# CIS DigitalOcean Foundations Benchmark

v1.0.0 - 07-29-2025

# Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

**NOTE**: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

# Table of Contents

# Overview

All CIS Benchmarks™ (Benchmarks) focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the Benchmarks are designed to be a key **component** of a comprehensive cybersecurity program.

## Important Usage Information

All Benchmarks are available free for non-commercial use from the CIS Website. They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)
- CIS Benchmarks™ Certified 3rd Party Tooling

These tools make the hardening process much more scalable for large numbers of systems and applications.

**NOTE**: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that ***ALL*** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

### Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

## Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.

- **Use the most recent version of a Benchmark**: This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

## Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

## Remediation

CIS has developed Build Kits for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's “Remediation” section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

**When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.**

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
  - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
  - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
  - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
  - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
  - When the initial deployment above is completes successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

## Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

**NOTE**: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the CIS Website. All other formats of the CIS Benchmarks™ (MS Word, Excel, and Build Kits) are available for CIS SecureSuite® members.

CIS-CAT® Pro is also available to CIS SecureSuite® members.

## Target Technology Details

This document provides foundational security recommendations of DigitalOcean's platform. Each recommendation is integral to consider when designing your infrastructure on the DigitalOcean platform. This Benchmark is intended to be used in tandem with the CIS DigitalOcean Service Category Benchmark as most of the provided recommendations are not product-specific.

To obtain the latest version of this guide, please visit http://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at BenchmarkInfo@cisecurity.org.

For Cloud Service Providers, the "Foundations" Benchmark is meant to be used as a first step which is complimented by "Service Category" Benchmarks as a second step. This relationship is further explained in the "Introduction" section.

## Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, platform deployment, and/or DevOps personnel who plan to develop, deploy, assess, or secure solutions using the DigitalOcean platform.

## Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

## Typographical Conventions

The following typographical conventions are used throughout this guide:

| Convention | Meaning |
|---|---|
| `Stylized Monospace font` | Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented. |
| `Monospace font` | Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented. |
| `<Monospace font in brackets>` | Text set in angle brackets denote a variable requiring substitution for a real value. |
| *Italic font* | Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication. |
| **Bold font** | Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal). |

# Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable.  If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

## Title

Concise description for the recommendation's intended configuration.

## Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

### Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

### Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

## Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

## Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

## Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

## Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

## Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

## Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

## Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

## References

Additional documentation relative to the recommendation.

## CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

## Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide security focused best practice hardening of a technology; and
  - limit impact to the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is more critical than manageability and usability
  - acts as defense in depth measure
  - may impact the utility or performance of the technology
  - may include additional licensing, cost, or addition of third party software

## Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

**Author**
Beatrix H

**Contributor**
Mike Wicks

**Editor**
David Lopez
Heather Cannon
Tim Lisko

# Recommendations

## 1 Introduction

This introduction section and the subsections herein provide informative articles which instruct on the use of the CIS Foundations and Service Category Benchmarks. No recommendations will be found in this section, just articles of relevant information.

Please carefully review the articles in this introductory section and orient yourself with our structured approach to Benchmarking for Cloud Service Providers (CSPs). This approach differs from other CIS Benchmarks because:

- there are too many different products/services in CSP product directories to practically cover in any one Benchmark,
- architectural and design decisions will affect the scope and relevance of recommendations, and
- there are a variety of methods for interfacing with CSP products and services.

**Cloud Benchmarks - A Two-Step Approach to Securing Your Cloud Environments:**

- **Step 1:** Start with Foundations Benchmarks. Apply as many recommendations as **practical** for your environment; "100%" 'compliance' is not always possible. Not all Foundations Benchmark recommendations can be applied at the same time, and not all recommendations will be relevant to your environment. Use the recommendation Profile Levels and your understanding of your unique environment architecture to determine which recommendations are in scope.
- **Step 2:** Use the Service Category Benchmarks for service-specific defense-in-depth recommendations. Apply recommendations only for the services **IN USE** in your environment. Use the recommendation Profile Levels, and your understanding of your unique environment architecture to determine which recommendations are in scope.

## 1.1 CIS DigitalOcean Foundations Benchmarks

The suggested approach for securing your DigitalOcean cloud environment is to start with the **latest version** of the CIS DigitalOcean Foundations Benchmark. Because CSP environments are constantly changing, previous versions of the Foundations Benchmarks should not be used. Previous releases may contain incorrect product names, outdated procedures, deprecated features, and other inaccuracies. The CIS Foundations Benchmark provides prescriptive guidance for configuring a subset of DigitalOcean Services with an emphasis on foundational, testable, and architecture agnostic settings for services.

The DigitalOcean Foundations Benchmark is what you should start with when beginning to secure your DigitalOcean environment. It is also the foundation for which all other DigitalOcean Service Category Benchmarks are built on so that as you grow your cloud presence and usage of the services offered you have the necessary guidance to securely configure your environment as it fits with your company's policy.

All CIS Benchmarks are created and maintained through consensus-based collaboration. Should you have feedback, suggested changes, or just like to get involved in the continued maintenance and development of CIS DigitalOcean Benchmarks, please register on CIS WorkBench at https://workbench.cisecurity.org and join the CIS DigitalOcean Benchmarks Community.

## 1.2 CIS DigitalOcean Services Benchmarks

After configuring your environment with the CIS DigitalOcean Foundations Benchmark, we suggest pursuing defense-in-depth and service-specific recommendations for your DigitalOcean Services by reviewing the Service Category Benchmarks. The Service Category Benchmarks are being produced with the vision that recommendations for all security-relevant products/services offered by a CSP should have a 'home,' but the Foundations Benchmarks should retain the most crucial recommendations and not be made vast, intimidating, and impractical.

The Service Category Benchmark recommendations should be applied **ONLY** for the CSP products and services that are actively **IN USE** in your environment. In each Service Category Benchmark, you may find that your environment uses none, or only a couple services from a list of many. Please review the services employed in your environment carefully to accurately scope the recommendations you apply. Failure to apply only the recommendations you need may introduce vulnerabilities, technical debt, and unnecessary expenses.

Using the DigitalOcean Product Directory (https://www.digitalocean.com/products) as a source of categorical grouping of these services, our vision is to produce a full set of CIS DigitalOcean Service Category Benchmarks to cover all security-relevant services. A list of planned and published Service Category Benchmarks for the DigitalOcean Community can be found on the community dashboard here: https://workbench.cisecurity.org/communities/190.

**Please Note - There is currently one Service Category Benchmark in the DigitalOcean Community (CIS DigitalOcean Services Benchmarks)** This family of Benchmarks will be expanded on in the future.

**Your help is needed to bring this vision to life!** Please consider joining our CIS DigitalOcean Community to contribute your expertise and knowledge in securing products and services from the DigitalOcean product family.

All CIS Benchmarks are created and maintained through consensus-based collaboration. Should you have feedback, suggested changes, or just like to get involved in the continued maintenance and development of CIS DigitalOcean Benchmarks, please register on CIS WorkBench at https://workbench.cisecurity.org and join the CIS DigitalOcean Benchmarks community.

# 2 Account Access

This section contains recommendations for configuring Account Access DigitalOcean for improved security.

## *2.1 Ensure Secure Sign In for Teams is Enabled (Manual)*

**Profile Applicability:**

- Level 1

**Description:**

At DigitalOcean, when a team owner requires team members to use a secure sign-in method, only team members who log in to DigitalOcean via **Google or GitHub** or a **DigitalOcean account with two-factor authentication (2FA)** can access the team. This functionality can be enabled during **team creation** or anytime thereafter.

**Rationale:**

Ensuring team members leverage secure sign in methodologies is important for:

- **Enhanced Security:** Secure sign-in methods, such as two-factor authentication (2FA) via Google, GitHub, or DigitalOcean's own 2FA, add an extra layer of protection against unauthorized access.
- **Access Control:** By requiring secure sign-in, team owners introduce a control which limits access to team resources to authorized members, thereby reducing the risk of unauthorized access and misuse of resources.
- **Risk Mitigation:** Enforcing secure sign-in mitigates risks associated with weak passwords or compromised accounts.

**Impact:**

There are no major adverse consequences to enabling secure sign on for Teams.

**Audit:**

1. Click the profile icon in the top right of the **Control Panel** https://cloud.digitalocean.com/ to open the drop-down menu.
2. Click `Switch Teams`.
3. Click the name of the team you want to audit for secure sign-in.
4. On the left menu of the Control Panel, click `Settings` to go to the Team Settings page.
5. View the status of secure sign-in in the `Secure sign-in section` within the `Team tab`.

**Remediation:**

1. To require secure sign-in for a team, first switch to the team in the **Control Panel** https://cloud.digitalocean.com/. Click the profile icon in the top right to open the drop-down menu, click `Switch Teams`, then click the name of team you want to update.

2. In the left menu of the control panel, click `Settings` to go to the `team settings page` [https://cloud.digitalocean.com/account/team] (https://cloud.digitalocean.com/account/team). In the `Secure sign-in` section, click `Enable`.
3. In the window that opens, click `Enable Secure Sign-In`. This notifies all team members via email that secure sign-in is now required.

If your DigitalOcean account doesn't use a secure sign-in, you are then prompted to **update your sign-in method**.
Similarly, when a team member without an accepted sign-in method tries to access the team, they are prompted to update their sign-in method to regain access to the team. This prevents team members from accessing the team until they switch to **Google or GitHub** or **enable 2FA on their DigitalOcean account**.

**References:**

1. https://docs.digitalocean.com/platform/accounts/settings/#sign-in-method
2. https://docs.digitalocean.com/platform/accounts/2fa/
3. https://docs.digitalocean.com/platform/teams/how-to/create/
4. https://cloud.digitalocean.com/
5. https://cloud.digitalocean.com/account/team

**CIS Controls:**

| **Controls Version** | **Control** | **IG 1** | **IG 2** | **IG 3** |
|---|---|---|---|---|
| v8 | 6.7 Centralize Access Control<br>Centralize access control for all enterprise assets through a directory service or SSO provider, where supported. | | ● | ● |

## *2.2 Ensure Two Factor Authentication for all Accounts/ Teams is Enabled (Manual)*

**Profile Applicability:**

- Level 1

**Description:**

To understand two-factor authentication (2FA), we must first understand *authentication factors*. An *authentication factor* is a piece of information used to verify that you're allowed to do something, like a keycard used to unlock a hotel door.

The following list presents a non-exhaustive list of authentication factors:

- **Something you know**: Private knowledge that only you have(e.g. Password or PIN).
- **Something you have**: Physical object that only you have(e.g. phone, a key, or a bank card).
- **Something you are**: Physical characteristic that only you have(e.g. Fingerprint or your voice).

With that in mind, consider that 2FA is a form of verification that requires two authentication factors. An example of this, in practice, is a bank requiring your bank card (something you have) and your PIN (something you know) before allowing you to withdraw funds.

When you first create your account, 2FA is disabled by default; but, enabling and subsequently auditing the functionality is simple.

**Rationale:**

Enabling two-factor authentication is important for:

- **Enhanced Security:** 2FA adds an extra layer of protection by requiring not just a password (something you know), but also a second form of verification, such as a code sent to your phone (something you have).
- **Compliance:** Implementing 2FA promotes an organization's adherence to many regulatory and cybersecurity frameworks (e.g. HIPAA, PCI DSS, etc.)

**Impact:**

Provided Two-factor authentication relies on device ownership, there is a risk of exploitation should the device be confiscated by a bad actor.

**Audit:**

1. Log in to the **Control Panel** https://cloud.digitalocean.com/.

2. Click the profile icon in the top right corner.
3. In the menu that opens, click `My Account` to go to your `My Account` page.
4. View the `Sign-in method` row.
   a. If you used Google or Github as your Sign-in method, Two-factor **authentication** is enabled, but the section will not appear.
   b. If you used email as your Sign-in method, the Two-factor authentication section will appear below the Sign-in method. The section will have a button labeled `Set Up 2FA` if it has not already been set up.
5. Scroll to the bottom of the page to view a listing of your team members. The fourth column shows each member's sign-in method and indicates if they enabled 2FA.

**Remediation:**

1. Log in to the **Control Panel** https://cloud.digitalocean.com/ and click the profile icon in the top right corner.
2. In the menu that opens, click `My Account` to go to your **My Account page**. Then, in the `Two-factor authentication` section, click `Set Up 2FA`.
3. When you click the `Set Up 2FA` button, the `Set up two factor authentication` window opens on the `Choose Method`step. You need to choose your authentication method: either using an authentication app or using SMS.
   **Using an Authentication App (Recommended)**
   Authenticator apps like **Google Authenticator**, **Authy**, **1Password**, **Microsoft Authenticator**, and **Duo** are small, free mobile applications used to generate security codes. They work globally and are more secure than SMS because they don't transmit the security codes across the network.
   When you choose this method, you need to scan the provided QR code using the authenticator app on your phone or tablet. This links your device to your DigitalOcean account.
   If you're unable to scan the QR code, click the Try this instead link directly underneath it to get a numerical code which you can enter manually. Follow the directions in your specific authenticator app to enter the code, then enter the PIN that the app gives you in the space provided. Once you've entered the PIN, the app links with your DigitalOcean account.
   Once your DigitalOcean account and 2FA app are linked, when you log in to DigitalOcean, you need to open the app and enter the code provided in the control panel to finish logging in.
   Some authenticator apps have features like backups and syncing to help you restore access to the app if you lose your device. We recommend using these features for added reliability.
   **Using SMS**
   If you select SMS, your mobile carrier must be able to deliver a text message, which means you need mobile signal or an internet connection. This may be inconvenient when traveling internationally. In addition, because SMS messages are vulnerable to being intercepted by hackers, they're not as secure as an app.

However, using SMS for 2FA still provides much stronger security for your account than not enabling 2FA at all.
   When you select SMS, you are prompted for the phone number. You cannot use VoIP or Telephony telephone numbers from services like Google Voice or Ooma. Once you enter the code, DigitalOcean sends a code via SMS. When you receive it, enter the code to link your phone and your account. From then on, you receive codes via SMS to enter into the control panel to complete your login.
4. Once you've configured your primary method for 2FA, you need to add a backup method. This is how you can regain access to your account if your 2FA device is lost or stolen. You can use backup codes or an authenticator app. We recommend using backup codes.
   **Backup Codes (Recommended)**
   Backup codes act like a second password, so store them in a secure place that you can access without your phone.
   Backup codes are visible on-screen when you enable 2FA. You can also download a .txt file called digitalocean_backupcodes.txt.
   Backup codes are single use, so it can be helpful to delete or cross out a backup code once you use it. If you only have a few valid backup codes left, you can generate more. When you regenerate backup codes, any remaining codes from before are no longer valid.
   **Authenticator App**
   You can use an authenticator app like Google Authenticator or Duo as your backup solution.
   We do not recommend this because it is phone-based, and only selectable as a backup option if you select SMS as your primary 2FA solution. In the scenario where you can't access your SMS messages and need to use a backup method, your phone might not be a valid option to use due to whatever is preventing SMS access.
   For this reason, we recommend using an authenticator app as your primary 2FA method with backup codes.

**Default Value:**

Two-factor authentication is disabled by default.

**References:**

1. https://en.wikipedia.org/wiki/Keycard_lock
2. https://cloud.digitalocean.com/account/profile
3. https://support.google.com/accounts/answer/1066447?hl=en
4. https://authy.com/
5. https://1password.com/
6. https://www.microsoft.com/en-us/account/authenticator
7. https://duo.com/

**Additional Information:**

If you log in to DigitalOcean with Google or GitHub, you manage 2FA with your Google or GitHub account instead of your DigitalOcean account.

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.4 Require MFA for Remote Network Access<br>Require MFA for remote network access. | ● | ● | ● |
| v8 | 6.7 Centralize Access Control<br>Centralize access control for all enterprise assets through a directory service or SSO provider, where supported. |  | ● | ● |

## *2.3 Ensure SSH Keys are Audited (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

Secure Shell (SSH) keys are a pair of cryptographic keys that operate as a more secure method to authenticate to a server as opposed to a password. Technically, SSH is a network protocol used to securely access and manage machines over an unsecured network.

SSH keys must be added prior to Droplet creation and cannot be retroactively added to Droplets when other keys are added. When the authorized keys are placed on a Droplet, they control access to the root account only, not named users accounts. Access for named users must be set up individually on the Droplet operating system, not via the DigitalOcean cloud platform.

Auditing SSH keys is a process that involves reviewing and verifying the security and appropriateness of SSH keys used within an organization. This process is crucial for maintaining security and compliance, especially in environments where SSH is used extensively for remote access and authentication. Some important aspects of SSH key use are ensuring the key is generated using a secure algorithm, ensuring the private key is securely stored, and verifying the public and private keys are correctly paired.

**Rationale:**

Auditing SSH keys is important for several reasons. including:

- **Compliance with Regulatory Requirements:** Implementing SSH keys promotes an organization's adherence to cybersecurity frameworks (e.g. SOC 2).
- **Prevention of Unauthorized Access:** If compromised or unmanaged, SSH keys can provide unauthorized access to systems. As such, auditing helps identify and mitigate this risk by ensuring all keys are accounted for and properly secured.

**Impact:**

There are no major adverse consequences to auditing SSH keys.

**Audit:**

To check if your DigitalOcean account has an SSH key associated:

1. Log into your **Control Panel**.
2. Select `Settings` in the bottom left of the panel.
3. Select the `Security` tab in the settings menu.
4. In the `SSH Keys` section, you should see a list of all the SSH keys associated with your DigitalOcean account. Each SSH key is typically identified by a name

you provided when you added it. If there are SSH keys listed, it means you have SSH keys associated with your account.

5. Verify the key details by clicking on each SSH key to view its details, including the name, fingerprint, and the date it was added. This can help you confirm the existence of your SSH key.

If you do not see any SSH keys listed in this section, it means that there are no SSH keys associated with your DigitalOcean account. In that case, follow the steps outlined in the remediation.

**Remediation:**

*Add SSH Keys to a Team*

### Using the Control Panel

1. Log in to the **Control Panel** and switch to the team you want to use.
2. In the left menu, click Settings, then click the Security tab to go to the **team security settings page**.
3. In the `SSH Keys` section, click `Add SSH Key` to open the `New SSH key` window.
4. Copy your public key into the `Public Key` field. It's safe to freely share your **public SSH keys** because you cannot recreate a private key using a public key. You can only use a public key to validate the user who holds the associated private key.
5. Enter a name in the `Key Name` field, which lets you identify this key in the Control Panel. We recommend using the name of the machine you copied the public key from.
6. Finally, click `Add SSH Key` to add the key to your team.

### Using the API or CLI
### CLI

1. Install `doctl`, the official DigitalOcean CLI.
2. Create a personal access token and save it for use with `doctl`.
3. Use the token to grant `doctl` access to your DigitalOcean account.

```
doctl auth init
```

4. Finally, run

```
doctl compute ssh-key create
```

Basic usage looks like this, but you can read the usage docs for more details:

```
doctl compute ssh-key create <key-name> [flags]
```

### API

1. Create a personal access token and save it for use with the API.
2. Send a POST request to https://api.digitalocean.com/v2/account/keys.

### cURL

Using cURL:

```
curl -X POST \
  -H "Content-Type: application/json" \
  -H "Authorization: Bearer $DIGITALOCEAN_TOKEN" \
  -d '{"name":"My SSH Public Key","public_key":"ssh-rsa
AEXAMPLEaC1yc2EAAAADAQABAAAAQQDDHr/jh2Jy4yALcK4JyWbVkPRaWmhck3IgCoeOO3z1e2dBo
wLh64QAM+Qb72pxekALga2oi4GvT+TlWNhzPH4V example"}' \
  "https://api.digitalocean.com/v2/account/keys"
```

### Go

Using **Godo**, the official DigitalOcean API client for Go:

```
import (
    "context"
    "os"

    "github.com/digitalocean/godo"
)

func main() {
    token := os.Getenv("DIGITALOCEAN_TOKEN")

    client := godo.NewFromToken(token)
    ctx := context.TODO()

    createRequest := &godo.KeyCreateRequest{
        Name:      "My SSH Public Key",
        PublicKey: "ssh-rsa
AEXAMPLEaC1yc2EAAAADAQABAAAAQQDDHr/jh2Jy4yALcK4JyWbVkPRaWmhck3IgCoeOO3z1e2dBo
wLh64QAM+Qb72pxekALga2oi4GvT+TlWNhzPH4V example",
    }

    transfer, _, err := client.Keys.Create(ctx, createRequest)
}
```

### Ruby

Using **DropletKit**, the official DigitalOcean API client for Ruby:

```
require 'droplet_kit'
token = ENV['DIGITALOCEAN_TOKEN']
client = DropletKit::Client.new(access_token: token)

ssh_key = DropletKit::SSHKey.new(
  name: 'My SSH Public Key',
  public_key: 'ssh-rsa
AEXAMPLEaC1yc2EAAAADAQABAAAAQQDDHr/jh2Jy4yALcK4JyWbVkPRaWmhck3IgCoeOO3z1e2dBo
wLh64QAM+Qb72pxekALga2oi4GvT+TlWNhzPH4V example'
)
client.ssh_keys.create(ssh_key)
```

**Python**

Using PyDo, the official DigitalOcean API client for Python:

```
import os
from pydo import Client

client = Client(token=os.environ.get("DIGITALOCEAN_TOKEN"))

req = {
  "public_key": "ssh-rsa
AEXAMPLEaC1yc2EAAAADAQABAAAAQQDDHr/jh2Jy4yALcK4JyWbVkPRaWmhck3IgCoeOO3z1e2dBo
wLh64QAM+Qb72pxekALga2oi4GvT+TlWNhzPH4V example",
  "name": "My SSH Public Key"
}

resp = client.ssh_keys.create(body=req)
```

## *Remove SSH Keys from a Team with the Control Panel*

1. Log in to the **Control Panel** and switch to the team you want to use.
2. In the left menu, click `Settings`, then click the `Security tab` to go to the team security settings page. The `SSH keys` section lists any keys already added to the team.
3. In the **(…)** menu next to each key in the table, you can edit the key or delete it entirely. Deleting an SSH key from a team only removes the ability to create new Droplets with that key already added. It does not remove that SSH key from any Droplet's SSH configuration.

Please refer to the following sources for additional information on working with SSH keys on DigitalOcean:

1. **SSH Essentials: Working with SSH Servers, Clients, and Keys**
2. **Understanding the SSH Encryption and Connection Process**

**References:**

1. https://cloud.digitalocean.com/account/profile
2. https://www.digitalocean.com/community/tutorials/ssh-essentials-working-with-ssh-servers-clients-and-keys

3. https://www.digitalocean.com/community/tutorials/understanding-the-ssh-encryption-and-connection-process#authenticating-the-user-s-access-to-the-server
4. https://docs.digitalocean.com/products/droplets/how-to/connect-with-ssh/
5. https://docs.digitalocean.com/products/droplets/how-to/add-ssh-keys/to-existing-droplet/
6. https://cloud.digitalocean.com/account/security
7. https://en.wikipedia.org/wiki/Home_directory
8. https://docs.digitalocean.com/products/droplets/how-to/add-ssh-keys/create-with-putty/#working-with-putty-s-public-key-format
9. https://docs.digitalocean.com/reference/doctl/how-to/install/
10. https://docs.digitalocean.com/reference/api/create-personal-access-token/
11. https://docs.digitalocean.com/reference/doctl/reference/compute/ssh-key/create/
12. https://docs.digitalocean.com/reference/api/digitalocean//#operation/sshKeys_create
13. https://github.com/digitalocean/godo
14. https://github.com/digitalocean/droplet_kit
15. https://github.com/digitalocean/pydo

### Additional Information:

Can't find your key pair? By default, your key files are saved to the hidden SSH folder in your home directory, and your public key ends in `.pub`.

- On Linux, your public key is typically `/home/your_username/.ssh/id_rsa.pub`.
- On macOS, it's typically `/Users/your_username/.ssh/id_rsa.pub`.
- On Windows, it's typically `/Users/your_username/.ssh/id_rsa.pub`. If you generated your key pair with PuTTYgen, you need to use PuTTYgen to view the public key in the appropriate format.

### CIS Controls:

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 4.6 Securely Manage Enterprise Assets and Software<br>Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential. | ● | ● | ● |

## *2.4 Ensure a Distribution List is used as the Team Contact Email (Manual)*

**Profile Applicability:**

- Level 1

**Description:**

The team contact email is where DigitalOcean sends operational alerts and maintenance notices. By default, the team contact email is the email address of the person who created the team.

Everyone on a team can view the team contact email, but only owners can change it on the team settings page.

Emails that are sent exclusively to the team contact email include:

- Resource alerts, like deployment failures and failovers
- Alert policy notifications
- Emergency migration or reboot notices
- SSL certificate renewal notices

Additionally, some team emails are sent only to people with specific roles:

- Billing emails are sent to owners and billers.
- Droplet password emails are sent to whoever created the related Droplet.
- Support ticket emails are sent to everyone who participated in the support ticket.

Using a distribution list email instead of an individual’s as the team contact prevents a single point of failure for account access if that person becomes unavailable.

**Rationale:**

Using a distribution list as the email contact email is important for several reasons, including:

- **Ensures multiple people receive communications:** A distribution list sends emails to a defined group of recipients, so all relevant team members get important notifications simultaneously without relying on a single individual.
- **Streamlines communication**: Distribution lists simplify sending emails to groups without typing each address individually, saving time and reducing errors.
- **Reduces risk**: If the contact email is tied to one person who leaves or is unavailable, critical messages could be missed. A distribution list avoids this by having multiple recipients who can respond or escalate as needed.

**Impact:**

There are no adverse consequences with using a distribution list as the team contact email.

**Audit:**

1. Log into the [Control Panel](https://cloud.digitalocean.com/).
2. Select `Settings` in the lower left hand corner.
3. Find `Team Contact Email` in the `Team` tab.
4. Confirm it is the distribution list email address. If not, follow the remediation steps.

**Remediation:**

1. Create a distribution email list according to your email service provider's instructions.
2. Log in to the [Control Panel](https://cloud.digitalocean.com/).
3. Select `Settings`.
4. Find `Team Contact Email` in the `Team` tab and select `Edit`.
5. Change the email address to the distribution list email address.
6. Select `Update`.

**Default Value:**

By default, the team contact email is the email address of the person who created the team.

**References:**

1. https://cloud.digitalocean.com/account/team
2. https://cloud.digitalocean.com/

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 17.1 Designate Personnel to Manage Incident Handling<br>Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard. | ● | ● | ● |

# 3 API

This section contains recommendations for configuring DigitalOcean API for improved security.

## *3.1 Ensure Legacy Tokens are Replaced with Scoped Tokens (Manual)*

**Profile Applicability:**

- Level 1

**Description:**

A token is a secure string used to authenticate and authorize access to an API or service (e.g. DigitalOcean's API). When you include a token in your API requests, it proves your identity and grants you permissions to perform certain actions on your resources.

**Legacy tokens** were the original personal access tokens that granted broad access (either full read/write or read-only) to all team resources.

**Custom scoped tokens** allow more fine-grained permission control when compared to legacy tokens. You can assign specific scopes (permissions) like creating droplets, reading databases, or updating firewalls to custom scoped tokens, which allows you to grant only the exact access needed.

Migrating to custom scoped tokens is essential for maintaining the security of your DigitalOcean resources.

**Rationale:**

Replacing legacy tokens with custom scoped tokens is important for many reasons, including: Granular Control: Scoped tokens provide fine-grained control over API access. You can tailor the token's permissions to the specific tasks it needs to perform. Token Management: Scoped tokens are easier to manage and revoke if they are compromised or no longer needed. Improved Security: By limiting token permissions to only what is necessary, scoped tokens reduce the risk and impact of token compromise. If a scoped token is compromised, the attacker's capabilities are confined to the token's limited scope, unlike legacy tokens which could allow full access.

**Impact:**

Applications or integrations built assuming legacy tokens' broad access might require significant updates to work with scoped tokens, causing temporary disruptions or additional development effort during migration.

Transitioning from legacy to scoped tokens requires updating all systems, scripts, and integrations that use the legacy tokens.

**Audit:**

1. Log in to your **Control Panel**.
2. Navigate to `API` in the lower left hand corner

3. Locate the `Tokens` tab.
4. Review your tokens. If a token has no scopes or only broad read/write access and was created before March 31, 2023, it is a legacy token.
5. Tokens with detailed scopes (e.g. **droplet:create**, **firewall:update**) are scoped tokens.

**Remediation:**

This process requires knowledge of any associated scripts, services, or applications that use the legacy token.

1. Log in to your **Control Panel**.
2. Navigate to `API` in the lower left hand corner.
3. Locate the `Tokens` tab.
4. Review your tokens. If a token has no scopes or only broad read/write access and was created before March 31, 2023, it is a legacy token.
5. Select `Generate New Token` and follow the guidance in our **How to Create a Personal Access Token** documentation.
6. Apply the new scoped token to the scripts and applications to which the legacy token was applied.
7. Once the scoped token has been applied, delete the legacy token.

**References:**

1. https://cloud.digitalocean.com/login
2. https://docs.digitalocean.com/reference/api/create-personal-access-token/#creating-a-token

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 0.0 Explicitly Not Mapped<br>Explicitly Not Mapped | | | |

## *3.2 Ensure Access Tokens Do Not Have Over-Provisioned Scopes (Manual)*

**Profile Applicability:**

- Level 1

**Description:**

**Over-provisioned scoped tokens** are personal access tokens that have been granted permissions in excess of what is needed for their intended use. Over-provisioned scoped tokens not only allow broader access than is necessary; but, broadens the organization’s risk footprint unnecessarily.

**Rationale:**

Checking for over-provisioned scoped tokens is important for many reasons, including:

- **Reduced Attack Surface**: Over-provisioned tokens grant more permissions than needed, creating a larger attack surface. If a token is compromised, the attacker can exploit these excessive permissions to cause greater harm.
- **Better Management and Auditability**: Scoped tokens with only the required permissions are easier to manage, track, and audit, reducing the risk of misuse or accidental changes.
- **Proactive Security**: Regularly reviewing token permissions allows you to identify and correct over-provisioned tokens, strengthening your security posture.

**Impact:**

There are no adverse consequences to checking for over-provisioned scoped tokens.

**Audit:**

This process requires knowledge of internal access controls.

1. Log in to your **Control Panel**.
2. Navigate to `API` then `Tokens`.
3. Select `Scopes` next to the token to be reviewed.
4. Review the scope of your tokens in accordance with your internal access controls.

**Remediation:**

This process requires knowledge of internal access controls.

1. Log in to your **Control Panel**.
2. Navigate to `API` then `Tokens`.

3. Review the scope of your tokens in accordance with your internal access controls.
4. If a token's scope is not in accordance with your internal access controls, select `Generate New Token`.
5. Create the token in accordance with your internal access controls.
6. Apply the newly generated token to scripts and/or applications associated with the out of scope token.
7. Delete the out of scope token.

**References:**

1. https://cloud.digitalocean.com/login

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts<br>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account. | ● | ● | ● |
| v8 | 6.8 Define and Maintain Role-Based Access Control<br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. | | | ● |

## *3.3 Ensure OAuth and Authorized Third-Party Applications are Appropriate (Automated)*

**Profile Applicability:**

- Level 1

**Description:**

OAuth 2 is an open standard for authorization that enables third-party applications to obtain limited access to DigitalOcean users accounts without requiring the user to share their credentials with the third-party application.

Reviewing OAuth applications for appropriateness involves evaluating whether an application's use of OAuth aligns with security policies. This process aims to ensure that only trustworthy applications are granted access to sensitive user or organizational data.

**Rationale:**

Reviewing OAuth applications for appropriateness is important for many reasons, including:

- **Preventing Unauthorized Access**: OAuth tokens can grant third-party applications access to sensitive data, including user accounts and customer data. If an untrusted or malicious app is authorized, the application could access, misuse, or leak sensitive information.
- **Limiting Scope and Permissions**: Reviewing third-party applications' permissions ensures that each application only receives the permissions necessary to perform their function. Overly broad permissions increase the organization's risk footprint as, if compromised, the third-party application could have unauthorized access to sensitive information.

**Impact:**

There are no adverse consequences to reviewing OAuth applications for appropriateness.

**Audit:**

1. Log in to your **Control Panel**.
2. Select `API` and click the `OAuth Applications` tab. Here, you will find a list of third-party applications allowed to interact with the DigitalOcean API on your users' behalf.
3. Select the `Authorized Applications` tab to review which applications have been granted access to your account.

**Remediation:**

1. Log in to your **Control Panel**.
2. Select `API` and click the `OAuth` tab.
3. Delete the OAuth applications you no longer use or cannot identify.
4. Select `API` and click the `Authorized Applications` tab.
5. Delete the OAuth applications you no longer use or cannot identify.

**References:**

1. https://cloud.digitalocean.com/login

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 2.2 Ensure Authorized Software is Currently Supported<br>Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently. | ● | ● | ● |
| v7 | 2.6 Address unapproved software<br>Ensure that unauthorized software is either removed or the inventory is updated in a timely manner | ● | ● | ● |

# 4 Principle of Least Privilege

This section contains recommendations for configuring Principle of Least Privilege (PoLP) on DigitalOcean for improved security.

## *4.1 Ensure Role-Based Access Controls are Implemented (Manual)*

**Profile Applicability:**

- Level 1

**Description:**

Role-Based Access Control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an organization. It involves assigning permissions to specific roles, rather than directly to individual users, and then assigning individual users to those specific roles. In doing so, the organization creates a layer of abstraction between users and permissions, making it easier to manage access rights across the organization.

The simplification of management access rights is achieved by grouping similar users together and defining what actions they can perform on specific resources. RBAC allows organizations to enforce security policies more efficiently, reduce administrative work, and ensure users have appropriate access to perform their job functions without excessive privileges.

DigitalOcean supports a customer's ability to enable RBAC by way of six predefined roles innate to all teams. In assigning these roles, customers are able to issue specific permissions at scale in a manner that upholds the principle of least privilege. The following list outlines the predefined roles as well as their affiliated permissions:

- **Owner:** Permits users full access to shared resources, billing information, and team settings.
- **Member:** Permits users full access to shared resources; but, does not allow them to change team settings. This user has no access to billing information.
- **Biller:** Permits the user full access to billing information; but, does not allow them to view team settings or shared resources.
- **Modifier:** Permits users to update; but, does not allow them to delete resources. This role is ideal for teams who wish to protect sensitive resources from deletion while still allowing members to manage them.
- **Billing viewer:** Permits read-only access to billing information only, giving users insight into billing details for cost analysis, transparency, and governance without exposing sensitive operational controls.
- **Resource viewer:** Permits read-only access to resources, ideal for audit or compliance purposes. Users with this role will not have permission to create, update, or delete resources.

**Rationale:**

Implementing RBAC is important for many reasons, including:

- **Better security:** RBAC reduces the risk of unauthorized access to sensitive data and systems. By assigning permissions based on roles rather than individuals, it ensures that users only have access to the resources necessary for their jobs.
- **Simplified administration:** Managing user access is more streamlined with RBAC. Instead of adjusting permissions for each user individually, administrators can assign or modify roles, saving time and reducing the likelihood of errors.
- **Improved compliance:** RBAC helps organizations meet regulatory requirements by providing clear audit trails and access controls, which aids in compliance reporting.

**Impact:**

Implementing RBAC can have several negative effects and challenges, especially as organizations grow and their access control needs become more complex. If permissions are too restrictive, users may be unable to perform necessary tasks efficiently, leading to unauthorized workarounds or requests for elevated access that can cause delays.

Without routine RBAC access reviews, users may accumulate permissions which exceed their needs. While RBAC aims to prevent this, the circumstance is difficult to avoid without automation.

**Audit:**

1. Log in to the **Control Panel**.
2. Verify you're working with the correct team by selecting the Profile icon in the top right and opening the drop-down menu. If you are not working with the correct team, click `Switch Teams` and select the team you'd like to audit
3. In the bottom left, click `Settings` to go to the **Team Settings** page. Find the list of the team's current membership in the Team Members section.
4. Review the `Membership List` for accuracy.
5. Review the `Role` affiliated with each `Team Member` for appropriateness and accuracy.
6. Review the `Status` affiliated with each `Team Member` to identify users who have not accepted their invitation to join the team.

Everyone on a team can view the membership table, which lists the entire team's current **roles** and the status of their invitations to the Team, which is either "Joined" or "Pending."

**Remediation:**

## Inviting New Members

If an Owner needs to invite additional team members to a team, they can do so through the following steps:

1. From the `Team Settings` page, click the `Invite Members` button to go to the `Invite Team Members` page.
2. Enter the email addresses of the team members you want to invite
3. Choose the role you want each new team member to have when they join the team
4. Optionally; but, as a best practice, require secure sign-in if it isn't already enabled for your Team

## Follow Up with Existing Members who haven't Joined the Team

When someone has not accepted their invitation to the team, the Status column lists them as "Pending." The (…) menu on the far right for pending team members has two options:

- **Resend email:** Sends the invitation to join the team again.
- **Cancel invite:** Revokes the invitation to join the team.

## Change Team Members' Roles

If a team member is assigned a role no longer congruent with their needs, the role should be changed through the following steps:

1. From the `Team Settings` page, locate the team members' name in the Membership table and select the (...) at the far right.
2. Select `Change Role`.

Select the role which matches the team members' needs.

When an Owner changes someone else's role to Owner, the original owner receives an email with a link to confirm the change. After the original Owner confirms the change, the invited Owner receives an email invitation to accept the new role.

## Remove Team Members

If an Owner needs to remove a team member from the team or the team member wishes to leave the team, the following steps should be followed:

1. From the `Team Settings` page, locate the team members' name in the Membership table and select the (...) at the far right
2. `Owners:` Select `Remove from team`
3. `Team members:` Select `Leave team`

**Default Value:**

When a team is created, the person who created the team is defaulted into the Owner role. This role cannot be changed until at least one additional person joins the team.

**References:**

1. https://cloud.digitalocean.com/
2. https://cloud.digitalocean.com/account/team
3. https://docs.digitalocean.com/platform/teams/how-to/manage-membership/#team-roles

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 6.8 Define and Maintain Role-Based Access Control<br>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently. | | | ● |
| v7 | 14.6 Protect Information through Access Control Lists<br>Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. | ● | ● | ● |

# 5 Security History

This section contains recommendations for using DigitalOcean's Security History for improved security.

## *5.1 Ensure Security History is Reviewed Regularly (Manual)*

**Profile Applicability:**

- Level 1

**Description:**

Your team's security history shows a record of actions that have been taken by team members within your Team (e.g.,Creating resources, deleting resources, amending API tokens, etc). Specifically, the history includes the action, the user who performed the action, the originating IP address, and how long ago the action happened.

If you need data older than what is available in your security history, open a Support ticket. For account activity, like logging in or joining a team, view your account's Activity tab.

**Rationale:**

Review the security history for your Team is important for many reasons, including:

- **Maintaining accountability:** Security history tracks when changes were made as well as the individual who orchestrated the change. This information is essential in troubleshooting.
- **Detect unauthorized actions:** Provided the security history is a log of account activity, team owners can identify actions taken by team members unauthorized to perform said action or unauthorized third parties with ease.

**Impact:**

There are no adverse consequences to reviewing security history.

**Audit:**

You can view a Team's security history in the Control Panel.

1. Log in to the Control Panel.
2. In the left menu, click `Settings`.
3. Click the `Security` tab to go to the Team security page.

**Remediation:**

Security History is a native feature to the DigitalOcean Control Panel; there is no remediation procedures.

**References:**

1. https://cloud.digitalocean.com/account/activity
2. https://cloud.digitalocean.com/account/security

**CIS Controls:**

| Controls Version | Control | IG 1 | IG 2 | IG 3 |
|---|---|---|---|---|
| v8 | 8.11 Conduct Audit Log Reviews<br>Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis. |  | ● | ● |
| v7 | 6.7 Regularly Review Logs<br>On a regular basis, review logs to identify anomalies or abnormal events. |  | ● | ● |

# Appendix: Summary Table

| CIS Benchmark Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| **1** | **Introduction** | | |
| **1.1** | **CIS DigitalOcean Foundations Benchmarks** | | |
| **1.2** | **CIS DigitalOcean Services Benchmarks** | | |
| **2** | **Account Access** | | |
| 2.1 | Ensure Secure Sign In for Teams is Enabled (Manual) | □ | □ |
| 2.2 | Ensure Two Factor Authentication for all Accounts/ Teams is Enabled (Manual) | □ | □ |
| 2.3 | Ensure SSH Keys are Audited (Automated) | □ | □ |
| 2.4 | Ensure a Distribution List is used as the Team Contact Email (Manual) | □ | □ |
| **3** | **API** | | |
| 3.1 | Ensure Legacy Tokens are Replaced with Scoped Tokens (Manual) | □ | □ |
| 3.2 | Ensure Access Tokens Do Not Have Over-Provisioned Scopes (Manual) | □ | □ |
| 3.3 | Ensure OAuth and Authorized Third-Party Applications are Appropriate (Automated) | □ | □ |
| **4** | **Principle of Least Privilege** | | |
| 4.1 | Ensure Role-Based Access Controls are Implemented (Manual) | □ | □ |
| **5** | **Security History** | | |
| 5.1 | Ensure Security History is Reviewed Regularly (Manual) | □ | □ |

# Appendix: CIS Controls v7 IG 1 Mapped Recommendations

| Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 3.3 | Ensure OAuth and Authorized Third-Party Applications are Appropriate | □ | □ |
| 4.1 | Ensure Role-Based Access Controls are Implemented | □ | □ |

# Appendix: CIS Controls v7 IG 2 Mapped Recommendations

| Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 3.3 | Ensure OAuth and Authorized Third-Party Applications are Appropriate | □ | □ |
| 4.1 | Ensure Role-Based Access Controls are Implemented | □ | □ |
| 5.1 | Ensure Security History is Reviewed Regularly | □ | □ |

# Appendix: CIS Controls v7 IG 3 Mapped Recommendations

| Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 3.3 | Ensure OAuth and Authorized Third-Party Applications are Appropriate | □ | □ |
| 4.1 | Ensure Role-Based Access Controls are Implemented | □ | □ |
| 5.1 | Ensure Security History is Reviewed Regularly | □ | □ |

# Appendix: CIS Controls v7 Unmapped Recommendations

| Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 2.1 | Ensure Secure Sign In for Teams is Enabled | □ | □ |
| 2.2 | Ensure Two Factor Authentication for all Accounts/ Teams is Enabled | □ | □ |
| 2.3 | Ensure SSH Keys are Audited | □ | □ |
| 2.4 | Ensure a Distribution List is used as the Team Contact Email | □ | □ |
| 3.1 | Ensure Legacy Tokens are Replaced with Scoped Tokens | □ | □ |
| 3.2 | Ensure Access Tokens Do Not Have Over-Provisioned Scopes | □ | □ |

# Appendix: CIS Controls v8 IG 1 Mapped Recommendations

| Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 2.2 | Ensure Two Factor Authentication for all Accounts/ Teams is Enabled | □ | □ |
| 2.3 | Ensure SSH Keys are Audited | □ | □ |
| 2.4 | Ensure a Distribution List is used as the Team Contact Email | □ | □ |
| 3.2 | Ensure Access Tokens Do Not Have Over-Provisioned Scopes | □ | □ |
| 3.3 | Ensure OAuth and Authorized Third-Party Applications are Appropriate | □ | □ |

# Appendix: CIS Controls v8 IG 2 Mapped Recommendations

| Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 2.1 | Ensure Secure Sign In for Teams is Enabled | □ | □ |
| 2.2 | Ensure Two Factor Authentication for all Accounts/ Teams is Enabled | □ | □ |
| 2.3 | Ensure SSH Keys are Audited | □ | □ |
| 2.4 | Ensure a Distribution List is used as the Team Contact Email | □ | □ |
| 3.2 | Ensure Access Tokens Do Not Have Over-Provisioned Scopes | □ | □ |
| 3.3 | Ensure OAuth and Authorized Third-Party Applications are Appropriate | □ | □ |
| 5.1 | Ensure Security History is Reviewed Regularly | □ | □ |

# Appendix: CIS Controls v8 IG 3 Mapped Recommendations

| Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| 2.1 | Ensure Secure Sign In for Teams is Enabled | □ | □ |
| 2.2 | Ensure Two Factor Authentication for all Accounts/ Teams is Enabled | □ | □ |
| 2.3 | Ensure SSH Keys are Audited | □ | □ |
| 2.4 | Ensure a Distribution List is used as the Team Contact Email | □ | □ |
| 3.2 | Ensure Access Tokens Do Not Have Over-Provisioned Scopes | □ | □ |
| 3.3 | Ensure OAuth and Authorized Third-Party Applications are Appropriate | □ | □ |
| 4.1 | Ensure Role-Based Access Controls are Implemented | □ | □ |
| 5.1 | Ensure Security History is Reviewed Regularly | □ | □ |

# Appendix: CIS Controls v8 Unmapped Recommendations

| Recommendation | | Set Correctly | |
|---|---|---|---|
| | | Yes | No |
| | No unmapped recommendations to CIS Controls v8 | □ | □ |

# Appendix: Change History

| Date | Version | Changes for this version |
|---|---|---|
| Jul 29, 2025 | 1.0.0 | Document Created |