BOMGAR™

# Bomgar Vault 17.2.1
# Best Practices for Securing Your Vault Environment



TC:11/21/2017

# Table of Contents

Best Practices for Securing Environments for Bomgar Vault ..... 3
General Security Guidelines ..... 4
Database Security ..... 5
Application Server Security ..... 6
Configuration ..... 7

# Best Practices for Securing Environments for Bomgar Vault

Many organizations may find that they are not ready to confront the ever-evolving dilemma of managing their internal and external privileged user access to critical systems and applications. Staying on the cutting edge of security is challenging in today's fast-paced, tech-savvy environment, especially with new software and hardware applications constantly fading in and out of trending status. While every organization's scenario is different, the following guidelines and best practices help secure your Bomgar Vault environment.

## What is Hardening?

The term "hardening" refers to the process of fortifying an environment against cyber-attacks, unauthorized access, and other vulnerabilities. Most operating systems are designed and initially configured with a focus on usability and functionality rather than security. Achieving a secure environment requires further configuration and advanced security measures, with careful consideration of the risks specific to the environment. Hardening against hackers and cyber-attacks is essential for any environment that is connected to the internet, but it is also crucial that internal security protocols are in place, including the physical security of hardware and data.

***Note:*** *This document is to serve only as a guide and is not a prescriptive procedure for how to perform security hardening for your organization. You should always consider and follow the recommendations of your organization's security team first, as their expertise and knowledge of your environment is crucial to achieving optimal security.*

# General Security Guidelines

When implementing Bomgar Vault, it is essential to maintain and enforce secure processes and procedures for your instance. A best practice for accomplishing this is to execute a multi-layered methodology to security, beginning with your operating system.

**IMPORTANT**

*Check and execute Microsoft Windows updates frequently. For more information about Microsoft Windows updates, please see What is Windows Update? at https://support.microsoft.com/en-us/help/12373/windows-update-faq.*

## Check for and Install Windows Updates

We strongly recommend that you install patches and updates on your Windows server as they become available from Microsoft. This greatly reduces the risk of exploitation of known vulnerabilities in Windows operating systems. Any other applications on your server should also be kept up-to-date with the latest security patches.

## Perform Regular Backups

Your Vault data should be backed up at least once a day. Use Microsoft SQL Maintenance Plan Wizard to configure an automated backup schedule for your SQL server.

## Optimize the Vault Database

A weekly Vault database optimization is recommended, using the Microsoft SQL Maintenance Plan Wizard. A full SQL instance is required to use this feature; it is not available in SQL Express.

## Review the System Log

Checking the system log for errors, failures, changes, and other unusual events should be a routine practice. Be sure to review the system log every time a Vault software update is performed. A security information and event management (SIEM) system can be used to automate analysis on a near real-time basis. For additional security, Vault can be configured to send log files to another server, reducing the risk of the files being tampered with.

***Note:*** *For an overview of SIEM systems, see Introduction to SIEM Services and Products at http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM.*

# Database Security

## Restrict Access to Vault Database

Access to your Vault database should be limited to a minimum number of users. We also recommend disabling the "SA" account in the SQL instance containing Vault, as well as disabling mixed mode for the Vault database.

## Use Windows Authentication to Access Vault Database

Windows Authentication uses Kerberos security protocol and offers robust password policies. It is far more secure than standard SQL Server Authentication and is highly recommended for accessing your Vault database.

## Restrict Access to Other Important Databases

The Vault database account should have access to the Vault database only, and no others. The most secure option is to have the Vault database be on its own server, with its own dedicated SQL instance. If this option is impractical in your environment, close attention should be given to the permissions on a shared SQL server to help mitigate risk. Access to other system databases, such as SQL master, should also be limited.

## Separate Vault Database from Other, Less Secure Databases

The SQL instance containing Vault should not be shared with other databases with lower security requirements. Sharing a SQL server with less secure applications, to which many parties have access, risks exposure to vulnerabilities such as SQL injection.

## Restrict Access to Backups

Access to database backups should be limited to a minimum number of users. We recommend protecting your backups with an approach similar to that of your production data.

# Application Server Security

## Encrypt Communication Using SSL/HTTPS

It is highly recommended that all communication between web browsers and your Vault server be encrypted and secured, using the SSL/HTTPS protocol. Installing a third-party domain, or self-signed SSL/HTTPS certificate on your website is also recommended for maximum security.

## Restrict Access to Vault File System

Access to your Vault directory should be limited to a minimum number of users. The file system contains the Vault encryption key and database connection information, which is vital in disaster recovery situations.

## Restrict Access to the Application Server

Users with login rights to the application server may be able to read plain text passwords and other sensitive information by accessing memory. Access to the application server should be limited to a minimum number of users.

## Application Pool Identity

The Vault application pool account does not need full rights to the entire system, only the Vault files and services. As such, a more limited account can be used than "LocalSystem" or "NetworkService."

## Encrypt Your Vault Encryption Key

Vault uses ASP.NET encryption to secure keys and other sensitive data. Your Vault encryption key and configuration files are encrypted upon installation and should be decrypted for troubleshooting purposes only.

**IMPORTANT**

*You should create a backup of the plain text encryption key that was entered during installation of Vault. In a disaster recovery scenario, Vault may not be accessible without a backup of the key. It is not recommended that the backup be stored digitally. Instead, a physical copy should be created and stored in a secure location such as a safe.*

## Review Activity and Permissions Logs

Check Vault's activity and permissions reports for login and permission failures and other unusual events, and periodically review who has access to the system, who has access to credentials, and what those with access are permitted to do within the system.

# Configuration

## Set Up Access to Sensitive Items

Vault allows you to set access to sensitive credentials by assigning security roles to your Vault users. It is better to start with roles having as few permissions as necessary and then grant access to specific items as needed.

## Login Password Requirements

Vault does not store password information for authentication into the system but instead can be configured to use Active Directory (AD), a RADIUS server, or a local account. Ensure the password policies on those authentication systems require sufficiently complex passwords.

## Maximum Login Failures

Vault can be configured to require the user to fill a Captcha after a number of failed login attempts. We recommend you set this number to 1, so that any time a bad password is entered, the Captcha is needed in order to proceed. In addition, configure your SIEM system to monitor for multiple failed authentication attempts.

## Two-Factor Authentication

Vault supports multifactor authentication to allow you to maintain the highest level of security within your Vault instance.