Hammerspace Security

Version 5.2 · Published 2026-11-20

For the latest version of this document, see docs.hammerspace.com/home/downloads

HAMMERSPACE

Table of Contents

About This Documentation 1
1. Key Security Features 2
2. Hammerspace Platform Access 3
3. Role-Based User Access 4
4. Login 5
5. Passwords 6
6. Administration CLI Access 7
7. Boot Security 8
8. Network Separation of Management and Data Access 9
9. Security Testing 10
10. Securely Storing Data in Public Cloud and Object Storage 11
11. Software Updates 12
12. Support Access 13
13. CVE Mitigation SLAs and Response Times 14
14. Health Heartbeat 15
15. Appendix 16
    15.1. Additional Documentation Resources 16

About This Documentation

This document is an informational security overview of the Hammerspace platform, not a configuration or administration guide. It summarizes the platform’s security architecture, key security features, and access controls.

© 2026 - Hammerspace

Chapter 1. Key Security Features

Hammerspace software enables the following security features:

- Role-based access user interface
- Administration shell is a restricted shell with a limited set of commands
- No user shells are available with general system access
- No privileged (root) user access
- No default passwords
- Management access (UI, CLI, and REST API) is only allowed using https or ssh
- A Hammerspace management user does not have access to the data stored in the system
- All management user activity is logged
- Network separation of management and data access
- No remote access to the system from Hammerspace by default
- Https connections for access to the User Interface as well as to Cloud and Object storage
- Data encryption when storing data in cloud and object storage
- Secure software updates and patches
- Metadata traffic for Global File System shares is protected with TLS 1.2/1.3 encryption
- Customers can install their own certificates for securing https/TLS connections

© 2026 - Hammerspace

Chapter 2. Hammerspace Platform Access

Hammerspace is based on a server installation of Linux with an upgraded kernel. Everything installed is provided by the Hammerspace software; it is not possible to add 3rd party packages before, during, or after the installation.

The configured services are minimal in order to reduce the potential vulnerability footprint. The platform is locked down with a firewall and a restricted administration shell. The firewall only allows for traffic on a certain set of ports. The open ports are specific to the network configuration applied (see network separation for further explanation).

See the *Hammerspace Installation and Licensing Guide* for a granular port listing with explanations per port.

© 2026 - Hammerspace

Chapter 3. Role-Based User Access

Hammerspace includes three default management roles for Graphical User Interface (UI), Command Line (Admin CLI) and REST API access:

- Admin: Full rights to execute Hammerspace management commands
- Data owner: Rights only to set and view data management policies
- Viewer: Read-only access to the management environment

Custom roles can also be created to specify the exact permissions for the desired role.

Active Directory

Active Directory (AD) is the recommended method to manage administrative access to Hammerspace. This allows for management access to be controlled using the same security policies as configured with Active Directory.

Local Management Users

If AD is not in use, local management users can be created and managed within Hammerspace. Local management users do not have access to data. Local management account security behavior is controlled by the login policy. The system can be configured to automatically lock a local management account after a number of failures within a certain amount of time. This login policy only applies to local management users and not to management users managed by Active Directory.

The following options are available as part of the local user login policy.

+ .Admin CLI: Local-user login options

```
--allowed-networks Space separated list of allowed networks

--lock-after-failures The number of consecutive login failures after which an account will be locked

--lock-after-failures-clear Clears all login failure lock attributes

--lock-failure-interval Time in seconds between failed login attempts that constitutes consecutive
failures. When not set, the default is 15 minutes.

--lockout-time The amount of time in seconds an account remains locked due to too many consecutive login
failures. When not set, the default is 10 minutes.
```


© 2026 - Hammerspace

Chapter 4. Login

Management access can further be restricted by configuring which network(s) or host(s) are allowed to log in to the management address.

© 2026 - Hammerspace

Chapter 5. Passwords

Hammerspace does not contain any default passwords for users. The password for the local admin user is set during installation by the customer. When deploying in the cloud, each deployment has a unique, auto-generated password. The password can also be changed after installation is completed.

The following rules apply to the creation of a management-user password:

- The password is 8-20 characters long.
- The password contains at least one of each of the following:
  - lower case letter
  - upper case letter
  - digit
  - non-alphanumeric character



If the password for the `admin` user is lost, contact Hammerspace Support, who can help you reset it. Be prepared to provide video-console access to the active Anvil node.

© 2026 - Hammerspace

Chapter 6. Administration CLI Access

Hammerspace has limited the command access for users when they log in using ssh. They are limited to a set of Hammerspace-only commands designed to offer all the required functionality to manage Hammerspace. No operating system access is granted.

The operating system that is running Hammerspace software is locked down and does not allow for generic logins. There is no sudo access to the underlying operating system for a Hammerspace management user.

© 2026 - Hammerspace

Chapter 7. Boot Security

The boot loader configuration is locked and cannot be modified by a console user to try to get to a pre-console state.

© 2026 - Hammerspace

Chapter 8. Network Separation of Management and Data Access

Management access is restricted to management network role and therefor separates, at the network layer, management traffic and data traffic. An SMB/NFS/S3 client computer cannot, assuming proper segregation of the networks, get access to the management shell/UI even if login credentials are known.

© 2026 - Hammerspace

Chapter 9. Security Testing

Hammerspace executes periodic security tests as part of the development and release process

- Pentest (executed per release, by 3rd party, report available upon request)
- Pentest (executed internally on a frequent basis)
- Virus scanning on images before product release (includes marketplace security scanning)
- Nessus scans

[[3rd-party-external-security-scans]] = 3rd-Party, External Security Scans

The following vendors have executed independent security scans of the Hammerspace product and Hammerspace have passed their testing

- Amazon AWS marketplace security scan (checks for known vulnerabilities, malware, or viruses, best practices and so forth)
  - Complies with best practices with regards to Security for AWS marketplace
  - Completed and passed AWS Well-Architected review
- Google Cloud marketplace security scan
  - Complies with best practices with regards to Security for Google Cloud marketplace
- Azure marketplace
  - Complies with best practices with regards to Security for Azure marketplace
- 3rd party Penetration Test
  - Report available upon request

© 2026 - Hammerspace

Chapter 10. Securely Storing Data in Public Cloud and Object Storage

Hammerspace utilizes https connections into object storage to ensure the network transfers are safe.

In addition to a secure connection, customers can also configure Encryption of the data before it is sent over the wire. The encryption key(s) are provided either by utilizing the integrated Key Management capabilities of the product, Entrust nShield HSM or AWS Key Management Service.

After the KMS is configured, any new file instances placed in object, whether by objective or on demand, will be encrypted by default, in both existing and new object volumes. Encryption at rest can be disabled on a per object volume (bucket) basis.

© 2026 - Hammerspace

Chapter 11. Software Updates

Hammerspace software update mechanism is also protected. All updates (patches, software updates) are signed by Hammerspace, otherwise they cannot be applied. The software updates cannot be reverse-engineered and applied without being signed by Hammerspace.

© 2026 - Hammerspace

Chapter 12. Support Access

By default, Hammerspace support personnel do not have any remote access to the installed system. Remote access can be enabled if necessary to resolve issues. See the Enable Remote Support Access Knowledge Base article for details.

© 2026 - Hammerspace

Chapter 13. CVE Mitigation SLAs and Response Times

These Vulnerability Remediation SLAs define the maximum time allowed between the identification of a security vulnerability and the implementation of a remediation or approved mitigating control. Compliance with these SLAs is monitored and tracked as part of Hammerspace's secure development and operations processes. For more information, see the *Hammerspace Version 5.2 Vulnerability Remediation SLAs Document* (HS3011-USEN-17).

Severity	Definition	Remediation SLA
Critical	**Actively exploitable or severe impact**	**≤ 72 hours**
High	High impact, no known active exploit	≤ 14 days
Medium	Moderate impact	≤ 30–60 days
Low	Low impact or informational	≤ 90 days

Severity Remediation Table

© 2026 - Hammerspace

Chapter 14. Health Heartbeat

By default, the product will send a health heartbeat every 24 hours to report back system health, status, and basic configuration. The health heartbeat is sent over a secure network transport to a US-based, Hammerspace-managed, resilient endpoint.

This functionality can be disabled if desired; however, by doing so, proactive support and the ability to detect potentially incorrect configurations will be limited.

The health heartbeat contains the following information:

- Cluster info, settings and status
- Hammerspace License info
- Configured Nodes
- Configured Volumes
- Configured Objectives
- Configured Email and Heartbeat configuration
- Configured NTP settings
- Configured Snapshot schedules
- Configured Volume Groups
- Latest events and errors from product and node system logs and events
- Basic resource utilization from product nodes

Private data such as file data or file names, usernames, or any credentials are NOT included in the health heartbeat.

© 2026 - Hammerspace

Chapter 15. Appendix

The following sections contain additional information that may be useful to Hammerspace administrators.

15.1. Additional Documentation Resources

Every Hammerspace title is available at docs.hammerspace.com: the product user guides, the solution guides, the compliance and security documents, and the Hammerspace Knowledge Base. Read any title online, or download it as a PDF from the title's own pages or from the Downloads page.

The following titles may be of special interest to users of this guide:

- Assimilation Overview [Solution Guide]: An overview of a typical data migration with Hammerspace using assimilation and data orchestration.
- Objectives Guide [Solution Guide]: How to configure Hammerspace objectives.
- Hammerscript and the Hammerspace Toolkit Guide [Solution Guide]: An introduction to the concepts of Hammerspace metadata, and the tools to manipulate metadata and put it to work to achieve business objectives for data.
- S3 Guide [Solution Guide]: This document covers the creation and management of S3 servers, bucket containers, and buckets, as well as user access control and security considerations, ensuring seamless multi-protocol data access and efficient data management.

To download Hammerspace software and licenses, use the Hammerspace Licensing and Delivery Portal. To open a support case, use the Hammerspace Support Hub.

© 2026 - Hammerspace