Security Features of the Nasuni Filer

Nasuni Corporation – Boston, MA

The Nasuni Filer offers a number of security features that clients can leverage to safeguard their data.

Connection Control

- **HTTPS proxy server** (*Configuration → HTTPS Proxy*): You can configure the Nasuni Filer to use a proxy server for all outbound HTTPS connections. All Nasuni Filer-initiated HTTPS traffic goes through the proxy server that you specify. A valid User Name and Password might be required, depending on your proxy configuration.
- **Firewall protection** (*Configuration → Firewall*): You can specify which network hosts are allowed to connect to the Nasuni Filer user interface and the Nasuni Support SSH port.
- **SSL certificates** (*Configuration → SSL Certificates*): You can use SSL Certificates when accessing the Nasuni Filer's Web-based user interface (the default is self-signed certificate). You can generate a Certificate Request, and add signed certificates. You can also create a self-signed certificate instead of a certificate request. Note: production systems should always utilize a valid CA-signed certificate.
- **Remote access** (*Volumes → select volume → Properties → Remote Access*): You can enable or disable access to a volume by your remote offices attached to your Nasuni.com account.

Access Control

- **Role-based access control** (*Configuration → Users/Groups*): You can define specific access permissions for groups and users to perform actions within the Nasuni Filer user interface.
- **Login**: You must enter a valid username and password to access the Nasuni Filer user interface.
- **Change password** (*Configuration → Change Password*): You can change the password of the currently logged-in user. Strong passwords are required.
- **Snapshot directory access** (*Volumes → select volume → Snapshot Directory Access*): You can enable or disable access to the directory that presents a file system view of historic snapshot data.
- **CIFS authentication** (*Configuration → General CIFS Settings*): You can select either Public security or Authenticated Access (which includes Active Directory and LDAP Directory Services) for CIFS file shares.

- **CIFS Shares** (*Volumes → select volume → Properties → CIFS Shares → Edit Share*): You can configure a number of security features of shares, including the following:
    - **Visible Share**: You can enable whether a share is visible when browsing the Nasuni Filer.
    - **Read Only Share**: You can select that a share be read-only, so that users cannot change the contents of the share.
    - **Allowed Hosts**: You can specify which hosts are allowed to access the share.
    - **Hide Unreadable Files**: You can specify that files and folders that the user cannot access do not appear in folder listings.
    - **Mobile Access**: You can enable or disable access to data by mobile devices.
    - **Web Access**: You can enable or disable access to data via Web browsers.
    - **Authentication** (Active Directory or LDAP Directory Services only): If Active Directory or LDAP Directory Services security is chosen, you can select whether to authenticate all users, or to authenticate only the groups and users that you explicitly specify.
    - **SMB Encryption**: You can select whether clients must use SMB encryption when connecting to the share.

- **NFS Exports** (*Volumes → select volume → Properties → NFS Exports → Edit Export*): You can configure a number of security features of exports, including the following:
    - **Allowed Hosts**: You can specify which hosts are allowed to access the export.
    - **Read-Only**: You can select that an export be read-only, so that users cannot change the contents of the export.

- **Mobile service settings** (*Services → Mobile Service Settings*): You can configure a number of security features of Mobile Access, including the following:
    - **Session Expiration**: You can limit how long users can use Mobile Access before reauthenticating.
    - **Limit to a single device**: You can limit users to using a single mobile device.
    - **Allowed Devices**: You can specify which device types to permit Mobile Access on.

- **Data Migration Service** (*Services → View Migrations*): You can configure a number of security features of the Data Migration Service, including the following:
    - **File permissions**: You can specify how to handle existing permissions of copied files, including creating customized permissions rules.
    - **Password retention**: You can select whether or not to retain passwords for automatic reconnection.

Data Protection

- **Encryption** (*Configuration → Encryption Keys*): The Nasuni Filer automatically encrypts your data on-premises using your encryption keys that remain under your control. You can upload your encryption keys to the Nasuni Filer as well as generate keys for use, and then download them for safekeeping. You can also escrow your encryption keys with Nasuni. You can enable and disable specific encryption keys.
- **Antivirus protection** (*Volumes → select volume → Properties → Antivirus Service*): You can enable or disable antivirus protection for CIFS and NFS volumes. The Antivirus Service scans every new or modified file for the presence of viruses and other malware.
- **Snapshot retention** (*Volumes → select volume → Properties → Snapshot Retention*): For compliance purposes or your own best practices, you can specify the deletion of older snapshots from cloud storage, based on a configured policy for a specific volume. By default, all snapshots are permanently maintained.
- **Remote Support Service** (*Services → Remote Support Service*): You can enable or disable remote access to your Nasuni Filer by Nasuni support personnel, as well as specify an automatic deactivation timeout after enabling the service.

Monitoring and Logging

- **Email notifications** (*Configuration → Email Settings*): You can configure the dispatch of email notifications when certain conditions occur on the Nasuni Filer.
- **SNMP monitoring** (*Configuration → SNMP Monitoring*): You can configure monitoring of the Nasuni Filer via the Simple Network Management Protocol (SNMP).
- **File Alert Service** (*Volumes → select volume → Properties → File Alert Service*): For compliance and other purposes, you can receive a daily summary email that details when files and directories whose names match patterns you specify are written to the Nasuni Filer.

- **File System Auditing and Logging** (*Volumes → select volume → Properties → Auditing*): You can configure extensive file system auditing and logging of operations for a volume, including creating, deleting, renaming, closing, reading, and writing files, directories, and links. You can also log file and directory ownership and permission changes.