Nextcloud

Security and authentication

White paper

> “Nextcloud understands the necessity to provide core principle baseline security requirements, as such Nextcloud 11 is built on these security principles to ultimately deliver a secure solution to their customers.”

nccgroup
freedom from doubt

nextcloud.com

Nextcloud

Contents

Verified Enterprise-Class Security

Our customers care deeply about security and so do we. Nextcloud aligns with industry standards such as Clause 14 of ISO/IEC27001-2013 and related standards, guidance and security principles.

Our solution is built around combined assurance layers consisting of newly applied rich security features, applied best practices which are governed by policy and the design itself validated by industry standard testing processes.

In this white paper, we will provide a high-level overview of the security features in Nextcloud and how we ensure the highest security standards in our development processes.

Integration

New technology should fit into existing processes and infrastructure. Nextcloud enables you to leverage existing security investments:

Authentication Support

LDAP / Active Directory

Nextcloud has extensive LDAP/Active Directory support with an easy installation wizard.

Kerberos

Nextcloud can work with Kerberos and other authentication mechanisms like OAuth2, OpenID Connect, JWT, CAS or Any SQL database mediated by Apache modules.

SSO/SAML 2.0

Nextcloud supports Single Sign On (SSO) and provides native SAML 2.0 (and Shibboleth) authentication in its web front end. The native SAML integration negates the need for external software like Apache modules. Native SAML is compatible with all webservers and supports group memberships, flexible session management and app specific passwords.

Two-factor authentication

Nextcloud includes Universal 2nd Factor (U2F) and Time-based One-Time Password (TOTP) second factor apps to increase the security of user login handling.

Automated or manual provisioning

Nextcloud offers an easy to use, REST-style provisioning API to create and configure user accounts.

Existing storage and database technology

Nextcloud supports any existing storage solution, including object store technologies, keeping data under control of trusted IT administrators and managed with established policies. Nextcloud works with industry standard SQL databases like PostgreSQL, MySQL and MariaDB for user and metadata storage.

Existing security tools

Nextcloud offers built in monitoring tools and integrates with existing MDM, DLP, event logging and backup tools, enabling existing tool chains to be used to monitor, back up and restore systems.

Current security policies and processes

Thanks to the on-premise nature of Nextcloud and its ability to leverage existing data storage and database technologies, current security policies and governance processes can continue to be used to manage, control and secure operations with Nextcloud. Nextcloud GmbH does at no point have access to your data and can not interfere with regulated processes, keeping your IT department in control.

Control over data flow

Control is key to security. With Nextcloud, your IT department takes back control over its data, managed under its policies and procedures. Nextcloud integrates in the tooling you use in your data center like logging and intrusion detection and works with existing authentication mechanisms like SAML, Kerberos and LDAP.

Logging and monitoring

Nextcloud has built in monitoring and logging tools, compatible with industry standard tools like Splunk, Nagios and OpenNMS. It also offers a full, compliance-ready activity log for reporting and auditing purposes.

Permission

Administrators can set permissions on sharing and access to files using groups. Permissions of underlying storage, like Windows Network Drive access rights, are respected by Nextcloud.

Fine-grained File Access Control

The powerful workflow tools in Nextcloud enable administrators to limit access to data in accordance to business and legal requirements and perform automatic actions like file conversion. Describe restrictions like “XLSX files from the HR department are not to be accessible outside company IP ranges” or “employees in the US shouldn’t access customer data from European data centers” for Nextcloud to enforce.

Encryption

Nextcloud uses industry-standard SSL/TLS encryption for data in transfer. Additionally, data at rest in storage can be encrypted using a default military grade AES-256 encryption. Keys can be handled with the built-in key management or you can opt for a custom key management for integration with your existing infrastructure. As keys never leave the Nextcloud server, external storage systems never have access to unencrypted data.

Virus scanning

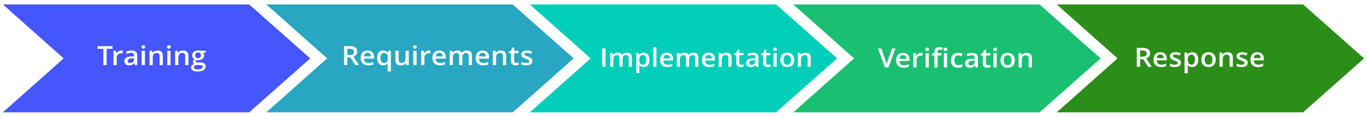
Nextcloud supports integration with ClamAV for automated scanning of all uploaded files.

Data Rentention

Nextcloud allows administrators to define rules for data retention, allowing regular cleanup of files or give assurances that data stays put for a set amount of time.

Security in development processes

Nextcloud follows industry standard security processes. We treat security bugs like technical debt: fixing them later is expensive for all parties involved. Our strategy is to prevent them from happening through a rigorous focus on security through the entire life cycle of our product and to get those which find their way through found and fixed as soon as possible.



Training → Requirements → Implementation → Verification → Response

Training

- We provide detailed documentation about common web security vulnerabilities for our developers
- We organize internal and public security training
- To facilitate learning and awareness, developers are asked to fix security issues they caused themselves

Requirements

- Privacy and security risks are analyzed and requirements are established
- We employ advanced threat modeling / attack surface analysis
- Designs are reviewed for security implications

Implementation

- Unsafe functions are forbidden (e.g. unserialize, non-prepared statements and unsafe comparisons)
- Our internal functions are designed to provide secure defaults for developers
- We employ a strict mandatory code review process with 2 reviewers besides the original developer

Verification

- We regularly run static and dynamic security scans like Burp, Veracode and others
- We follow industry-standard security processes and have them independently verified

Response

- We follow industry best practices in disclosing security issues fixed in a release: 2 weeks after the release advisories with CVE identifiers are published
- We run a successful bug bounty program at Hacker One, a responsible disclosure platform where over 3,000 security experts have reported over 24,000 security issues. Our program awards up to $5,000, making our bounties among the highest in the open source industry
- Statistics show a massive decrease of valid external security reports

More information

On our website you can find more details and download the security scan results, find links to our public security training efforts, our Bug Bounty program and the review of our development processes by the NCC Group.

nextcloud.com/secure

Capabilities

In the following section we provide more details on the features and capabilities Nextcloud employs and supports to protect the security of your data.

Authentication capabilities

The Nextcloud authentication system supports pluggable authentication including Two-factor authentication and device specific passwords, complete with a list of connected browsers and devices on the users' personal page. As extra protection, device specific password tokens can be denied access to the file system.

Included are Universal 2nd Factor (U2F) and Time-based One-Time Password (TOTP) second factor apps, enabling users to use tools like Yubikeys or Google Authenticator to secure their accounts.

Active sessions can be invalidated through the list, by removing the user in the admin settings or by changing passwords. Admins can enable or disable Two-factor authentication for users on the command line.

Nextcloud supports SAML 2.0 (including "Shibboleth") and Kerberos authentication and has extensive LDAP directory integration.

Brute force protection

Brute Force Protection logs invalid login attempts and slows down multiple attempts from a single IP address (or IPv6 range). This feature is enabled by default and protects against an attacker who tries to guess a password from one or more users.

You can find more information on hardening your Nextcloud installation in our extensive hardening guide as part of our documentation.

Rate Limiting

Rate Limiting allows a developer to specify how often an IP range or a user may send a request in a specific time period. This can be useful for expensive API calls, to prevent users from accessing too much data in a smaller attempt of time or harden bruteforce stuff further. It is used by Nextcloud apps to protect users from spam and overloading.

Password handling

Administrators can set password quality policies enforced by Nextcloud. Password reset tokens are invalidated when critical information like user email has been changed to protect against phishing attacks. Nextcloud will ask system administrators for password confirmation on security critical actions.

Security hardening

Nextcloud employs a wide variety of extra security hardening capabilities, including:

Content Security Policy 3.0

CSP is a HTTP feature that allows the server to set specific restrictions on a resource when opened in a browser. Such as only allowing to load images or JavaScript from specific targets.

CSP 3.0 is the latest and strictest version of the standard, increasing the barrier for attackers to exploit a Cross-Site Scripting vulnerability.

Same-Site Cookies

Same-Site cookies are a security measure supported by modern browsers that prevent CSRF vulnerabilities and protect your privacy further. Nextcloud enforces the same-site cookies to be present on every request by enforcing this within the request middle ware.

We include the __Host prefix to the cookie (if supported by browser and server). This mitigates cookie injection vulnerabilities within potential third-party software sharing the same second level domain.

Encrypted Session Data

Nextcloud stores user session data including login state, user name and other data in an encrypted way. The encryption key is stored in a cookie on the client which has to be sent to the server with every request for data the user sends to the server. Without the cookie, session content can not be decrypted and the user will have to log in again.

This protection is especially important when using Server-side Encryption (the users' private key will be stored as part of the session data) and when remote storage requires the Nextcloud server to provide and thus store the login credentials of the user.

The encryption of the session provides an additional barrier against unauthorized access. An attacker would have to make modifications to the Nextcloud server code to be able to intercept user data. And if, intentionally or not, data from the session is stored or backed-up, it will not be readable, also avoiding compliance violations.

Nextcloud Apps

Nextcloud apps are developed using the MVC like Nextcloud App Framework. This framework is designed in a 'secure by default' model, having authentication checks and CSRF checks opt-out for app developers.

Apps uploaded to our app store have to follow our best practices. An automatic code scan is employed to ensure certain potentially dangerous development patterns are rejected.

For example, we employ Strict Comparison enforcement. This means that Nextcloud forces PHP to confirm data is of the same type when doing comparisons. This avoids unexpected and potentially compromising behavior of PHP. This check is performed by the code scanner.

Other features

There is a wide variety of smaller and larger features employed to harden Nextcloud against attacks.

- **mod_unique_id support**. Nextcloud supports mod_unique_id which enables request ID's (used for logging) to be generated by the web server. This allows administrators to relate log information for tracking potential security incidents.
- **Included root certificate**. To avoid problems with improperly configured hosts, Nextcloud ships with a root certificate bundle containing certificates shipped by Mozilla Firefox. The bundle is regularly synchronized with Mozilla's list.
- **Support for security headers by the web server.** This enables administrators to configure their web server to serve a number of HTTP headers that prevent security issues.
- **Trusted domains**. Nextcloud checks domains in the Host header to ensure users can't access the side using another domain which could result in Nextcloud generating faulty URL's that redirect users to a compromised server.
- **Preventing directory traversals**. The Nextcloud internal filesystem code has a number of protections built in like forbidding character sequences such as "..\" or "../".

Learn more about hardening features in our blog on security hardening:

https://nextcloud.com/?p=1334

Encryption

Nextcloud employs industry-standard TLS to encrypt data in transfer. Usage of Object Storage like Amazon S3 or other external storage systems can be secured through Server-side Encryption while End to End encryption in the clients can ensure data is never readable by unauthorized users even in case of a full server compromise. More information on Server and Client side encryption is covered in separate whitepapers.

Server-side Encryption

Server-side Encryption can also be used on local storage. However, inherent to the concept of Server-side Encryption, encryption keys will be present in memory of the Nextcloud server during the time a user is logged in and could be retrieved by a determined attacker. We take care to ensure keys are not stored unencrypted on permanent storage and at rest keys are encrypted using a strong cipher.

Key management

Nextcloud supports pluggable encryption key handling. If you have an external key server, it can be made to work with Nextcloud.

Our default encryption key handling enables administrators to set a system wide recovery key for encrypted files. This ensures that, even when users lose their password, files can always be decrypted. Encrypted files can be shared but after changing encryption settings, shares will have to be re-shared. Using our command line tools, data can be encrypted, decrypted or re-encrypted when needed.

If you face a regulatory or compliance need to encrypt data at rest but do not need to actually secure this data, locally encrypting data using our built in key management may satisfy compliance requirements.

End to End Client-side Encryption

Nextcloud is the first vendor to introduce a complete, enterprise-grade seamlessly integrated solution for end to end encryption in a file sync and share product.

The Nextcloud solution works on a per-folder level and features an easy to use, server-assisted but fully secure key management with Cryptographic Identity Protection, our method of securely signing and handling user certificates. Users can easily access their data on any of their devices using the clients (not via the web interface!) and share with other users, securely. The Nextcloud E2E Encryption design is unique in delivering on enterprise demands like a complete audit log, an optional offline administrator recovery key and support for a secure HSM (hardware security module) to be able to issue new identities to users.

The End to End Encryption feature ensures that neither the Nextcloud server itself nor any code it provides (like in the browser) has ever access to the unencrypted data.

Conclusion

Nextcloud considers security of the utmost importance. Without proper security measures, there are no benefits of a self hosted solution with regards to privacy and control. Our development processes as well as passive and active security measures adhere to the highest standards, as attested by independent, third party review.

Customers looking for the highest standards in security and privacy find it at Nextcloud.

You can find a full report by security experts NCC Group for download on nextcloud.com/secure.

Contact our sales team for more information:

Andreas Rode
Head of Sales

Email: sales@nextcloud.com
Phone: +49 711 252428-94

nextcoud.com

Nextcloud GmbH
Hauptmannsreute 44A
70192 Stuttgart
Germany

Email	sales@nextcloud.com
Phone	+49 711 252428-90
Fax	+49 711 252428-20

nextcloud.com