NIC

EMPOWER

November 13-15, Oslo Spektrum

Martin Ehrnst

GitHub a toolkit for platform engineers

NIC
EMPOWER

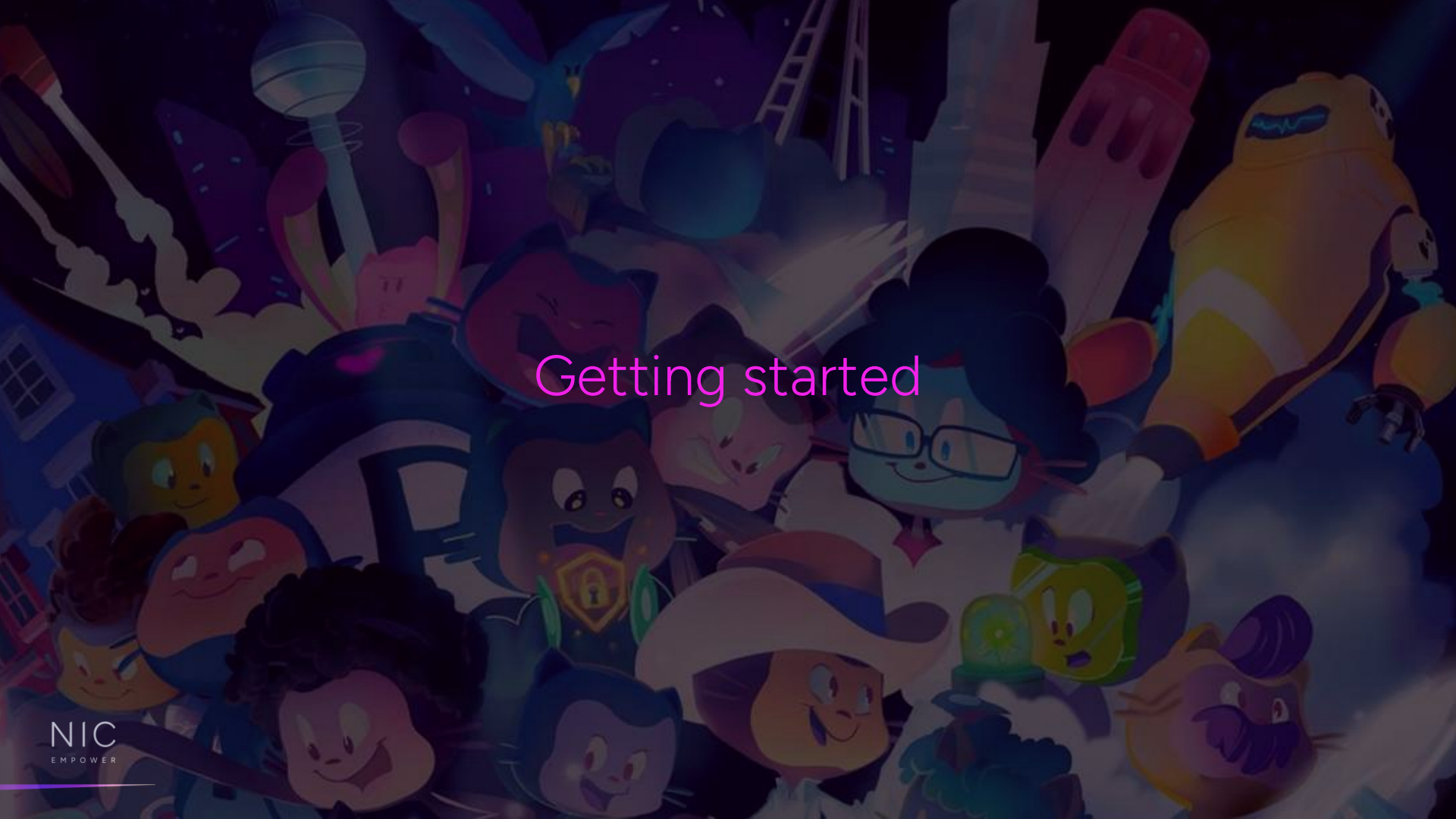
Simplifai

NIC
EMPOWER

Simplifai

The menu

- Day 0 getting started
- Security settings
- Shared Workflows
- Runners
- Self-service



Getting started

NIC
EMPOWER

GitHub Enterprise

NIC
EMPOWER

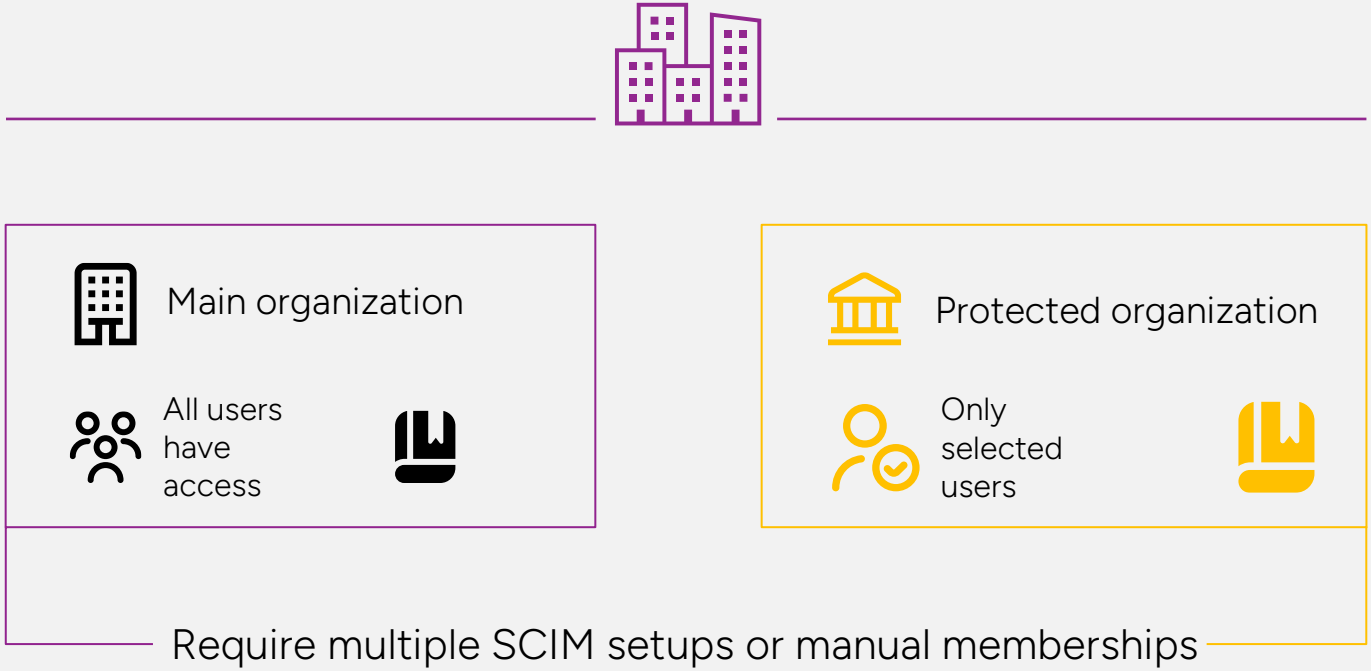
Main organization

All users have access

Protected organization

Only selected users

NIC
EMPOWER


Main organization
All users have access
Protected organization
Only selected users
Require multiple SCIM setups or manual memberships

NIC
EMPOWER

Type / to search

Try Enterprise free for 30 days

How do you want to manage users on your enterprise?

Your enterprise type determines whether members can contribute to public repositories in addition to private company ones, and how members are given access to your enterprise.

Enterprise with personal accounts

Best if your company does public, open source and private work or if you have an existing organization. Members can use their personal GitHub accounts.

- Members can use their own GitHub accounts for work within your enterprise. SAML SSO authentication can be enforced.
- Your enterprise can publish public repositories and members can work seamlessly between public and private company repositories.

Continue

Learn more about Enterprise Cloud

Enterprise with managed users

Best if your company only does private, internal work and needs member accounts to be provisioned from your identity provider.

- Your enterprise, its members, and its repositories cannot be discovered or shared publicly.
- Member accounts are provisioned and authenticated via your company's identity provider.

Continue

Learn more about Enterprise Managed Users

Need more information? Contact your partner or seller.
If you don't have a partner or seller and would like to get in contact with one, contact sales.

Try Enterprise free for 30 days

How do you want to manage users on your enterprise?

Your enterprise type determines whether members can contribute to public repositories in addition to private company ones, and how members are given access to your enterprise.

Enterprise with personal accounts

Best if your company does public, open source and private work or if you have an existing organization. Members can use their personal GitHub accounts.

- Members can use their own GitHub accounts for work within your enterprise. SAML SSO authentication can be enforced.
- Your enterprise can publish public repositories and members can work seamlessly [illegible] public and private company repositories.

Continue

Learn more about Enterprise Cloud

Enterprise with managed users

Best if your company only does private, internal work and needs member accounts to be provisioned from your identity provider.

- Your enterprise, its members, and its repositories cannot be discovered or shared publicly.
- Member accounts are provisioned and authenticated via your company's identity provider.

Learn more about Enterprise Managed Users

Need more information? Contact your partner or seller.

If you don't have a partner or seller and would like to get in contact with one, contact sales.

About Enterprise Managed Users

Learn how your enterprise can manage the lifecycle and authentication of users on GitHub from your identity provider (IdP).

With Enterprise Managed Users, you manage the lifecycle and authentication of your users on GitHub from an external identity management system, or IdP:

- Your IdP **provisions new user accounts** on GitHub, with access to your enterprise.
- Users must **authenticate on your IdP** to access your enterprise's resources on GitHub.
- You control **usernames, profile data, organization membership, and repository access** from your IdP.
- If your enterprise uses OIDC SSO, GitHub will validate access to your enterprise and its resources using your IdP's **Conditional Access Policy (CAP)**. See "About support for your IdP's Conditional Access Policy."
- Managed user accounts **cannot create public content** or collaborate outside your enterprise. See "Abilities and restrictions of managed user accounts."

> **Note**
>
> Enterprise Managed Users is not the best solution for every customer. To determine whether it's right for your enterprise, see "Choosing an enterprise type for GitHub Enterprise Cloud."

Identity management systems

GitHub partners with some developers of identity management systems to provide a "paved-path" integration with Enterprise Managed Users. To simplify your configuration and ensure full support, **use a single partner IdP for both authentication and provisioning.**

Partner identity providers

Partner IdPs provide authentication using SAML or OIDC, and provide provisioning with System for Cross-domain Identity Management (SCIM).

Partner IdP	SAML	OIDC	SCIM
Entra ID	✓	✓	✓
Okta	✓	✗	✓
PingFederate	✓	✗	✓

When you use a single partner IdP for both authentication and provisioning, GitHub provides support for the application on the partner IdP and the IdP's integration with GitHub.

Other identity management systems

If you cannot use a single partner IdP for both authentication and provisioning, you can use another identity management system or combination of systems. The system must:

- Adhere to **GitHub's integration guidelines**
- Provide **authentication using SAML**, adhering to SAML 2.0 specification
- Provide **user lifecycle management using SCIM**, adhering to the SCIM 2.0 specification and communicating with GitHub's REST API (see "Provisioning users and groups with SCIM using the REST API")

GitHub does not expressly support mixing and matching partner IdPs for authentication and provisioning and does not test all identity management systems. **GitHub's support team may not be able to assist you with issues related to mixed or untested systems.** If you need help, you must

Abilities and restrictions of managed user accounts

Learn what users can and cannot do if you manage accounts from an identity provider (IdP).

With Enterprise Managed Users, you can control the user accounts of your enterprise members through your identity provider (IdP). See "About Enterprise Managed Users."

Managed user accounts can contribute only to private and internal repositories within their enterprise and their own private repositories. They have read-only access to the wider GitHub community. These visibility and access restrictions apply to all requests, including API requests.

Authentication

- Managed user accounts authenticate using only your identity provider, and have no password or two-factor authentication methods stored on GitHub. As a result, they do not see the sudo prompt when taking sensitive actions.

GitHub Actions

- Managed user accounts cannot create workflow templates for GitHub Actions.
- Entitlement minutes for GitHub-hosted runners are not available for managed user accounts.
- Enterprise Managed Users can trigger workflows in organizations where they are not members by forking the organization repository, then creating a pull request targeting the organization repository.

GitHub Apps

Managed user accounts:

- Cannot install GitHub Apps on their user accounts, unless the app is an internal app. See "Internal GitHub Apps."
- Can install GitHub Apps on a repository if the app doesn't request organization permissions and if the managed user account has admin access to the repository.

Abilities and restrictions of managed user accounts

GitHub Pages

- Managed user accounts are limited in their use of GitHub Pages. See "About GitHub Pages."

Interactions

- Managed user accounts can view all public repositories, but cannot interact with repositories outside of the enterprise in any of the following ways:
  - Push code to the repository
  - Create issues or pull requests within the repository
  - Create or comment on discussions within the repository
  - Comment on issues or pull requests, or add reactions to comments
  - Star, watch, or fork the repository
- Managed user accounts cannot follow users outside of the enterprise.

Repository management

repository.

GitHub Apps

Managed user accounts:

- Cannot install GitHub Apps on their user accounts, unless the app is an internal app. See "Internal GitHub Apps."
- Can install GitHub Apps on a repository if the app doesn't request organization permissions and if the managed user account has admin access to the repository.

GitHub Enterprise Cloud - Enterprise ehrnst | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating GitHub Enterprise Cloud - Enterprise ehrnst.

1 Basic SAML Configuration

Edit

Identifier (Entity ID)	https://github.com/enterprises/ehrnst
Reply URL (Assertion Consumer Service URL)	https://github.com/enterprises/ehrnst/saml/consume
Sign on URL	https://github.com/enterprises/ehrnst/sso
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*

2 Attributes & Claims

Edit

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

3 SAML Certificates

Token signing certificate

Edit

Status	Active
Thumbprint	[redacted]
Expiration	10/13/2027, 6:13:46 PM
Notification Email	martin@ehrnst.no
App Federation Metadata Url	https://login.microsoftonline.com/e5806cb5-f8f4-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional)

Edit

Required	No
Active	0
Expired	0

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot | martin@ehrnst.no EHRNST (EHRNST.NO)

Home > Enterprise applications | All applications > GitHub Enterprise Cloud - Enterprise ehrnst

GitHub Enterprise Cloud - Enterprise ehrnst | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Manage claim

Save | Discard changes | Got feedback?

Name: nameidentifier

Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Name identifier format *: Email address

Source *: Attribute / Transformation / Directory schema extension

Source attribute *: user.mail

Claim conditions

Advanced SAML claims options

App Federation Metadata Url	https://login.microsoftonline.com/e5806cb5-f8f4-...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

Verification certificates (optional) — Edit

Required	No
Active	0
Expired	0

NIC EMPOWER

Save SAML settings

Team synchronization

Team synchronization lets you manage team membership through your configured identity provider. Learn more.

Enable for Entra ID

SSH certificate authorities

New certificate authority

There are no SSH certificate authorities associated with this enterprise.

IP allow list

An IP allow list lets your enterprise limit access based on the IP address a person is accessing from. Learn more about enforcing policies for security settings.

☐ **Enable IP allow list**
Enabling will allow you to restrict access by IP address to resources owned by this enterprise.

Save

☐ **Enable IP allow list configuration for installed GitHub Apps**

Microsoft

martin@ehrnst.no

Permissions requested

Review for your organization

GitHub team synchronization
microsoft.github.com

This application is not published by Microsoft or your organization.

This app would like to:

- Read all group memberships
- Read all users' full profiles
- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Does this app look suspicious? Report it here

Cancel | Accept

NIC
EMPOWER

Your SAML provider is using the RSA-SHA256 **Signature Method** and the SHA256 **Digest Method**.

The assertion consumer service URL is https://github.com/enterprises/ehrnst/saml/consume

Test SAML configuration

You need to test your SAML configuration before saving.

Save SAML settings

Team synchronization

Team synchronization lets you manage team membership through your configured identity provider. Learn more.

Review pending request

Your team synchronization setup is pending review and approval.

SSH certificate authorities

New certificate authority

There are no SSH certificate authorities associated with this enterprise.

IP allow list

An IP allow list lets your enterprise limit access based on the IP address a person is accessing from. Learn more about enforcing policies for security settings.

- [ ] **Enable IP allow list**

ehrnst-enterprises
Demo enterprise

Overview
Organizations
People
Policies
Code Security
Billing & Licensing

Overview
Usage
Cost centers
Budgets and alerts
Licensing
Payment information
Payment history
Billing contacts
Marketplace apps
Sponsorships

Settings
Compliance

Payment Information

Manage billing for this account through Microsoft Azure. To enable usage beyond included allotments and manage spending limits, an Azure Subscription ID must be added to your account. Learn more about Azure subscriptions

Azure subscription

MVP-Sponsorship

[redacted]

Security settings

NIC
EMPOWER

Settings

Demo org
Organization, part of ehrnst-enterpris... Switch settings context

Go to your organization profile

General

Access
- Billing and plans
- Organization roles
- Repository roles
- Member privileges
- Import/Export
- Moderation

Code, planning, and automation
- Repository
- Codespaces
- Planning
- Copilot
- Actions
- Webhooks
- Discussions
- Packages
- Pages
- Hosted compute networking

Security
- Authentication security
- Deploy keys
- Code security
- Compliance
- Verified and approved domains
- Secrets and variables

Third-party Access
- GitHub Apps
- OAuth app policy
- Personal access tokens

Member privileges

Base permissions

Base permissions to the organization's repositories apply to all members and excludes outside collaborators. Since organization members can have permissions from multiple sources, members and collaborators who have been granted a higher level of access than the base permissions will retain their higher permission privileges.

Read

Repository creation

Members will be able to create only selected repository types. Outside collaborators can never create repositories.

- [ ] **Public**
  Members will be able to create public repositories, visible to anyone.
- [x] **Private**
  Members will be able to create private repositories, visible to organization members with permission.
- [x] **Internal**
  Members will be able to create internal repositories, visible to all enterprise members.

Save This setting has been set by enterprise administrators.

Repository forking

- [ ] **Allow forking of private and internal repositories**
  If enabled, forking is allowed on private, internal, and public repositories. If disabled, forking is only allowed on public repositories. This setting is also configurable per-repository.

Save

Outside collaborators

- [ ] **Allow repository administrators to invite outside collaborators to repositories for this organization**
  If disabled, only organization owners may invite collaborators to repositories. Learn more about managing permissions for outside collaborators.

Save

Repository comments

- [x] **Allow members to see comment author's profile name in private repositories**
  If enabled, members will be able to see comment author's profile name in issues and pull requests for private repositories.

Save

NIC
EMPOWER

Settings

Demo org

Organization, part of ehrnst-enterpris... Switch settings context

Go to your organization profile

- General

Access

- Billing and plans
- Organization roles
- Repository roles
- Member privileges
- Import/Export
- Moderation

Code, planning, and automation

- Repository
  - General
  - Topics
  - Rulesets
  - Rule insights
  - Bypass requests Preview
  - Custom properties
- Codespaces
- Planning
- Copilot
- Actions
- Webhooks
- Discussions

Rulesets

New ruleset

protect_main

3 branch rules • targeting 9 repositories

NIC EMPOWER

Settings

Demo org
Organization, part of ehrnst-enterpris... Switch settings context

Go to your organization profile

General

Access
- Billing and plans
- Organization roles
- Repository roles
- Member privileges
- Import/Export
- Moderation

Code, planning, and automation
- Repository
  - General
  - Topics
  - Rulesets
  - Rule insights
  - Bypass requests Preview
  - Custom properties
- Codespaces
- Planning
- Copilot
- Actions
- Webhooks
- Discussions
- Packages
- Pages
- Hosted compute networking

Security
- Authentication security
- Deploy keys
- Code security
- Compliance
- Verified and approved domains
- Secrets and variables

Third-party Access
- GitHub Apps
- OAuth app policy
- Personal access tokens

Rulesets / protect_main Active

Ruleset Name

protect_main

Enforcement status

Active

Bypass list

Add bypass

Exempt roles or teams from this ruleset by adding them to the bypass list.

Repository admin	Role	Allow for pull requests only
Enterprise owners	Role	Always allow

Targets

Which repositories and branches do you want to make a ruleset for?

Target repositories

Repository targeting determines which repositories will be protected by this ruleset. Use inclusion patterns to expand the list of repositories under this ruleset. Use exclusion patterns to exclude repositories.

Target: All repositories

Target branches

Branch targeting determines which branches will be protected by this ruleset. Use inclusion patterns to expand the list of branches under this ruleset. Use exclusion patterns to exclude branches.

Branch targeting criteria — Add target

Default

Rules

Which rules should be applied?

Branch rules

- [ ] **Restrict creations**
  Only allow users with bypass permission to create matching refs.
- [ ] **Restrict updates**
  Only allow users with bypass permission to update matching refs.

NIC
EMPOWER

Settings

Demo org
Organization, part of ehrnst-enterpris... Switch settings context

Go to your organization profile

General

Access
Billing and plans
Organization roles
Repository roles
Member privileges
Import/Export
Moderation

Code, planning, and automation
Repository
General
Topics
Rulesets
Rule insights
Bypass requests Preview
Custom properties
Codespaces
Planning
Copilot
Actions
Webhooks
Discussions
Packages
Pages
Hosted compute networking

Security
Authentication security
Deploy keys
Code security
Compliance
Verified and approved domains
Secrets and variables

Third-party Access
GitHub Apps
OAuth app policy
Personal access tokens

Rulesets / protect_main Active

Ruleset Name
protect_main

Enforcement status
Active

Bypass list

Add bypass

Exempt roles or teams from this ruleset by adding them to the bypass list.

Repository admin Role	Allow for pull requests only	···
Enterprise owners Role	Always allow	···

Targets

Which repositories and branches do you want to make a ruleset for?

Target repositories

Repository targeting determines which repositories will be protected by this ruleset. Use inclusion patterns to expand the list of repositories under this ruleset. Use exclusion patterns to exclude repositories.

Target: All repositories

Target branches

Branch targeting determines which branches will be protected by this ruleset. Use inclusion patterns to expand the list of branches under this ruleset. Use exclusion patterns to exclude branches.

Branch targeting criteria — Add target

Default

Rules

Which rules should be applied?

Branch rules

- [ ] Restrict creations
  Only allow users with bypass permission to create matching refs.
- [ ] Restrict updates
  Only allow users with bypass permission to update matching refs.

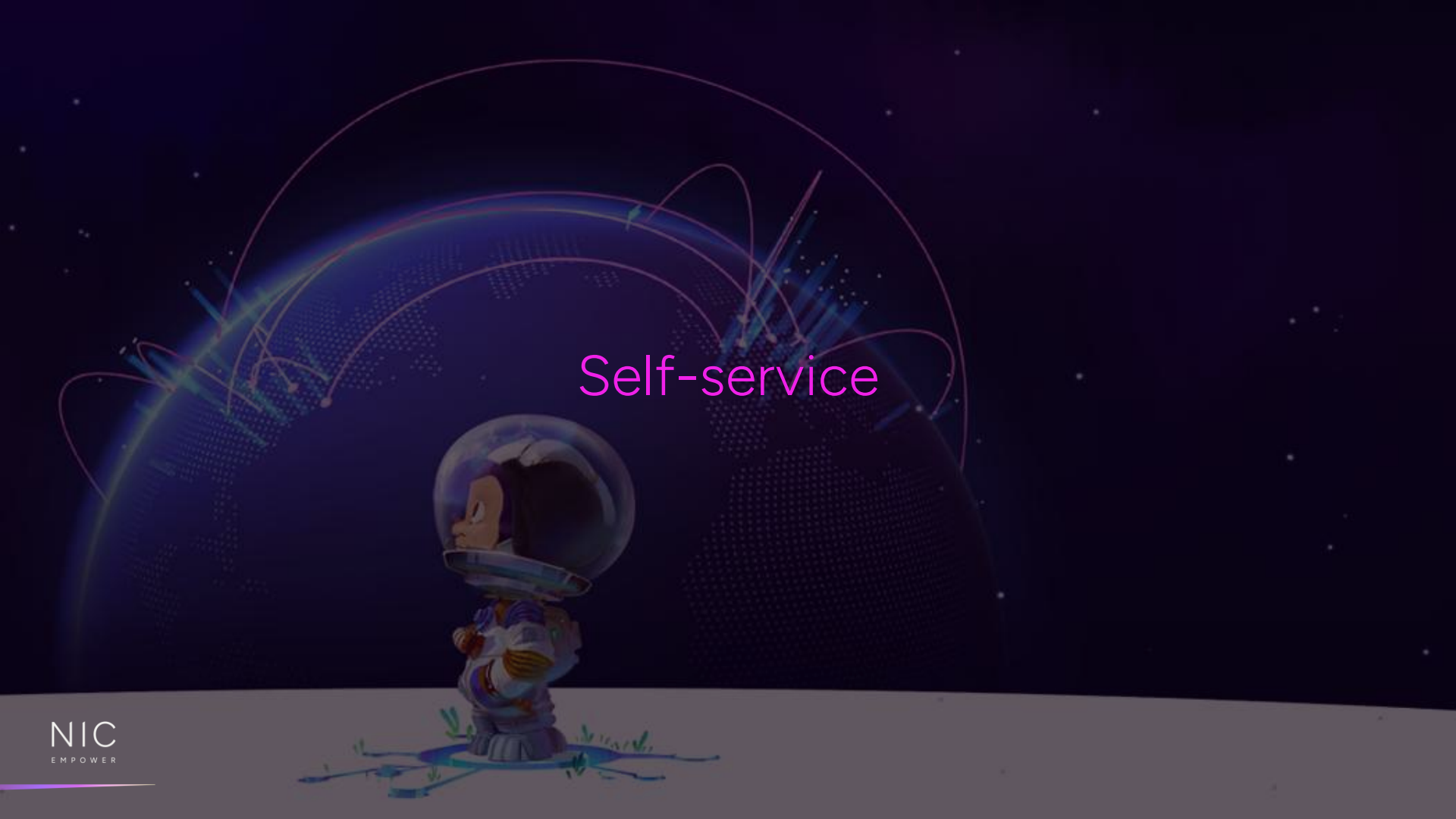
NIC
EMPOWER

Runners

NIC
EMPOWER

Shared Workflows

NIC
EMPOWER


Self-service
NIC
EMPOWER

terraform { Untitled-1

```
terraform {
    required_providers {
        github = {
            source = "integrations/github"
            version = "~> 6.0"
        }
    }
}

provider "github" {
    token = var.github_token
}

resource "github_repository" "example" {
    name = "example"
    description = "This is your first repository"
    visibility = "internal"
    repository_template {
        template_owner = "adatum-inc"
        template_repo = "start-from-template"
    }
}
```

$ # Create a new github repo from a templa Untitled-1

```
# Create a new github repo from a template

gh repo create my-new-repo --template adatum-inc/start-from-template --internal
```

Vipps MobilePay

Search

Catalog

APIs

Docs

Create...

Grafana

Design System

Tech Radar

Test Portal

Linkerd

Settings

DevTools

Create a new component

Create new software components using standard templates in your organization

New GitHub repository

Create a new, internal repository in GitHub. Can optionally add manifests, workflows and identities for deploying VippsService (application) and/or VmJob (batch). Read more in our tech docs.

1 I need some information :) — 2 VippsService/VmJob? — 3 Review

GitHub repository name*

The name of the repository you will create on GitHub/vippsas

Admin team*

Admin team for GitHub repo to be created. This team will also be responsible for reviewing and approving changes to the prod environment.

System*

Choose a sensible system for your component. A system is a collection of one or multiple components, resources, and APIs.

BACK NEXT

Backstage

NIC
EMPOWER

Vipps MobilePay

Search

Catalog

APIs

Docs

Create...

Grafana

Design System

Tech Radar

Test Portal

Linkerd

Settings

DevTools

Create a new component

Create new software components using standard templates in your organization

New GitHub repository

Create a new, internal repository in GitHub. Can optionally add manifests, workflows and identities for deploying VippsService (application) and/or VmJob (batch). Read more in our tech docs.

1. I need some information :)
2. VippsService/VmJob?
3. Review

☑ Add manifests, workflows and identities to build and deploy your VippsService and/or VmJob?

App name*
test-app
Unique name of the component

Kubernetes namespace*
test-namespace
Provide the namespace where your application will run. This template does NOT create a new namespace.

Docker port*
8080

Internet port*
80

Number of replicas*
3
The number of replicas for your deployments

CPU request per pod*
Set your CPU request (m)

Memory request per pod*
Set your memory request (Mi)

BACK REVIEW

NIC
EMPOWER

Vipps MobilePay

Search

Catalog

APIs

Docs

Create...

Grafana

Design System

Tech Radar

Test Portal

Linkerd

Create a new component

Create new software components using standard templates in your organization

New GitHub repository

Create a new, internal repository in GitHub. Can optionally add manifests, workflows and identities for deploying VippsService (application) and/or VmJob (batch). Read more in our tech docs.

I need some information :) — VippsService/VmJob? — 3 Review

Repo Name	test-repo
Admin Team	group:default/team-test
System	system:default/user-test
Vippsservice Or Vmjob	✅

BACK CREATE

NIC
EMPOWER

Using “only” GitHub

NIC
EMPOWER

README.md > ## Summary

```md
## Summary

- Pay attention to the user in GitHub, and choose the one that fulfill your needs
- Do basic security setup before launch.
    - Ie re-enable SAML will throw everyone out.
- Any solution you make should simplifly daily tasks. Not lock it in.
```

Thanks!

Don’t forget to evaluate

NIC
EMPOWER

Simplifai