TECHNICAL WHITE PAPER

Nasuni Access Anywhere Security Model

The Nasuni Access Anywhere add-on service delivers high-performance, VPN-less file access for remote and hybrid users, integrates an organization's file shares with Microsoft Teams, and provides productivity tools such as desktop synchronization and external file and folder sharing to enhance user productivity and provide access to files seamlessly from anywhere on any device. This white paper outlines the security elements of the Nasuni Access Anywhere service.

20 December 2022

Table of Contents

Introduction

Nasuni is a leading provider of file data services, including file storage, backup, ransomware protection, and file access for hybrid workers. The Nasuni File Data Platform is a cloud-native replacement for traditional network-attached storage (NAS) and file server infrastructure but with many more advanced capabilities. The Nasuni approach to data services creates a scalable, innovative platform for digital acceleration, business growth, and data insights previously unachievable.

The Nasuni platform is architected on an advanced security model that enables cloud object storage to be safely used for traditional NAS and file server use cases, offering greater protection against ransomware and other threats to meet the requirements of the most security-conscious enterprises. For a detailed overview of this security model, see the Nasuni File Data Platform Security Model technical white paper.

Nasuni Access Anywhere is an add-on service to the Nasuni File Data Platform that delivers high-performance, VPN-less file access for remote and hybrid users, integrates an organization's file shares with Microsoft Teams, and provides productivity tools such as desktop synchronization and external file and folder sharing to enhance user productivity and provide access to files seamlessly from anywhere on any device. Nasuni Access Anywhere extends the security model of the Nasuni platform with its own set of robust, enterprise-class security elements. This white paper outlines those elements.

Encryption - Data in Transit

HTTPS is configured by default for all users of Access Anywhere. HTTPS is a secure version of the HTTP protocol that uses the TLS protocol for encryption and authentication. TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the public Internet. TLS uses a combination of symmetric and asymmetric cryptography to achieve this. Access Anywhere supports TLS 1.2 and TLS 1.3 but does not support the earlier TLS 1.1 and 1.0 variants. Port 443 is required to be open for HTTPS to work outside of the corporate network.

Encryption – Data at Rest

HTTPS is configured by default for all users of Access Anywhere. HTTPS is a secure version of the HTTP protocol that uses the TLS protocol for encryption and authentication. TLS is a cryptographic protocol that provides end-to-end security of data sent between applications over the public Internet. TLS uses a combination of symmetric and asymmetric cryptography to achieve this. Access Anywhere supports TLS 1.2 and TLS 1.3 but does not support the earlier TLS 1.1 and 1.0 variants. Port 443 is required to be open for HTTPS to work outside of the corporate network.

Two-factor authentication may also be configured and turned on within Nasuni Access Anywhere. This provides the option of One Time Password (OTP) using an application such as Google Authenticator or Microsoft Authenticator, an emailed code, or a shared secret.

Identity Authentication

Nasuni Access Anywhere users are authenticated against the customer's Identity Management System. Out-of-the-box support is included for Microsoft Active Directory, LDAP, and SAML. Once authenticated, clients use the authentication token for the remainder of the session.

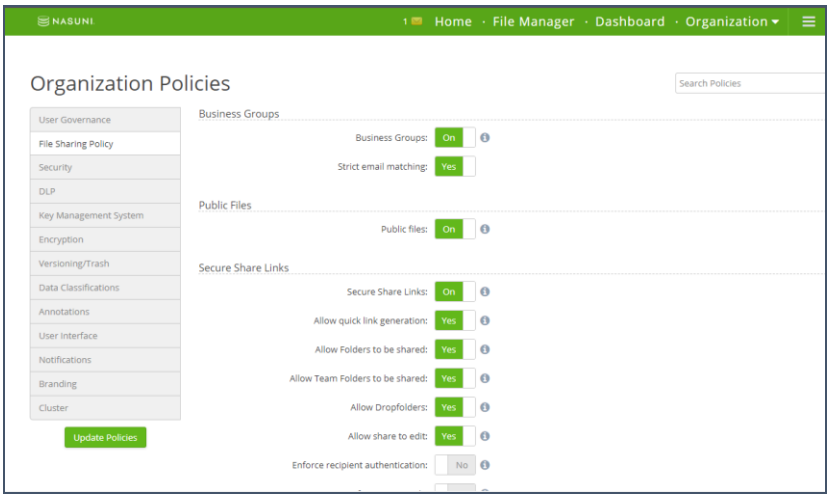
Data Loss Protection

Files can be securely shared using Nasuni Access Anywhere in several ways:

- Private links can be created for files, which can be combined with passwords to secure the file, or external users can be configured that require authentication before access. Links can be set to be time expired and/or combined with private links and passwords for additional file security.
- Watermarks unique to each user and file preview, or shared file downloads can be added to files.
- Additionally, external participants with whom files are shared can be required to view them in a web browser in a read-only manner. This prevents users from being able to download, copy, or edit sensitive data. This can be combined with the watermarks feature to deter external users from taking photos of content and provide a tracking mechanism if this occurs.

Access Control Permissions

Nasuni Access Anywhere transparently supports the Access Control Permissions that are configured on the Nasuni Edge Appliances. These permissions are the single source of truth for access to files.

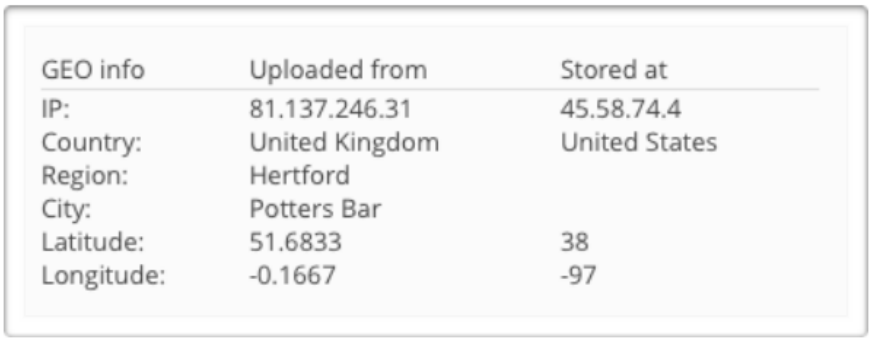


Restrict by IP Address

Nasuni Access Anywhere supports the ability to safelist or blocklist IP addresses to allow or deny connections. This can be done at the Organization level (tenant) or on a per-user basis.

Geo Location Logging

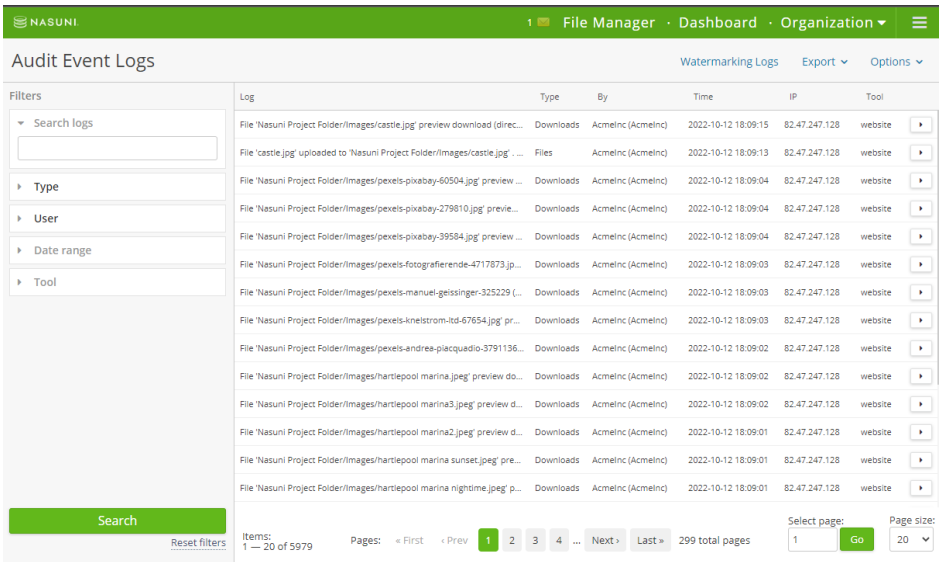
The geographic locations of where a file is uploaded from and where a file is uploaded to is recorded and logged for each file, as are the IP addresses. Proving document location can be important for certain industries and is an important part of any audit flow.



GEO info	Uploaded from	Stored at
IP:	81.137.246.31	45.58.74.4
Country:	United Kingdom	United States
Region:	Hertford	
City:	Potters Bar	
Latitude:	51.6833	38
Longitude:	-0.1667	-97

Audit Security

All file events that occur when using Nasuni Access Anywhere are recorded.
Reports can be accessed online, archived, and exported as .cvs or Microsoft Excel files, and can be used to satisfy Subject Access Requests (SARs) for various compliance regimes, such as GDPR, CCPA, or HIPAA. The audit events can be configured to be output in Syslog format so that log aggregators such as Splunk can be used to monitor and collate the resultant logs.

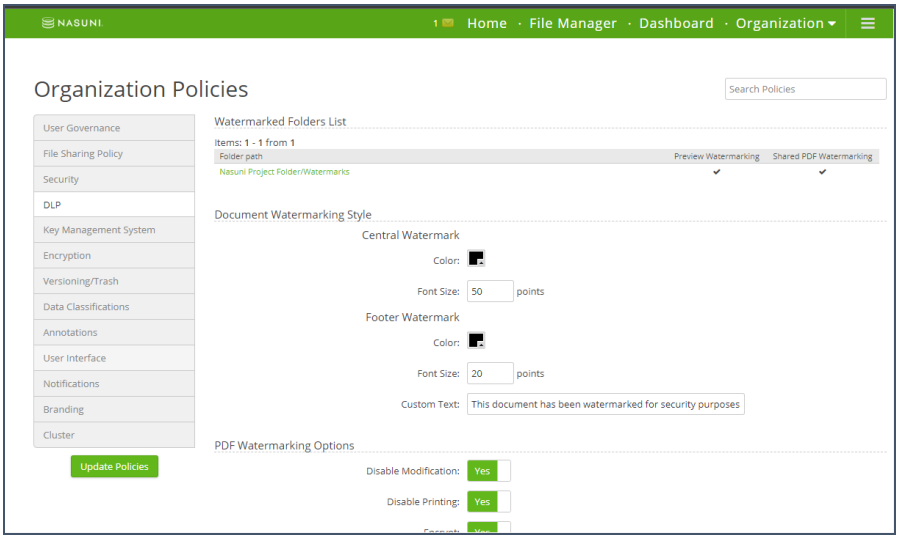


Acceptable Use Policies

Acceptable use policies enable organizations to present policies and optionally required acceptance for access to the system. Policy acceptance is logged and can also be required by users downloading shared files and folders.

Governance Options

There are comprehensive governance, compliance, and security options that can be configured by a Nasuni Access Anywhere Administrator.

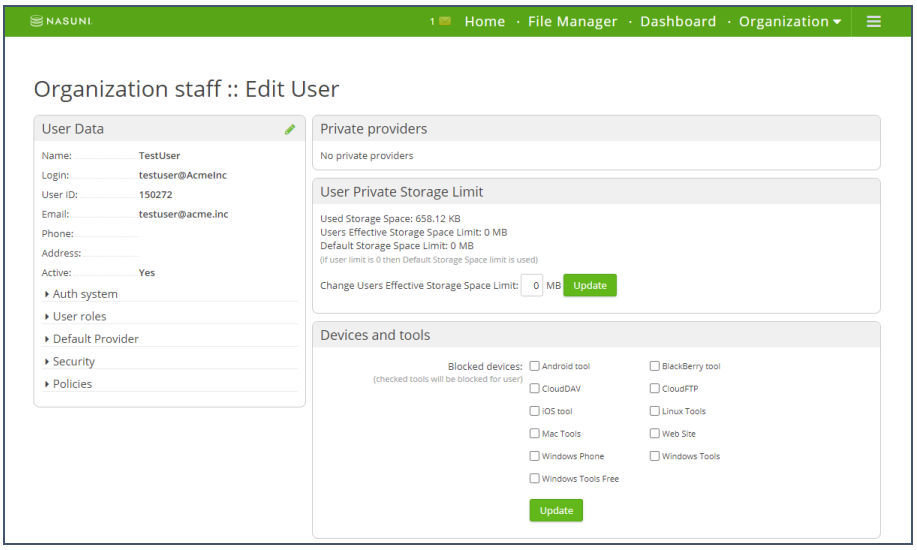


Bring Your Own Device Security

The Nasuni Access Anywhere Administrator controls which devices and access clients that each user can connect from. By default, all devices and access clients are enabled.

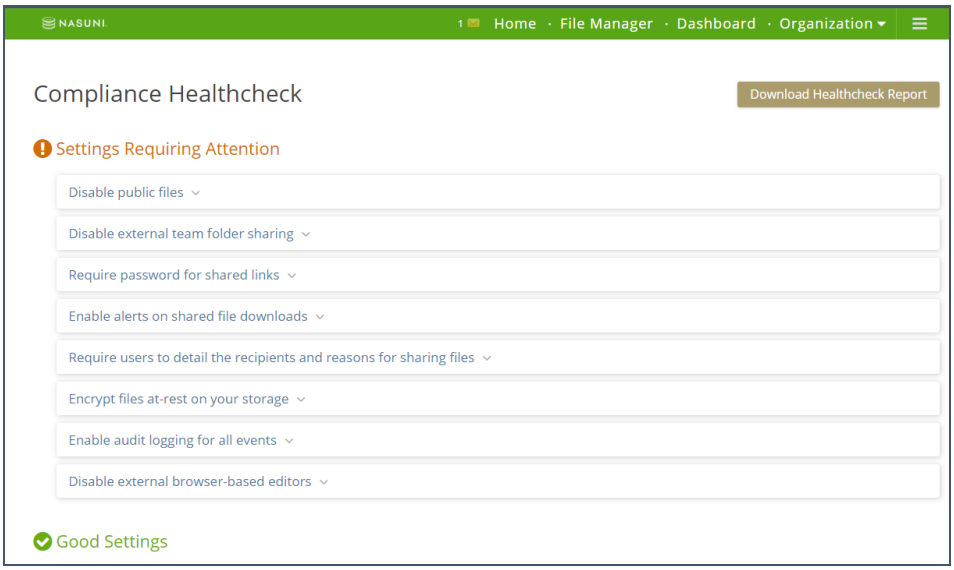
The Administrator can entirely disable a user's access, or just choose to disable access from any of the devices or access clients from the users' settings, instantly disabling user access.

This can be combined with IP safe listing and block listing to, for example, satisfy scenarios such as enabling an external user to access a folder from their offices but only from that IP address.



Compliance Report

The compliance report recommends settings to an Administrator that could be changed within Nasuni Access Anywhere to enhance security. The Administrator can jump from the online report directly to where the setting can be changed in the Policies section.



Product Design and Testing

Nasuni Access Anywhere is developed using the OWASP principle of Security by Design. Each product release, service pack, and patch is security-audited and. tested through the use of multiple third-party security products.

Best practices in developing secure software are followed, as mandated by legislation such as GDPR / CCPA, protecting against, for example, injection attacks, cross-site request forgery, and session hijacking. Third-party vulnerability code scans are also conducted for each release.

When using Nasuni Access Anywhere, the following cookies formats are used (the unqualified hostname of the web address is <site> and the unqualified hostname of https://files.example.com is files).

Cookie	Type	What For	Retention
PHPSESSID	Functional	Unique ID of the session	Session
<site> just_logged_in	Functional	Start page logic (0 or 1)	1 year
autologin	Functional	Token for "remember me" feature	14 days
<site> <various>	Functional	Remembers settings between sessions, such as what folders and panels are collapsed, and the last sort order. For example, files_mainTree_ openedFoldersKeys	1 year

Certifications

Nasuni is ISO 27001:2013 compliant. ISO 27001 is the International Standard for Organizations that formalizes internal controls known as Information Security Management Systems (ISMS) and is the gold standard for security excellence around the globe.

Additionally, the UK entity Vehera LTD (Storage Made Easy), which was acquired by Nasuni, is Cyber Essentials Certified. Cyber Essentials is a UK government information assurance scheme, operated by the National Cyber Security Centre (NCSC), that encourages organizations to adopt good practices in information security. It includes an assurance framework and a set of security controls to protect information from threats coming from the Internet.

It specifically covers:

- Boundary firewalls and Internet gateways
- Secure configuration
- Access Control
- Malware Protection
- Patch Management

It was developed in collaboration with industry partners, including the Information Security Forum (ISF), the Information Assurance for Small and Medium Enterprises Consortium (IASME), and the British Standards Institution (BSI), and is endorsed by the UK Government.