Cloud Security Principles

Introduction

Slack's mission is to make people's working lives simpler, more pleasant and more productive. We believe that we must make your data secure, and that protecting it is one of our most important responsibilities. We're committed to being transparent about our security practices and helping you understand our approach.

The National Cyber Security Centre (NCSC) has created 14 Cloud Security Principles to help organisations configure, deploy and use cloud services securely.

This document outlines how Slack meets those 14 principles, including what is the responsibility of Slack (the service provider) and what is the responsibility of the customer.

The controls on this document are based on Slack Enterprise Grid.

Document format

Each **NCSC Cloud Security Principle** is represented by a heading. Some Cloud Security Principles also contain **NCSC Considerations**, which are also represented by subheadings. All principles and considerations are followed by **NCSC Guidance**, which are formatted in italics. Please note that all **principles**, **considerations** and **guidance** are taken from NCSC's documentation and are not written by Slack.

Slack's responses to NCSC's **principles**, **considerations** and **guidance** can be found under the subheadings **Slack responsibility** and **Customer responsibility**.

1. NCSC Cloud Security Principle: Data in transit protection

NCSC Guidance: *User data transiting networks should be adequately protected against tampering and eavesdropping.*

This should be achieved through a combination of:

- *network protection - denying your attacker the ability to intercept data*
- *encryption - denying your attacker the ability to read data*

Slack responsibility

All data transmitted between Slack clients and the Slack service is done so using strong encryption protocols. Slack supports the latest recommended secure cipher suites to encrypt all traffic in transit, including use of TLS 1.2 protocols, AES256 encryption and SHA2 signatures, whenever supported by the clients.

Within Slack networks, with Enterprise Key Management (EKM) enabled, all data is encrypted prior to transmission. Without EKM, data may be transmitted without encryption between certain hosts within Slack's virtual private cloud (VPC). Data routed through the public internet is never transmitted unencrypted.

On 4 March 2020, Slack will discontinue support for Transport Layer Security (TLS) versions 1.0 and 1.1. We're making this change to align with industry best practices for security and data integrity.

After 4 March, requests sent to Slack from any service that has not been upgraded to TLS 1.2 will fail.

Customer responsibility

After 4 March 2020, customers will not be able to transmit data to or from Slack over an insecure connection (e.g., TLS 1.0 or 1.1).

2. NCSC Cloud Security Principle: Asset protection and resilience

NCSC Guidance: *User data, and the assets storing or processing it, should be protected against physical tampering, loss, damage or seizure.*

The aspects to consider are:

- *Physical location and legal jurisdiction*
- *Data centre security*
- *Data at rest protection*
- *Data sanitisation*
- *Equipment disposal*
- *Physical resilience and availability*

2.1. NCSC Consideration: Physical location and legal jurisdiction

NCSC Guidance: *In order to understand the legal circumstances under which your data could be accessed without your consent you must identify the locations at which it is stored, processed and managed.*

You will also need to understand how data-handling controls within the service are enforced, relative to UK legislation. Inappropriate protection of user data could result in legal and regulatory sanction, or reputational damage.

Slack responsibility

Slack will not access data in the services except in accordance with its agreement with customers and our policies. All customer data resides entirely in our AWS production environment, physically located within various AWS data centres to provide better redundancy.

The exact location of data can vary, but this can be configured with International Data Residency (discussed below).

Slack provisions services in accordance with the laws applicable to it as a service provider. Customers in the U.K. contract with Slack Technologies Limited, an Irish company.

Customer responsibility

Customers are responsible for choosing the region where certain types of data at rest are stored.

Data residency for Slack allows global teams to choose the region where certain types of data at rest are stored. You can contact our sales team to set up data residency for your organization. Customers must store all Slack data in a single region.

As of February 2020, we offer data storage in the United States as well as Frankfurt, Germany and Paris, France. Customer data stored in Frankfurt is backed up in Paris and customer data stored in Paris is backed up in Frankfurt. For an up-to-date list of data regions, please see Data residency for Slack.

The United States is the default data region for customers that do not contact our sales team to set up data residency.

Note: *The data residency feature does not change any aspects of Slack other than the data storage location. Slack will continue to store and process all other categories of data in accordance with your written agreement for Slack Services and Slack's Privacy Policy.*

How data residency for Slack works

Customer data

The following categories of customer data will be stored at rest in a data centre within the customer's selected region as of the date data residency is enabled:

- Messages, posts and snippets
- Files (e.g., images, docs, etc.) uploaded to the Service
- Search index of customer data
- App- or bot-generated messages and files

Other categories of customer data, such as user profile information and channel names, channel topics and channel descriptions, might be delayed or unavailable for storage in the data residency region.

Other data

The following categories of data may be processed and stored in regions outside of the customer's data region:

- Workspace and channel membership information
- Data used to measure seat count, usage and revenue
- Data used for analytics and to measure quality of service, e.g., logs (sanitized logs)
- IDs generated by Slack on behalf of the customer (UID, EID, TID)

Data migration

If a new workspace or Enterprise Grid org is set up in a data residency region, customer data will be stored in the selected region starting the date the workspace or org is created.

For existing customers wishing to enable data residency, customer data can be migrated to a selected data region at any time. When a workspace or Enterprise Grid is migrated, all new user data will start residing in this region. However, old data will continue to live in the United States.

Soon, Slack will migrate the customer data stored in the U.S. to the customer's selected data region. The length of data migration will depend on the volume of message data and the migration process will not affect the ability for users to use Slack.

Shared channels

If organizations connected by a shared channel are in the same data region, all of their customer data will remain in that data region as well. If the organizations are located in different data regions, the following will happen:

- Each organization's messages will live in their respective data regions
- The search index for the shared channel will live in all regions

If the shared channel is disconnected, all organizations will get a copy of the other party's previously shared data.

Note: *Enterprise Key Management (EKM) is not currently integrated with data residency, but we may offer this capability in the future.*

Additional resources:

- Data residency for Slack

2.2. NCSC Consideration: Data centre security

NCSC Guidance: *Locations used to provide cloud services need physical protection against unauthorised access, tampering, theft or reconfiguration of systems. Inadequate protections may result in the disclosure, alteration or loss of data.*

Slack responsibility

All customer data resides entirely in our AWS production environment. Physical protections are entirely provided by AWS, which has a wide range of security certifications and attestations to its physical security. More data on AWS data centre security can be found here.

Customer responsibility

Not applicable. Customers are not able to physically access data centres. Physical security is provided by AWS.

2.3. NCSC Consideration: Data at rest protection

NCSC Guidance: *To ensure data is not available to unauthorised parties with physical access to infrastructure, user data held within the service should be protected regardless of the storage media on which it's held. Without appropriate measures in place, data may be inadvertently disclosed on discarded, lost or stolen media.*

Slack responsibility

Data at rest in Slack's production network is encrypted using FIPS 140-2 compliant encryption standards, which applies to all types of data at rest within Slack's systems—relational databases, file stores, database backups, etc. All encryption keys are stored in a secure server on a segregated network with controlled and very limited access. Slack has implemented appropriate safeguards to protect the creation, storage, retrieval, and destruction of secrets such as encryption keys and service account credentials.

Customer responsibility

Customers are responsible for integrating and managing Amazon Web Services Key Management Service for Enterprise Key Management (EKM).

At Slack, we are committed to ensuring that your data is protected. By default, Slack encrypts data at rest and data in transit as part of our foundational security controls.

Slack Enterprise Key Management (EKM) adds an extra layer of protection and is available as an add-on for our most security-conscious Enterprise Grid customers. Slack EKM helps you meet your security objectives without affecting any of the Slack features your teams require.

With Slack EKM, messages and files are encrypted using your own keys (stored in Amazon's Key Management Service). Having the power to use your own keys means that you have complete control over your customer data in Slack. On top of that, administrators can revoke key access in a targeted and precise manner so that teams experience minimal disruption in service. Slack keeps working, and so do your teams.

Administrators get detailed visibility into how your keys are being accessed to encrypt and decrypt messages and files in Slack. This information is logged into AWS KMS's CloudWatch and CloudTrail solutions. Slack EKM is offered as an add-on to Enterprise Grid. Get all the details at https://slack.com/intl/en-gb/enterprise-key-management.

To address security threats, administrators can revoke access in a very targeted manner. Access to messages and files can be revoked at the organizational, workspace, channel, time-frame and file levels.

This revokes your access to the customer data as well as the underlying Slack service's access to the data.

The Slack experience—from features to performance—remains the same. Teams can keep collaborating, using all the Slack features they regularly use, even when some of the data has restricted access.

Additional resources:

- Slack Enterprise Key Management
- How We Built Slack Enterprise Key Management

2.4. NCSC Consideration: Data sanitisation

NCSC Guidance: *The process of provisioning, migrating and de-provisioning resources should not result in unauthorised access to user data.*

Inadequate sanitisation of data could result in:

- *your data being retained by the service provider indefinitely*
- *your data being accessible to other users of the service as resources are reused*
- *your data being lost or disclosed on discarded, lost or stolen media*

Slack responsibility

By default, Slack encrypts customer data at rest and data in transit as part of our foundational security controls. Slack defines policies and standards requiring media be properly sanitised once it is no longer in use. Slack's hosting provider is responsible for ensuring removal of data from disks allocated to Slack's use before they are repurposed. More info on AWS processes for sanitising data can be found here.

Customer responsibility

Not applicable. Customers are not able to physically access data centres. Data sanitisation is provided by AWS.

2.5. NCSC Consideration: Equipment disposal

NCSC Guidance: *Once equipment used to deliver a service reaches the end of its useful life, it should be disposed of in a way which does not compromise the security of the service or user data stored in the service.*

Slack responsibility

Slack's hosting providers are responsible for ensuring that equipment is disposed of in a responsible manner. More information about AWS hardware disposal can be found in the Device Management section here.

Customer responsibility

Not applicable. Customers are not able to physically access data centres. Equipment disposal is provided by AWS.

2.6. NCSC Consideration: Physical resilience and availability

NCSC Guidance: *Services have varying levels of resilience, which will affect their ability to operate normally in the event of failures, incidents or attacks. A service without guarantees of availability may become unavailable, potentially for prolonged periods, regardless of the impact on your business.*

Slack responsibility

Slack utilizes services deployed by its hosting provider to distribute production operations across four separate physical locations. These four locations are within one geographic region, but protect Slack's service from loss of connectivity, power infrastructure and other common location-specific failures. Production transactions are replicated among these discrete

operating environments to protect the availability of Slack's service in the event of a location-specific catastrophic event.

Slack also retains a full backup copy of production data in a remote location significantly distant from the location of the primary operating environment. Full backups are saved to this remote location at least once per day and transactions are saved continuously. Slack tests backups at least quarterly to ensure that they can be successfully restored. Further physical resilience is ensured by our hosting providers.

Customer responsibility

Not applicable.

3. NCSC Cloud Security Principle: Separation between users

NCSC Guidance: *A malicious or compromised user of the service should not be able to affect the service or data of another.*

Factors affecting user separation include:

- *where the separation controls are implemented – this is heavily influenced by the service model (e.g. IaaS, PaaS, SaaS)*
- *who you are sharing the service with - this is dictated by the deployment model (e.g. public, private or community cloud)*
- *the level of assurance available in the implementation of separation controls*

Slack responsibility

Slack is hosted in an Amazon Web Services Virtual Private Cloud. It is a multi-tenant solution where data is logically separated. Every API call at all layers of the technology stack uses a teamID as the primary key. When a user logs into Slack, credentials are checked with our user database and a secret token is generated per User Agent session. This ensures that all calls from the user are directed to the correct team. Logical separation ensures that customers can only access their own data and no one else's.

Customer responsibility

With Slack Enterprise Key Management (EKM), messages and files are encrypted using your own keys (stored in Amazon's Key Management Service); this encryption provides another mitigation and strengthens the separation between different customers' data.

Additional resources:

- Slack Enterprise Key Management

4. NCSC Cloud Security Principle: Governance framework

NCSC Guidance: *The service provider should have a security governance framework which coordinates and directs its management of the service and information within it. Any technical controls deployed outside of this framework will be fundamentally undermined.*

Having an effective governance framework will ensure that procedure, personnel, physical and technical controls continue to work through the lifetime of a service. It should also respond to changes in the service, technological developments and the appearance of new threats.

Slack responsibility

Slack's security team, led by our chief security officer (CSO), is responsible for the implementation and management of our security program. The CSO is supported by the members of Slack's security team, who focus on security architecture, product security, enterprise security operations, production security operations, and risk and compliance.

Slack also has a data protection officer (DPO). To communicate with our data protection officer, please email dpo@slack.com.

Slack is continuously monitoring, auditing and improving the design and operating effectiveness of our security controls. These activities are regularly performed by both third-party credentialed assessors and Slack's internal risk and compliance team. Audit results are shared with senior management and all findings are tracked to resolution in a timely manner. Slack adheres to ISO 27001, 27017, 27018, SOC 2, FedRAMP, HIPAA, GDPR and EU/U.S. Privacy Shield. Certificates for applicable frameworks can be found here, under the section titled Compliance certifications and regulations.

Customer responsibility

Not applicable.

5. NCSC Cloud Security Principle: Operational security

NCSC Guidance: *The service needs to be operated and managed securely in order to impede, detect or prevent attacks. Good operational security should not require complex, bureaucratic, time consuming or expensive processes.*

There are four elements to consider:

- ***Configuration and change management** – you should ensure that changes to the system have been properly tested and authorised. Changes should not unexpectedly alter security properties*
- ***Vulnerability management** – you should identify and mitigate security issues in constituent components*
- ***Protective monitoring** – you should put measures in place to detect attacks and unauthorised activity on the service*
- ***Incident management** – ensure you can respond to incidents and recover a secure, available service*

5.1. NCSC Consideration: Configuration and change management

***NCSC Guidance:** You should have an accurate picture of the assets which make up the service, along with their configurations and dependencies.*

Changes which could affect the security of the service should be identified and managed. Unauthorised changes should be detected.

Where change is not effectively managed, security vulnerabilities may be unwittingly introduced to a service. And even where there is awareness of the vulnerability, it may not be fully mitigated.

Slack responsibility

The configuration management tool Chef is utilized to centrally manage Slack's production servers throughout their lifecycle and to ensure that baseline security configurations are consistently pushed out to all servers. Chef is configured to run periodically and will automatically revert any deviation from the baseline security requirements. Any changes made to the Chef recipes are required to go through Slack's Change Control processes.

Slack’s security team receives threat intelligence feeds on a daily basis through industry partners, public accessible feeds, etc., to monitor new vulnerabilities and threats. The team will assess the risks and impact of the newly reported vulnerability against the Slack production environment and will determine appropriate remediation strategies accordingly, as per Slack's Vulnerability Management Policy.

In addition, weekly Nessus scans are performed to detect vulnerable services running across the production environment. Any exceptions will be reported to members of the Slack Service Engineering team for investigation/triage.

Slack's hosting provider, Amazon Web Services (AWS), is responsible for patching and fixing flaws within the infrastructure, as well as maintaining the configuration of its infrastructure devices. For more information, please see AWS's Shared Responsibility Model.

Customer responsibility

Customers are responsible for tracking changes to their org via audit logs.

Audit logs provide a record of changes to and use of Enterprise Grid that helps keep your org secure and protect against misuse.

Logs are accessible via the Audit Logs API.

The Audit Logs API can be used by security information and event management (SIEM) tools to provide analysis of how your Slack organization is being accessed. You can also use this API to write your own applications to see how members of your organization are using Slack.

Additional resources:

- Audit logs on Enterprise Grid
- Monitoring workspace events with the Audit Logs API

5.2. NCSC Consideration: Vulnerability management

NCSC Guidance: *Service providers should have a management processes in place to identify, triage and mitigate vulnerabilities. Services which don't, will quickly become vulnerable to attack using publicly known methods and tools.*

Slack responsibility

Slack maintains an internal vulnerability management program for identifying and patching issues. As part of this program, the Slack team will engage third parties for "Red Team" exercises, the findings of which will then be resolved. More info can be found about Slack's Red Team engagements here. As part of this program, Slack runs vulnerability scanners pointed at both internal and external endpoints, triages potential vulnerabilities, and works with teams for patching.

Slack also runs a bug bounty program (located here) to facilitate the intake and resolution of externally reported vulnerabilities. We also utilize this program to facilitate responsible disclosure of potential vulnerabilities. All submissions to this program are validated for accuracy, triaged and tracked to resolution by Slack's product security team. We have a blog post about the three-year anniversary of the program here.

Customer responsibility

Not applicable.

5.3. NCSC Consideration: Protective monitoring

NCSC Guidance: *A service which does not effectively monitor for attack, misuse and malfunction will be unlikely to detect attacks (both successful and unsuccessful). As a result, it will be unable to quickly respond to potential compromises of your environments and data.*

Slack responsibility

Slack monitors servers, workstations and mobile devices to retain and analyze a comprehensive view of the security state of its corporate and production infrastructure. Administrative access, use of privileged commands, and system calls on all servers in Slack's production network are logged. Analysis of logs is automated, to the extent practical, to detect potential issues and alert responsible personnel. All production logs are stored in a separate network that is restricted to only the relevant security personnel. We use go-audit for syscall monitoring, and have more information on that and the practices we follow here. We also have more information on our distributed security alerting processes here.

Customer responsibility

Customers are responsible for monitoring their org via audit logs.

Audit logs provide a record of changes to and use of Enterprise Grid that help keep your org secure and protect against misuse.

Logs are accessible via the Audit Logs API.

The Audit Logs API can be used by security information and event management (SIEM) tools to provide analysis of how your Slack organization is being accessed. You can also use this API to write your own applications to see how members of your organization are using Slack.

Additional resources:

- Audit logs on Enterprise Grid
- Monitoring workspace events with the Audit Logs API

5.4. NCSC Consideration: Incident management

NCSC Guidance: *Unless carefully pre-planned incident management processes are in place, poor decisions are likely to be made when incidents do occur, potentially exacerbating the overall impact on users.*

These processes needn't be complex or require large amounts of description, but good incident management will minimise the impact to users of security, reliability and environmental issues with a service.

Slack responsibility

Slack has established policies and procedures (also known as runbooks) for responding to potential incidents. The runbooks define the types of events that must be managed via the incident response process and classifies them based on severity. In the event of an incident, affected customers will be informed via email from our customer experience team. Incident response procedures are tested and updated at least annually.

Customer responsibility

Customers are responsible for having an incident management process in place.

6. NCSC Cloud Security Principle: Personnel security

NCSC Guidance: *Where service provider personnel have access to your data and systems you need a high degree of confidence in their trustworthiness. Thorough screening, supported by adequate training, reduces the likelihood of accidental or malicious compromise by service provider personnel.*

The service provider should subject personnel to security screening and regular security training. Personnel in these roles should understand their responsibilities. Providers should make clear how they screen and manage personnel within privileged roles.

Slack responsibility

Slack ensures that background verifications are completed for all people working at Slack prior to beginning work. These activities are performed within the legal limits of the local jurisdiction.

The concept of least privilege is applied to all Slack systems as they are all able to scope permissions based upon a defined profile.

Access to customer data is restricted specifically to a select group of privileged engineers. The exact roles and job requirements of these individuals are outlined in Slack's internal Access Matrices. Slack performs quarterly access reviews to ensure that system authorization is always backed by a necessary business justification. In the event that an employee is terminated or leaves, Slack revokes all system access as soon as possible (always within 24 hours).

Customer responsibility

Customers are responsible for hiring and training their own personnel, as well as ensuring the correct roles are assigned to users.

7. NCSC Cloud Security Principle: Secure development

NCSC Guidance: *Services should be designed and developed to identify and mitigate threats to their security. Those which aren't may be vulnerable to security issues which could compromise your data, cause loss of service or enable other malicious activity.*

Slack responsibility

Operational security at Slack begins with our Secure Development Lifecycle (blog here), which ensures that all new features released are reviewed by the product security team. There is also a dedicated team within the product security umbrella that is focused on developing secure-by-default libraries for Slack engineers to use. Both teams collaborate extensively with the broader engineering organization to educate developers on security best practices, and to ensure that security is part of development workflows from the architecture phases of projects.

Customer responsibility

Customers are responsible for the secure development of internal integrations added to their org.

Additional resources:

- Best practices for security

8. NCSC Cloud Security Principle: Supply chain security

NCSC Guidance: *The service provider should ensure that its supply chain satisfactorily supports all of the security principles which the service claims to implement.*

Cloud services often rely upon third party products and services. Consequently, if this principle is not implemented, supply chain compromise can undermine the security of the service and affect the implementation of other security principles.

Slack responsibility

Slack's subprocessors (external providers that process customer data) are evaluated by Slack risk and compliance personnel to ensure that they employ adequate security controls throughout their respective environments. In the event that Slack onboards another subprocessor, Slack personnel will perform security reviews as part of the due diligence process. Slack performs annual risk assessments of subprocessors to ensure that they are adequately maintaining their security and compliance posture.

All roles and responsibilities between Slack and the subprocessors are defined and reviewed by both legal and security teams prior to onboarding a subprocessor.

We do provide contractual commitments through our Terms of Service (ToS) or a Master Services Agreement (MSA) to ensure that third-party providers maintain, at a minimum, reasonable levels of security.

Slack has a Security Review program for our App Directory Applications. For details of the process, please see Slack App Security Review.

Customer responsibility

Customers are responsible for reviewing third-party apps added to their org.

Slack is at its most powerful when you connect it to tools you already use. With your permission, apps and integrations can access your workspace's information to help you automate tasks and get work done.

To make your data more secure, it's important to understand how apps work with Slack. That way, you can come up with a policy for reviewing and approving integrated tools.

Get to know apps for Slack

By default, members can install any app from the Slack App Directory or build internal integrations to fit your company's needs. Depending on your security preferences, Workspace Owners can control how apps are installed, and by whom.

Org owners and org admins can manage apps for all workspaces in their org from the Admin dashboard:

- Approve apps for members to install
- Restrict apps so members cannot install them
- View all installed, approved and restricted apps across their org

Approve or restrict apps for your org

If there's an app management policy in place for your org, apps will need to be approved before members can install them to their workspace. Org owners and org admins can approve or restrict apps for every workspace in their Enterprise Grid org.

Note: If an app is approved at the org level, Workspace Owners can still restrict it for their workspace. If an app is restricted at the org level, Workspace Owners can't approve it for their workspace.

View your org's apps

Org owners and org admins can see which apps are installed, approved or restricted across workspaces in their org, along with details about what permissions the app requires.

Understand app permissions

All apps in our App Directory have a unique set of permissions, called scopes, that tell you what information the app can access and how that information can be used. Generally speaking, an app will ask permission to do the following:

- Post information
- Perform actions
- Access information

An app's full set of permissions is listed when the app is installed. You can find a detailed list of scopes in our API documentation.

Enable app approval settings

Workspace Owners can enable the Approve apps setting for a workspace to control how and what is installed.

Control which apps can be installed

Workspace Owners can control exactly which apps get installed by creating lists of approved and restricted apps. In the App Directory, members will clearly see which apps are approved for the workspace, which apps need approval and which apps are not allowed.

Decide who can manage apps and integrations

By default, only Workspace Owners can manage apps. With the Approve apps setting turned on, Owners can allow selected members to manage approved apps and respond to app installation requests.

Develop an approval policy

Whether members are requesting apps or installing them as needed, protect your workspace by developing an app approval policy aided by your IT, security and policy teams.

Carefully consider internal protocols relating to data management to devise a policy that feels right for your team. Here are some questions to include in your review:

Installing apps

- Is there a valid business reason for using the app?
- Are other apps being used for this purpose?
- How long will the app be needed in the workspace?
- What is the app's privacy policy?
- How often will the app post to a channel?
- Are there any additional costs or licences?

Creating internal integrations

- Who will maintain the integration?
- Are additional servers, databases or integrations needed?
- Does the app use token validation?
- Is data encrypted at rest?
- Is TLS being used to encrypt traffic?
- Have the OWASP Top 10 Application Security Risks been reviewed?

Additional resources:

- Security recommendations for approving apps
- Manage apps on Enterprise Grid

9. NCSC Cloud Security Principle: Secure user management

NCSC Guidance: *Your provider should make the tools available for you to securely manage your use of their service. Management interfaces and procedures are a vital part of the security barrier, preventing unauthorised access and alteration of your resources, applications and data.*

The aspects to consider are:

- *Authentication of users to management interfaces and support channels*
- *Separation and access control within management interfaces*

9.1. NCSC Consideration: Authentication of users to management interfaces and support channels

NCSC Guidance: *In order to maintain a secure service, users need to be properly authenticated before being allowed to perform management activities, report faults or request changes to the service.*

These activities may be conducted through a service management web portal, or through other channels, such as telephone or email. They are likely to include such functions as provisioning new service elements, managing user accounts and managing consumer data.

Service providers need to ensure that all management requests which could have a security impact are performed over secure and authenticated channels. If users are not strongly authenticated then an imposter may be able to successfully perform privileged actions, undermining the security of the service or data.

Slack responsibility

Slack provides customers with controls to manage their users and admin users (see customer responsibility below).

Customers contacting our customer experience (support) team will be required to verify their identity. Support agents ask customers to use the use /verify command within the product to generate a six-digit verification code to identify themselves. This is used whenever administrative actions are requested.

Customer responsibility

Customers are responsible for integrating and managing their identity provider (for single sign-on and provisioning) as well as assigning roles in Slack.

Slack uses role-based access control (RBAC) and each role has its own level of permissions and access.

For an Enterprise Grid org, member permissions exist at both the org and workspace level.

For an overview of org-level and workspace-level roles and permissions, please see:

- Permissions in a Slack workspace
- Permissions in an organisation

Access to workspace-level or org-level administration would require the user to authenticate (please see 10. Identity and authentication) and have an administrative role (workspace owner/admin, org owner/admin).

Additional resources:

- Permissions in Slack
- Permissions in an organisation

9.2. NCSC Consideration: Separation and access control within management interfaces

NCSC Guidance: *Many cloud services are managed via web applications or APIs. These interfaces are a key part of the service's security. If users are not adequately separated within management interfaces, one user may be able to affect the service, or modify the data of another.*

Your privileged administrative accounts probably have access to large volumes of data. Constraining the permissions of individual users to those absolutely necessary can help to limit the damage caused by malicious users, compromised credentials or compromised devices.

Role-based access control provides a mechanism to achieve this and is likely to be a particularly important capability for users managing larger deployments.

Exposing management interfaces to less accessible networks (e.g. community rather than public networks) makes it more difficult for attackers to reach and attack them, as they would first need to gain access to one of these networks.

Slack responsibility

Slack provides customers with controls to manage their users and admin users (see customer responsibility below).

Customer responsibility

Customers are responsible for managing admin/persistent accounts used for installing apps that use Slack's admin and Discovery APIs.

Slack has APIs for managing app approvals, creating and managing workspaces, managing invite requests, resetting sessions, provisioning and managing user accounts and groups and creating audit logs.

All admin.* scopes are obtained using the normal OAuth flow, but there are a few extra requirements. The OAuth installation **must be initiated by an Enterprise Grid admin or**

owner. Also, the installation must take place **on the Enterprise Grid org, not on an individual workspace,** using the workspace switcher during the install flow.

Slack also has a Discovery API.

Our Discovery API lets Org Owners on the Enterprise Grid plan use approved third-party apps to export or act on messages and files from Slack. The Primary Org Owner or an Org Owner can request to enable the Discovery API. Once enabled, it will be accessible to all Org Owners.

All discovery.* scopes are obtained using the normal OAuth flow, but there are a few extra requirements. The OAuth installation **must be initiated by an Enterprise Grid owner**. Also, the installation must take place **on the Enterprise Grid org, not on an individual workspace,** using the workspace switcher during the install flow.

Tokens for apps using the APIs above will be generated through our existing OAuth process, which means that they will be associated with the user who installs them.

We will not be adding procedures to ensure that the requester to API methods is the app and not the user who installed the app. Since these OAuth tokens are tied to the user/email who authorizes it, we recommend that customers create an admin/persistent account (with owner level permissions) to install these apps, so as to prevent any service disruption.

Additional resources:

- Managing app approvals
- Creating and managing workspaces
- Managing invite requests
- Resetting sessions
- Provisioning and managing user accounts and groups
- Creating audit logs
- A guide to Slack's Discovery APIs

10. NCSC Cloud Security Principle: Identity and authentication

NCSC Guidance: *All access to service interfaces should be constrained to authenticated and authorised individuals.*

Weak authentication to these interfaces may enable unauthorised access to your systems, resulting in the theft or modification of your data, changes to your service, or a denial of service.

Importantly, authentication should occur over secure channels. Email, HTTP or telephone are vulnerable to interception and social engineering attacks.

Slack responsibility

Slack provides customers with controls to manage their identity and authentication (see customer responsibility below).

Customer responsibility

Customers are responsible for integrating and managing their identity provider (for single sign-on and provisioning) as well as onboarding and offboarding of users (members and guests).

SAML-based single sign-on (SSO) gives members access to Slack through an identity provider (IDP) of your choice.

You'll need to set up a connection (or connector) for Slack with your IDP. Many providers we work with have created help pages for enabling Security Assertion Markup Language (SAML) with Slack. If your preferred identity provider doesn't have a connector with Slack, you can use a custom SAML connection.

You can choose who is required to use single sign-on to access your org: all members or all members except guests.

We recommend using the "All members except guest accounts" option, as this allows guests to sign in using their email address and password.

Owners of an org can bypass SSO authentication by using the link at the bottom of the login page. This guarantees access to your org, even if your IDP is having issues.

For an added layer of security, you can require your guests and owners to use two-factor authentication (2FA) when they sign in to Slack.

For members, mandatory 2FA should be set up through your identity provider.

For users authenticating via SSO, your identity provider is responsible for enforcing password policy.

For users authenticating via an email address, the password must be at least six characters long and can't be things like *password, 123456* or *adbcdef.* For security reasons, you can't reuse your previous password.

Slack supports member provisioning with the System for Cross-domain Identity Management (SCIM) standard. To use provisioning, you'll need to use a connector app alongside a supported identity provider. If you want to build a custom script to handle provisioning, see our SCIM API for details.

SCIM provisioning allows Workspace Owners and admins to manage members more efficiently.

What you can do:

- Create or deactivate a member
- Sync and update members' profile fields
- Create or delete an identity group
- Add or remove members from an identity group

Additional resources:

- Mandatory workspace two-factor authentication
- SAML single sign-on
- Manage members with SCIM provisioning

11. NCSC Cloud Security Principle: External interface protection

NCSC Guidance: *All external or less trusted interfaces of the service should be identified and appropriately defended.*

If some of the interfaces exposed are private (such as management interfaces) then the impact of compromise may be more significant.

You can use different models to connect to cloud services which expose your enterprise systems to varying levels of risk.

Slack responsibility

Slack configures all Access Control Lists (ACLs), security groups and ports/protocols/services to deny all by default, and permit by exception. This ensures that Slack only exposes the appropriate interfaces necessary for our customers to use the service and unnecessarily broadening the attack surface. We run scanners and automated tools to verify that these resources are properly protected.

Customer responsibility

Users access and access to customer-facing management interfaces are over the internet.

Customers are responsible for integrating and managing their identity provider (for single sign-on and provisioning), onboarding and offboarding of users (members and guests) as well as assigning roles in Slack.

Please see 10. Identity and authentication.

12. NCSC Cloud Security Principle: Secure service administration

NCSC Guidance: *Systems used for administration of a cloud service will have highly privileged access to that service. Their compromise would have significant impact, including the means to bypass security controls and steal or manipulate large volumes of data.*

The design, implementation and management of administration systems should follow enterprise good practice, whilst recognising their high value to attackers.

Slack responsibility

The concept of least privilege is applied to all Slack systems as they are all able to scope permissions based upon a defined profile. Slack utilizes a Role-Based Access Control (RBAC) model to assign system users' access. The RBAC access is defined based on users' roles and job function and adhere to the Default Access Standard.

Slack employees with access to production environment, internal tools and customer data are reviewed on a quarterly basis to ensure that their access is appropriate based on job roles and responsibilities. Any discrepancies (users no longer requiring access) are triaged accordingly.

Access to Slack's production environment requires users to log in to a Bastion Host via SSH keys and two-factor authentication.

All of the system commands that the privileged engineers need to execute in order to view customer data are logged and many would alert the security team. The security team has automated alerts that are designed to detect the unauthorized activity of a malicious actor, insider or otherwise, who is attempting to view customer data with no clear business need. Such activity would be detected and treated as a potential breach.

Customer responsibility

Customers are responsible for managing privileged accounts. That includes org admin and org owner user accounts as well as admin/persistent accounts (with owner level permissions) used to install admin apps (see Separation and access control within management interfaces).

Customers can use strong authentication (see Identity and authentication) for these accounts and monitor their activity for suspicious behavior (see Protective monitoring).

13. NCSC Cloud Security Principle: Audit information for users

NCSC Guidance: *You should be provided with the audit records needed to monitor access to your service and the data held within it. The type of audit information available to you will have a direct impact on your ability to detect and respond to inappropriate or malicious activity within reasonable timescales.*

Slack responsibility

For internal Slack logs, Slack aggregates all audit logs (network logs, syslogs, etc.), at the Audit D level, into one logging tool within our separate Security VPC. For more details on Slack's approach to logging and alerting, please see Section 5.3 of this document.

Customer responsibility

Customers are responsible for monitoring their logs and integrating and managing their security information and event management (SIEM) provider (if relevant).

Members can view access logs for their account to check for any unusual or suspicious activity. They can see:

- The time and date of each new login
- The IP address of each device that has accessed their account
- A list of devices that have accessed their account

In addition, audit logs provide a record of changes to and use of Enterprise Grid that helps keep your org secure and protect against misuse.

Logs are accessible via the Audit Logs API.

The Audit Logs API can be used by security information and event management (SIEM) tools to provide analysis of how your Slack organization is being accessed. You can also use this API to write your own applications to see how members of your organization are using Slack.

Additional resources:

- Audit logs on Enterprise Grid
- Monitoring workspace events with the Audit Logs API

14. NCSC Cloud Security Principle: Secure use of the service

NCSC Guidance: *The security of cloud services and the data held within them can be undermined if you use the service poorly. Consequently, you will have certain responsibilities when using the service in order for your data to be adequately protected.*

The extent of your responsibility will vary depending on the deployment models of the cloud service, and the scenario in which you intend to use the service. Specific features of individual services may also have bearing. For example, how a content delivery network protects your private key, or how a cloud payment provider detects fraudulent transactions, are important security considerations over and above the general considerations covered by the cloud security principles.

Slack responsibility

Slack has compiled extensive documentation on how to securely configure and use Slack, and we continue to build new features and offer additional tips on security best practices.

Customer responsibility

Customers are responsible for defining and communicating terms of service related to access to their users.

Org owners and admins can outline the rules to join and use their Slack org in a custom terms of service (TOS):

- Only org owners and admins can set or modify custom TOS
- You can set different terms for members and guests
- New members must agree to your terms when they create an account, and you can require existing members to agree the next time they sign in to Slack

Customers are responsible for claiming domains.

If your company owns or operates under multiple web domains, we can help you claim them for your Enterprise Grid org, preventing people from creating unsanctioned workspaces outside of your org.

Customers are responsible for configuring their corporate network in accordance with requirements.

If you're an IT admin, you can whitelist Slack workspaces using an SSL proxy within your corporate network. By limiting connections to your entire Slack org and/or to a list of external workspaces, you can prevent anyone on your network from signing in to a non-whitelisted workspace.

IT admins can configure an on-premises or cloud-based proxy server to intercept traffic to slack.com. The proxy inserts new HTTP headers (X-Slack-Allowed-Workspaces-Requester and X-Slack-Allowed-Workspaces) that lists the workspaces your employees can access.

Once enabled, your team will be able to access the whitelisted org and/or external workspace(s) and continue using Slack normally. If anyone tries to sign in to a workspace that isn't on the whitelist, they'll see an error message.

Customers are responsible for which devices access Slack, and how.

Enterprise mobility management (EMM)—also known as mobile device management (MDM)—gives organisations control over how their company data is used and accessed on mobile devices.

Once Slack is connected to an EMM provider, you can choose who is affected:

- All members (excluding guests) will be required to update to the Slack for EMM app; guests can sign in from any device
- All members (including guests) will be required to update to the Slack for EMM app and must use an approved device to access Slack
- All members and guests can use either the regular Slack app or the Slack for EMM app and sign in from any device

To further protect your org's data, you can choose to block file downloads and copying content, require secondary authentication or require a mandatory mobile browser on unmanaged mobile devices. The latest version of the Slack app is required.

Additional resources:

- Customise your terms of service on Enterprise Grid
- Claim domains for Enterprise Grid
- Whitelist Slack workspaces for your network
- Enable enterprise mobility management for your org
- Mobile security for Enterprise Grid orgs