault for 30 days, you may wish to automatically prevent that user from having the ability to log in. The default setting is 0, which disables user inactivity timeout.

### Available special characters

Set the non-alphanumeric characters that may be used in Vault passwords.

> ***Note:*** *The* ***Available special characters*** *setting can be overwritten by criteria assigned within a password template.*

### Timeout for inactive sessions

Set the expiration time period for Vault user session inactivity. For example, if a user is logged into Vault and is not actively using Vault for a certain amount of time, the system logs them out.The default setting is 10 minutes, but time-out may be set anywhere from 5 to 60 minutes.

### Externally accessible URL

The URL of your Vault site.

### Allow all SSL Certificates in Remote Service Connections

Check to enable SSL certificate validation for remote services. It is recommend you enable this setting after remote services have been configured to leverage a valid SSL certificate, or after copying the root certificate information into the trusted root store for a self-signed certificate.

### Enable syslog audit

Bomgar Vault generates syslog messages. To enable or disable the logging of syslog event messages in Vault, select or de-select the checkbox.

> ***Note:*** *To learn more about configuring syslog, please see log into the Bomgar Self-Service Center and go to https://ssc.bomgar.com/ssc/SolutionFAQ.aspx?id=1358 .*

## Workflow configuration

### Timeout

Set the number of hours (1 - 99) to wait for workflow approval before Vault automatically takes action.

### Action

Choose whether Vault automatically rejects or accepts a workflow item if not approved in the time designated in the timeout setting.

### Skip approval

Check the box to enable the sending of email notifications to designated administrators or credential owners whenever a workflow approval is skipped. Then, choose who receives the email notifications: **System administrators**, **Credential administrators**, and/or **Credential owner**.

## Login Security

### Show image after

Bomgar Vault uses Captcha for secure logging of Vault users. Specify the number of times an incorrect password may be entered by a Vault user before Vault displays a Captcha image that must be entered correctly before login.

## Credential Configuration

### Time for credential opening

Set the number of hours that credentials may be available for check out. Multiple values, separated by commas, may be entered.

### Number of passwords to store

Set the number of passwords Vault archives for each user. The default setting is 30.

### Time to store each password

Set the number of days to maintain the password history. If a user attempts to change a password to one of the historically saved passwords, the attempt fails. If you do not want to maintain a password history, enter the value **0** to disable the setting.

### Enable sequential case number for the credential check out

If enabled, the **Incident number** field on the **Check-out Credential** page increases incrementally each time a credential is checked out. This setting aids in management and reporting.

## Email server configuration

### SMTP Server

Enter the name of the email server that sends workflow notification emails.

### From address for e-mail

Enter the email address from which workflow notification emails are sent.

### Port

Enter the port number of the SMTP server that sends workflow notification emails.

### Ignore email server timeouts

Check the box to restrict email forwarding in case of an SMTP server timeout. Enable this setting to prevent duplicate emails from being sent.

### Authentication required

Check the box if the SMTP server requires authentication to send notification emails. If checked, complete the following fields:

- **Domain\user or e-mail:** Enter the username/domain name or email address needed for authentication.
- **Password:** Enter the password needed for authentication.
- **SSL/TLS:** Check the box if the SMTP server requires a secure connection.

## Directory synchronization

### Synchronize directories

Check the box to automate synchronization between Vault and its associated directories.

### Synchronization time

Enter the time interval in minutes for each synchronization between Vault and its associated directories.

# Security Providers Settings for Vault

The **Security Providers** tab allows you to set up and manage security providers, such as RADIUS and DUO, in Vault. Here, you can configure security providers as needed to meet your requirements. You can also edit and delete existing security providers.

## New Security Provider

Click **New Security Provider** to begin configuring a security provider for your Vault application.

### Name

Type the name of the security provider you are adding to your Vault application.

### Type

Select a provider type from the dropdown menu: **Active Directory**, **eDirectory**, **DUO**, **RADIUS**, **LDAP**, or **Bomgar Verify**.

> ***Note:*** *Some platforms have more complex connection requirements than others, requiring additional fields and information to be completed for them.*

### Used for

Select whether the security provider is being used for login authentication, for credential rotation, or for both.

## Existing Security Providers

### Name

Displays the name of the security provider.

### Type

Displays the security provider type (**Active Directory**, **eDirectory**, **DUO**, **RADIUS**, **LDAP**, or **Bomgar Verify**).

### Used for

Indicates if the security provider is used for authentication, credential rotation, or both.

### View

Click the **View** icon to view the security provider's settings.

### Edit

Click the **Edit** icon to make minor changes to a security provider's settings.

### Delete

Click the **Delete** icon to delete the security provider. A popup dialog asks you to confirm deletion.

# Authentication Settings for Vault

The **Authentication** tab allows you to set up and manage authentication methods in Vault. Navigate to **Administration > Settings > Authentication**.

During the Vault installation process, you are required to set up Active Directory for your initial login. Here, you can configure other authentication methods as needed to meet your requirements. You can also edit and delete existing authentication methods.

### Priority

Set the priority of the new authentication configuration by entering a number in the **Priority** field.

### Primary Authentication

Select the primary security provider being used to authenticate to the Vault application and to rotate credentials. Also, add or edit an existing provider from this selection. For new providers, enter the provider's **Name**, **Type**, **Used for** information (what it is being used for), and the web URL, if needed. Click **Accept**.

### Secondary Authentication

Select the secondary security provider being used to authenticate to the Vault application and to rotate credentials. Also, add or edit an existing provider from this selection. For new providers, enter the provider's **Name**, **Type**, **Used for** information (what it is being used for, and the web URL, if needed. Click **Accept**.

### Add

Click **Add** to implement a new primary and secondary authentication combination.

## Edit

If you would like to make minor changes to an authentication method, you can edit an existing method by clicking the **Edit** icon.

## Delete

### Are you sure you want to delete ____?

Choose to delete the authentication method.

# Platforms Settings for Bomgar Vault

The **Platforms** tab lists all of the systems Vault can connect to and allows you to add and to validate your access to those systems. Bomgar Vault comes with a number of common platforms and connectors preconfigured. Before creating custom platforms, review the default platforms listing to see if they meet your needs.

## Filter Platforms

Filter the platforms based on the type of system for which you wish to make a connection. You can refresh the list to show exactly what you need, such as particular applications, services that you need to restart, databases, or operating systems.

The dropdown platform search list presents the following system types by which you can filter, streamlining the platform listing:

- Application
- Database
- Default (Windows Domain)
- Network
- Networking
- Operating System
- Services
- Telephony

## New Platform Detail

Click **New Platform Detail**.

### Platform dependent

Select what type of platform to add.

### Platform name detail

Type a name for the platform.

### Connection type

Choose whether an automatic or a manual connection is needed for operation.

> ***Note:*** *Some platforms have more complex connection requirements than others, requiring additional fields and information to be completed for them.*

## Edit

If you would like to make minor changes to a platform's settings, you can edit them by clicking the **Edit** icon.

## Delete

**Are you sure you want to delete ____?**

Choose to delete the platform.

> ***Note:*** *Vault does allow deletion of a platform that is actively associated with a user credential.*

# Templates Settings for Bomgar Vault

On the **Templates** tab, default password templates are available to assign to credential polices for rotation. A password template is simply a pattern that the software uses to generate new credentials. As you configure your credentials and credential policies, you can assign a password template to that credential or even multiple credentials.

If the default password parameters do not meet your requirements, there are different ways to create templates that work for your platforms and passwords. If you would like to make minor changes to a template, you can edit and use an existing template. If there is not a default template that meets your needs, you can create a completely new template.

## New Password Template

Click **New Password Template** to create a new password template for your credentials and credential policies.

## Basic

### Length

Set the number of characters the password must possess.

### Uppercase

Set the number of uppercase letters that must be included in the password.

### Lowercase

Set the number of lowercase letters that must be included in the password.

### Numbers

Set how many numerical values must be included in the password.

### Minimum characters different with old password

Set the number of characters that must be different from the previous password.

### Specials

Set the number of special characters that must be included in the password.

#### Special Characters

### Parameters

Check the **Parameters** option to use the default special characters listed under the **General** tab.

### Personalized

Check the **Personalized** option to enter custom special characters allowed in passwords.

## Advanced

### Exclude repeated characters

Check this option if you would like characters NOT to be repeated within the same password.

#### Initial characters

### Uppercase

Check if you would like for your passwords NOT to include uppercase letters.

### Lowercase

Check if you would like for your passwords NOT to include lowercase letters.

### Numbers

Check if you would like for your passwords NOT to include numbers.

### Specials

Check if you would like for your passwords NOT to included special characters.

## Edit

If you would like to make minor changes to a template, you can edit an existing template by clicking the **Edit** icon.

## Delete

### Are you sure you want to delete ____?

Choose to delete the password template.

# Disclaimer Settings for Vault

Vault includes the option to display a disclaimer before users check out credentials.

## Visible Disclaimer

When the box labeled **Visible Disclaimer** is checked, you can enable the textbox to accept your input and to display the disclaimer text your organization requires. Uncheck **Visible Disclaimer** to disable the disclaimer.

Add your organization's disclaimer or terms of use for checking out credentials. Displaying a disclaimer for checking out credentials requires the user to agree to or decline the disclaimer.

> ***Note:*** *If the disclaimer is enabled and the user declines the disclaimer, the credential cannot be checked out.*

# Check Out Reasons Settings for Vault

Checking out a credential in Vault requires the user to indicate a reason why the credential is being checked out. Reasons are selected from a dropdown list when you check out a credential.

### Reason Type

Type a new reason for checking out a credential. Then click **Add Reason Type** for it to appear in the list **Reason Type** list and in dropdowns.

## Delete

### Are you sure you want to delete ____?

Choose to delete the reason type.

# Debug Logs Settings for Bomgar Vault

You can set the number of days to retain certain event logs in Vault.

## Number of days to retain event logs (0 disabled)

Event log settings are shown for five event types, allowing you to limit the disk space used according to your needs. Enter 0 to disable retention of the event log. The **Current disk space used** column displays the amount of space used by the configuration you set here.

### System Events

Set how long (in days) the system retains system-related events.

### Security Audit

Set how long (in days) the system retains security events.

### Historical Credentials Activity

Set how long (in days) the system retains past credential activity.

### Historical e-mails activity

Set how long (in days) Vault stores email activity.

### Historical credential policy activity

Set how long (in days) the system retains past credential policy activity.

***Note:*** *If you have configured a syslog server, Vault may send some critical event logs to that server, making it unnecessary for you to retain logs within Vault over a long period.*

# Integrations Settings for Vault

In order to integrate with another product, such as Bomgar Remote Support or Bomgar Privileged Access, you must configure the Integration API.

## Search Integrations

### Name

Type the name of the integration as criteria for searching existing integration records.

### Active

When searching for a specific integration, filter by whether the integration is active or not by choosing **Yes**, **No**, or **Both**.

### Description

Search for words that appear in the **Description** field of existing integration records.

### Authentication Type

Select the authentication type for the integration you are searching for: **Windows authentication**, **Application authentication**, or **Both**.

### Clear Search

Click to erase all entered search criteria.

***Note:*** *Deleting an integration does not delete the record of events associated with the integration in Vault.*

## New Integration

Click **New Integration** to begin configuring the integration API.

### Name

Type a name for the integration.

### Description

Type a brief description about the integration, including what application is being integrated with Bomgar Vault.

### Active

Select whether the integration is active or not.

### Security Configuration

#### Authentication type

Select whether the third-party integration is being authenticated via Windows or an application.

#### Authentication credential

Type the credential needed to authenticate the third-party application.

#### Allowed IP Address

Type the IP address through which the integrating application can be reached.

#### Add IP Address

Click to add the IP address to the integration record.

### Checkout configuration

#### Reason

Specify a checkout reason for the integration.

#### Requested time (in hours)

Specify how long the integrated application can check out a credential (in hours) from Bomgar Vault.

#### Justification

The statement recorded in logs, showing the reason the credential was checked out using the integrated application.

#### Justification for skipping workflow approval

Type a statement to justify skipping workflow approval for credential checkout when using the third-party application.

## Edit

If you would like to make minor changes to an existing integration, you can edit them by clicking the **Edit** icon.

## Delete

#### Are you sure you want to delete ____?

Choose to delete the integration.

# Networks Settings for Bomgar Vault

## Search Networks

### Networks

Enter the network name to locate it within your records.

### Clear Search

Click to clear all search criteria.

## New Network

Click to add a network and associate it with the Bomgar Vault application.

### Networks Configuration

### Name

Type the name of the network you wish to add to Bomgar Vault.

## Edit

If you would like to make minor changes to a network's settings, you can edit it by clicking the **Edit** icon.

## Delete

### Are you sure you want to delete ____?

Choose to delete the network.

# System Info Settings for Vault

### Company Name

The name of the company which has been licensed to use Bomgar Vault.

### Serial Number

The unique reference number used by the Bomgar Technical Support to validate your company's license and purchase of Bomgar Vault.

### Version Number

The software version of Bomgar Vault the application is currently using for operation.

### Build Number

The unique reference identifier to show what specific build version of the Bomgar Vault software is in operation.

### Scheduler

The status of the Vault scheduler service.

### Number of endpoints licensed

The total number of endpoints your company has been licensed by Bomgar Corporation to use within the application.

### Number of endpoints in use

The actual number of endpoints being used by your company within the application.

### Number of credentials licensed

The total number of credentials your company has been licensed by Bomgar Corporation to use within the application.

### Number of credentials in use

The actual number of endpoints being used by your company within the application.

### Dispatcher

The status of the Vault Dispatcher service.

### Expiration date

The expiration date of the license issued by Bomgar.

### Last update date

The date the license was last updated.

### Rotation

Displays if the credential rotation feature has been enabled for the Vault application.

***Note:*** *When contacting Bomgar Technical Support, you must provide the* ***Company Name****,* ***Serial Number****,* ***Version Number****,* ***Build Number****, and* ***Last Update Date****.*

***Note:*** *The number of endpoints licensed is indicated in your license file; however, it is not a hard limit. You are able to add as many endpoints as needed. The Bomgar Vault EULA has a provision for a periodic audit of usage.*

### Upload File

Allows Vault administrators to update the system information with a new license file.

### Update License

Allows Vault administrator to update the current license file.