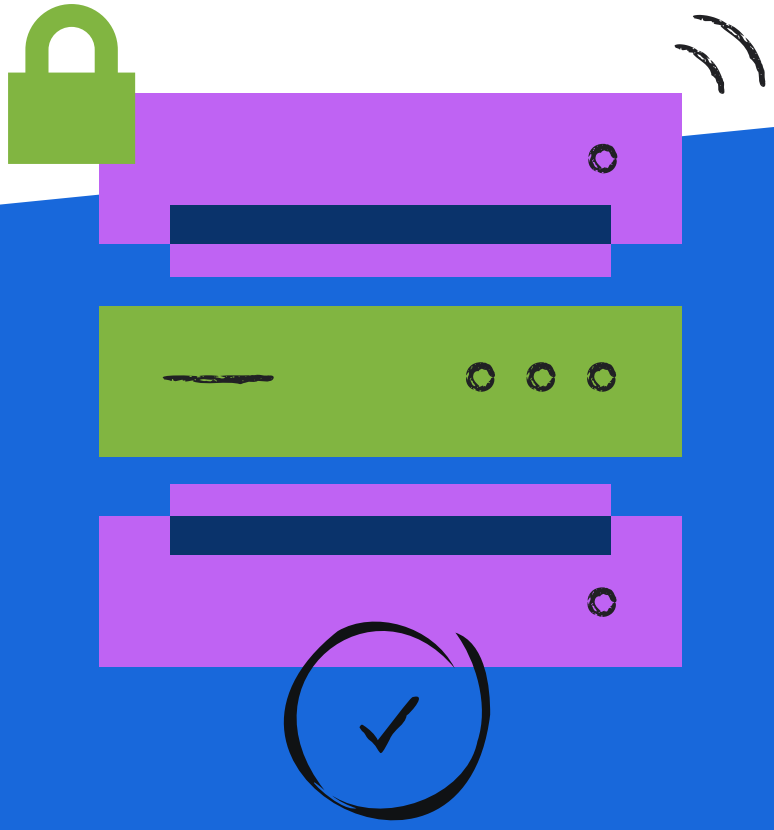
ATLASSIAN

Data Center security checklist and shared responsibilities

Security guidelines



Background

Continuing our commitment to providing our customers with the most secure products, we're pleased to introduce a security checklist that details the shared responsibilities of Atlassian and Data Center admins. This guideline provides a strong framework to help you build and sustain a secure environment.

CHECKLIST

Shared Responsibility Model

While Atlassian is committed to delivering secure products out of the box, we also rely on a shared responsibility model. This model requires customers to implement practices that continue beyond deployment and extend into operational phases. Some of these responsibilities include:

- Operating Atlassian software on private networks.
- Ensuring timely implementation of security fixes once they're released.
- Configuring Web Application Firewalls (WAF), VPNs, multi-factor authentication, and single sign-on capabilities.
- Implementing encryption and access controls.
- Performing regular backups.
- Conducting regular security audits.

This guide defines the roles and responsibilities for both Atlassian and Data Center admins that are required for the most secure product environment.

Atlassian doesn't take responsibility for self-managed hardware infrastructure.

Data Center security

This guide outlines the security measures that must be taken to ensure secure deployments for Data Center products. We've divided the responsibilities into the following sections:

- **Preparation and planning**
- **Installation**
- **Operational security best practices**
- **Advanced security measures**
- **Maintenance, backups, and upgrades**
- **Best practices for recovering after your instances have been compromised**

Preperation and planning

Product releases and updates

What Atlassian does

- ☐ Provide secure product releases and application-level security fixes.
  - Discover Long Term Support releases

Your role

- ☐ Upgrade software promptly to secure against known vulnerabilities.
  - Download the latest installation files from Data Center software download portal

Security features and configurations

What Atlassian does

- ☐ Develop products with built-in security features.
- ☐ Offer configuration guidance.
  - Check Data Center compliance and security | Atlassian

Your role

- ☐ Configure products securely.
- ☐ Manage access controls.
- ☐ Implement encryption to comply with policies.

Operating systems and software security

What Atlassian does

- ☐ Prioritize compatibility with modern, securely supported operating systems, ensuring its software solutions align with vendor-provided security updates.
  - Check supported platforms Confluence | Jira | Bitbucket | Bamboo | Crowd

Your role

- ☐ Implement the latest security updates.
- ☐ Harden the security of your operating systems.
- ☐ Manage up-to-date, secure software dependencies.

Installation and initial configuration

Infrastructure security

Ensure the security of physical and virtual servers, network security (firewalls, VPNs), and storage security (encryption, restricted access). Check out Confluence documentation.

Installation

Installing, setting up, and maintaining secure software is a collaborative effort. Make sure you select the right infrastructure for your needs and follow recommendations for secure initial setup.

What Atlassian does

- ☐ Provide secure configuration defaults to minimize vulnerability risks.
- ☐ Provide detailed guides for secure setup processes.
  - Installation Guide - Jira | Confluence
  - Infrastructure Options
- ☐ Offer a suite of tools for data encryption, user authentication, and access control. Configuration Options

Your role

- ☐ Tailor security configurations to specific deployment environments (cloud, on-premises, hybrid).
  - Kubernetes
  - Infrastructure Recommendations
  - Equipment Requirements
- ☐ Secure initial setup
  - Use a secure installation environment that is isolated from public networks.
- ☐ Apply the Principle of Least Privilege
  - Configure system access rights to strictly limit permissions to what is necessary for each user and service account during setup.
- ☐ Enable Websudo and IP Allowlisting for Configuration Access
  - Activate “websudo” for any administrative access and restrict IP addresses that can access the installation and configuration settings through IP allowlisting to ensure actions are authenticated and secure.
- ☐ Use secure, complex passwords
  - Set strong, unique passwords for all accounts created during setup, including admin accounts.

Installing, setting up, and maintaining secure software is a collaborative effort. Make sure you select the right infrastructure for your needs and follow recommendations for secure initial setup

Your role

- ☐ Implement network security measures
  - If possible, configure the installation environment to operate within private networks or VPNs to enhance security.
- ☐ Encrypt sensitive configuration data
  - Use encryption for sensitive information, including passwords and configuration files, to protect against unauthorized access.
  - Jira | Bamboo
- ☐ Set up authentication mechanisms:
  - Prepare for multi-factor authentication (MFA) and implement it once available from Atlassian
- ☐ Firewall configuration:
  - Configure firewalls to limit incoming connections only to those necessary for the operation and management of DC products.
  - Jira | Confluence | Bamboo
- ☐ Install the latest security fixes
  - Ensure that all software involved in the installation, including the operating system and dependencies, is up-to-date with the latest security updates.
- ☐ Document your configuration:
  - Keep detailed records of your installation and configuration settings for future reference and auditing purposes.
  - Jira
- ☐ Review default settings:
  - Carefully review and adjust default configuration settings to ensure they meet your security requirements.

Operational security best practices

Atlassian provides guidelines and tools to help you lay a solid security foundation for your operations. Your role as our customer is essential in ensuring the safety and protection of your data and business. To help you navigate the security measures in your environment, we've outlined a set of best practices and guidelines we recommend.

Data protection

Customer is responsible for protecting their data, which may involve encryption, backup and recovery procedures, and disaster recovery planning.

User Account and directory access control

- ☐ Run products under a dedicated, non-root user account. Secure directories against unauthorized access. We strongly recommend you:
  - Run products with a dedicated non-root user account.
  - Limit the user accounts who can access any directories.
  - To find out how to do this, check examples for DC products
    Jira | Confluence | Bitbucket | Crowd

- ☐ Monitor your binaries. If an attacker compromises an account on your system, they will usually try to gain access to more accounts. This is usually done by adding malicious code or by modifying files on the system. Consider how you might regularly verify that no malicious changes have been made.

Session and authentication security

Integrate DC products with an identity provider for single sign-on and multi-factor authentication.
Check out an example from:
Confluence

- ☐ Use personal access tokens for integrations. This provides your users a more secure way to authenticate API requests than basic authentication (using only username and password). **Learn how to manage personal access tokens**
- ☐ Disable basic authentication. If you've configured single sign-on, you can disable basic authentication for login and REST requests. Basic authentication is less secure than single sign-on and personal access tokens. **Learn how to disable basic authentication**
- ☐ Disable user accounts when people leave your organization. If required, you can also delete user accounts which will replace their name with an anonymized ID. **Delete and disable users**
- ☐ Restrict the number of users with powerful roles or group memberships. If only one department should have access to particularly sensitive information, then restrict access to the data to only those users. Don't let convenience overrule security. Don't give all staff access to sensitive data when there is no need.

Admin access

- ☐ Minimize the number of admins and avoid shared accounts. Avoid shared admin or user accounts and easily guessed usernames like 'admin'.
- ☐ Keep the number of people in the admin group limited. Remember that the people in the admin group have unrestricted access to the instance, including the ability to view restricted pages.
- ☐ Avoid creating new groups with the system admin global permission, as it may be difficult to keep track of which users have full access rights.
  - Explore how to do it in **Bitbucket**
- ☐ Use secure admin sessions to require admins to re-enter their password while accessing the admin functions.
- ☐ Set a short timeout for the admin sessions.
  - Check examples: **Jira** | **Confluence**
- ☐ Use Apache to lock down the administration interface to specific IP addresses. This can be used as a template for your reverse proxy of choice.
  - **Using Apache to limit access to the Confluence administration interface**

Activity monitoring

- ☐ Reduce the risk of brute-force attacks with Fail2Ban.
  - Check examples: **Jira** | **Confluence**
- ☐ Enable captcha on login to prevent brute force of passwords
- ☐ Use rate limiting to block REST API requests from anonymous users if you don't have a reason to allow them, or limit the number of requests to reduce the risk of DoS attacks.
  - Check examples: **Jira** | **Confluence**
- ☐ Review your audit log settings to make sure you're logging important admin and end-user actions. Make sure your logs are not accessible to the external network.
  - Check examples: **Jira** | **Confluence**
- ☐ Use access logs to identify unusual activity. Logs are written to the install directory, and you may want to monitor these logs using your preferred monitoring tool. Note that logs will be rotated after a certain amount of time. If there's a need to review logs in the longer term, ensure they are saved and backed up to an alternate disk to preserve historical data and aid in future analyses or investigations.
  - Check examples: **Jira** | **Confluence** | **Crowd**

Advanced security measures

- ☐ **Integrate Web Application Firewall (WAF).** These solutions provide dynamic, real-time rule updates to protect against vulnerabilities and attacks, while also ensuring that configurations are optimized to minimize latency and false positives. WAF safeguards the products from common threats such as injection attacks, predictable resource location attacks, HTTP DDoS, HTTP request smuggling, file path traversal, server-side request forgery (SSRF), and clickjacking

Maintenance, backups, and upgrades

Backup and restore

- ☐ Utilize Atlassian tools or native database backups, where available, for regular and testable backup strategies.
- ☐ Use your database's native backup tools to regularly back up production instances. If you use the backup/restore API, move all backup files to a dedicated secure storage for security and redundancy purposes.
  - Native database backup tools offer a much more secure, consistent, and reliable means of storing and restoring data while Data Center products are active. XML database backups of Data Center products may contain inconsistencies if the database is updated during backup.
  - Check examples: **DC Products** | **Jira** | **Confluence**

Subscribe to Advisory Alerts

- ☐ **Make sure your contact details and email subscription preferences are up-to-date** so you can receive security advisory alerts, monthly bulletins, and other important technical updates. To update your email subscription preferences visit **Atlassian email and privacy preferences**.

Regular security audits

- ☐ Know your company's security incident management process. Make sure you know who can help if a security incident occurs and what's the escalation path.
- ☐ Run regular security audits. These can help you identify potential threats and provide an opportunity to review your security policies and procedures.
- ☐ Perform 'what if' planning exercises. Consider questions like 'What is the worst thing that could happen if a privileged user's password were stolen while on vacation?
- ☐ Document your security measures, and regularly monitor that all measures are still in place. For example, after upgrading or migrating, someone may forget to apply the rule to the new system or version.
- ☐ Perform a security check-up when preparing for a major upgrade. Remember to apply Atlassian security recommendations.

Upgrade to the latest LTS

- ☐ For continued security, keep your software up to date. This is crucial for protecting against known vulnerabilities. To get the latest installation files, visit:
  - **Jira Software Data Center**
  - **Jira Service Management**
  - **Confluence Data Center**
  - **Bitbucket Data Center**
  - **Bamboo Data Center**
  - **Crowd Data Center**

Best practices for recovering after your instances have been compromised

Customers are responsible for monitoring their systems for security incidents and have procedures in place to respond to and mitigate any threats.

Step 1: Immediate post-compromise actions

1. Isolate the system. Disconnect the compromised instance from the network or internet.
2. Preserve evidence. Secure logs and data that could help in analyzing the incident.
3. Change passwords. Immediately change all administrative passwords.
4. Review user accounts. Check for unauthorized changes or new accounts.
5. Report the Incident. Contact Atlassian via SECREP and GSAC service desks with detailed information about the compromise and steps taken.

Step 2: Recovery and Communication

1. Immediate Isolation. Immediately isolate the compromised systems to prevent further spread of the threat.
2. Initial Assessment. Quickly assess the scope of the incident to understand which services and data are affected.
3. Check Atlassian service access
    - Check which Confluence pages the threat actor has visited.
    - Review access logs to determine which Bitbucket repositories were visited.
    - Identify if the threat actor accessed any Jira tickets.
4. Installing apps. Customers must be aware of the risk of installing apps.
5. Access Control. Customers must manage user accounts and access permissions, ensuring that only authorized personnel can access sensitive data and systems.
    - Determine if any customer data was compromised.
    - If the Bitbucket server was compromised, review your repositories for any committed credentials and rotate those credentials if found.
6. Plan for Recovery. Start restoring data from backups and consider rebuilding compromised systems.
7. Implement Security Measures. Based on initial findings, strengthen your security posture to prevent similar incidents. This could involve enhancing firewall rules, updating passwords, and implementing multi-factor authentication.

8. Communicate.
    - Internal Communication: Keep internal stakeholders informed about the incident status, recovery plans, and any required actions on their part.
    - External Communication: If customer data was compromised, communicate with affected customers about the data loss, steps taken to secure their data, and any actions they should take.
9. Follow Atlassian's Guidance. Once Atlassian provides insights and recommendations, incorporate them into your recovery and security enhancement efforts.
10. Root Cause Analysis. Collaborate with Atlassian to perform a thorough root cause analysis. Understand how the compromise occurred and implement measures to prevent recurrence.
11. Review and update the Incident Response Plan. Reflect on the incident response process and update your plan as necessary to improve future responses.

Step 3: Post-Recovery Analysis and Improvement

1. Review the Incident. Analyze the cause and response effectiveness and identify improvement areas.
2. Update Policies. Revise your security policies and incident response plans based on the incident review.
3. Schedule periodic security checks to uncover and fix vulnerabilities.
4. Stay Engaged with Atlassian. Utilize Atlassian resources for ongoing security best practices.
5. Educate Your Team. Ensure everyone understands the incident, its root cause, and the steps taken to prevent future compromises

ATLASSIAN

Atlassian unleashes the potential of every team. Our software development, service management and work management software helps teams organize, discuss, and complete shared work. The majority of the Fortune 500 and over 300,000 companies of all sizes worldwide - including NASA, BMW, Kiva, Deutsche Bank and Dropbox - rely on our solutions to help their teams work better together and deliver quality results on time. Learn more about our products, including Jira, Confluence and Jira Service Management at **Atlassian.com**.

Learn more at Atlassian.com.