Data Center security checklist and best practices

Background

Continuing our commitment to providing the most secure products for our customers, we're pleased to introduce a security checklist and best practices guide for admins.

This guide outlines the security measures that Atlassian takes to ensure secure deployments for Data Centre customers. It also covers recommendations and best practices for customers to ensure that they deploy and operate Atlassian software securely in their self-managed environment. We've divided our recommendations 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

With the checklist we also promote our shared responsibility model that clearly defines Atlassian and your, our customer's, roles and responsibilities in ensuring most secure way of running the business.

Download PDF version

Data_Center_security_checklist_and_best_practices.pdf

Shared Responsibility Model

We have implemented the Shared Responsibility Model, which covers both Atlassian's and customers' responsibilities pertaining to product releases and updates, security features and configurations, infrastructure security, as well as operating system and software security. This model sets out the specific security-related responsibilities and recommended best practices for customers to guarantee comprehensive development security through collaborative efforts.

Preparation and planning

Product releases and updates

What Atlassian does	Your role
☐ Provides secure product releases and application-level security fixes. • Discover Long Term Support releases	☐ Update software promptly to secure against known vulnerabilities. • To download the latest installation files visit Data Center software download portal

Security features and configurations

What Atlassian does	Your role
☐ Develops products with built-in security features and offers configuration guidance. • Check Data Center compliance and security | Atlassian	☐ Configure products securely. ☐ Manage access controls. ☐ Implement encryption as per policies.

Operating systems and software security

What Atlassian does	Your role
☐ Emphasizes compatibility with modern, securely supported operating systems, ensuring its software solutions align with vendor-provided security updates. • Check https://confluence.atlassian.com/doc/supported-platforms-207488198.html	☐ 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.

> Atlassian doesn't take responsibility for self-managed hardware infrastructure. Follow our recommendations and best practices included in this document.

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

- [ ] Commits to minimizing vulnerability risks by providing **secure configuration defaults**.
- [ ] Provides detailed guides for secure setup processes.
  - Installation Guide - Jira | Confluence
  - Infrastructure Options
- [ ] Offers 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**
  - Ensure the installation environment is secure and 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.
- [ ] **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 lay a solid security foundation for your operations. Your, our customer role is essential in making sure your data is safe and your business is protected.

> Atlassian doesn't take responsibility for self-managed hardware infrastructure. Follow our recommendations and best practices included in this document.

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'.
- [ ] **Limit the number of people in the admin group.** Members of this 'supergroup' can access all admin functions and access all content, including restricted pages, instead of creating a new group with system admin global permissions.

  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.

  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 you company 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.** Regular security audits can help you identify potential threats and also 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.** It's a good time to check your current configuration against our current recommendations.

Upgrade to the latest LTS

- [ ] **Upgrade to the latest supported LTS or feature version.** 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

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. **Investigate Malicious Activity**
    - Check if any malicious plugins were installed on your Atlassian services
    - 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.
5. **Plan for Recovery.** Start restoring data from backups and consider rebuilding compromised systems.
6. **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.
7. **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.
8. **Follow Atlassian's Guidance.** Once Atlassian provides insights and recommendations, incorporate them into your recovery and security enhancement efforts.
9. **Root Cause Analysis.** Collaborate with Atlassian to perform a thorough root cause analysis. Understand how the compromise occurred and implement measures to prevent recurrence.
10. **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.