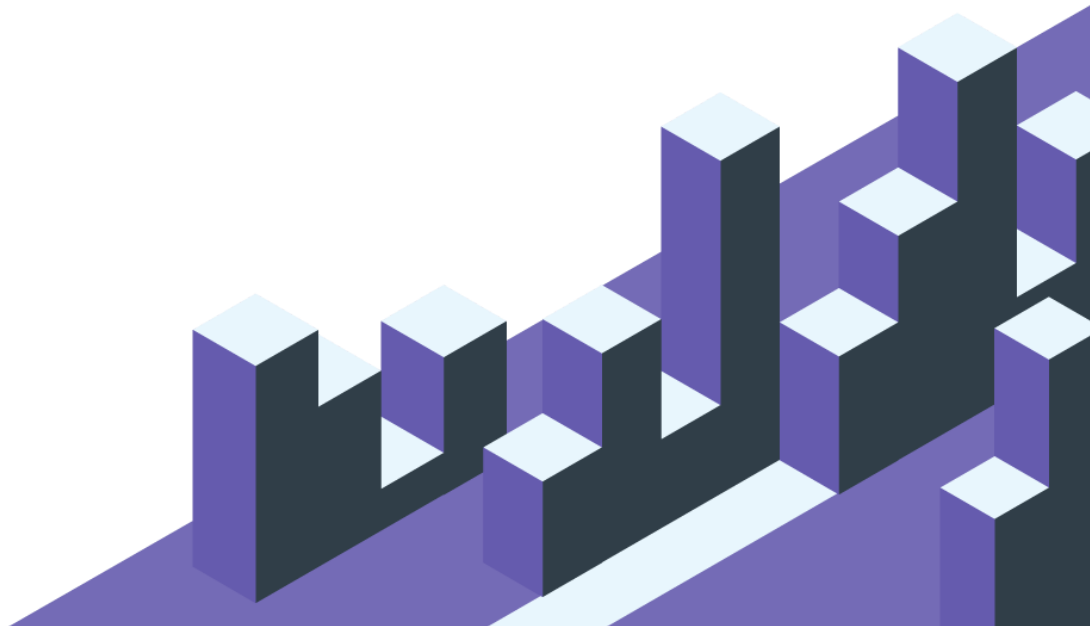


ZenHub

ZenHub Enterprise AWS Installation Guide



ZenHub Enterprise Installation Guide

Thank you for choosing **ZenHub Enterprise**! You are almost ready to start visualizing your GitHub workflow. This short guide below outlines the installation process. Please contact the ZenHub team at any time for assistance.

You will begin by setting up **ZenHub Enterprise** in EC2.

Configure security groups

If you do not already have a preferred security group for your ZenHub Enterprise instance, you will need to create one with the following rules:

Port	Service	Description
80	HTTP	Basic plain-text access if you do not enable HTTPS during setup
443	HTTPS	Encrypted SSL connection to ZenHub Enterprise, required for setup unless disabled
22	SSH	Secure shell access to the ZenHub Enterprise Instance

The security group should be configured such that ZenHub Enterprise can be communicated with on all of the above ports, both by your team (office IP range or 0.0.0.0/0) and by GitHub Enterprise.

Thus, you will need to make **two rules** for each port, such as:

Type	Protocol	Port Range	Source
HTTP	TCP	80	0.0.0.0/0 or Office IP Range
HTTPS	TCP	443	0.0.0.0/0 or Office IP Range
SSH	TCP	22	0.0.0.0/0 or Office IP Range
HTTP	TCP	80	IP of GitHub Enterprise (x.x.x.x/32) or security group that GitHub Enterprise is in
HTTPS	TCP	443	IP of GitHub Enterprise (x.x.x.x/32) or security group that GitHub Enterprise is in

For example, here is our security group:

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
HTTPS	TCP	443	Github and Zenhub Enterprise Security Group [REDACTED] (Enterprise)
SSH	TCP	22	Office IP Range 216.[REDACTED]/32
HTTP	TCP	80	Office IP Range 216.[REDACTED]/32
HTTP	TCP	80	Github and Zenhub Enterprise Security Group [REDACTED] (Enterprise)
HTTPS	TCP	443	Office IP Range 216.[REDACTED]/32

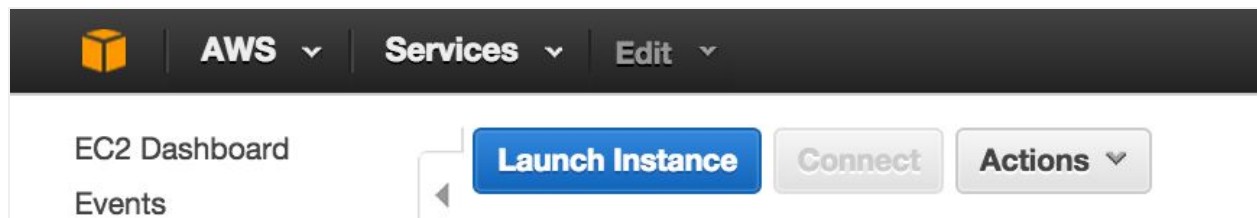
Ensure that both **ZenHub Enterprise** and **GitHub Enterprise** are allowing traffic inbound from one another on **TCP ports 443** and **80**.

Note: If you specified a security group for the previous two rules, you must ensure **GitHub Enterprise** can resolve the DNS for **ZenHub Enterprise** internally (10.x.x.x address).

If ZenHub Enterprise cannot resolve internally, you must whitelist GitHub Enterprise's public IP address.

Select a ZenHub Enterprise AMI for your region

Open the AWS Management console. Select **Instances** from the sub-nav on your left. Then click **Launch Instance**.



Note: ZenHub Enterprise should be launched in the same region and zone as your GitHub Enterprise installation. Refer to the following table for information about which AMI to use:

Region	AMI ID
us-east-1	ami-0bf67ea3d772ebce3
us-east-2	ami-03e6043b79da01e6f
us-west-2	ami-09cc3f8a8e695e549
us-west-1	ami-0f583eb6043c1c742

eu-north-1	ami-0ccd1045f4f4d3356
eu-west-1	ami-07da170f39ad5facf
eu-west-2	ami-04cd357e35fd02e32
eu-west-3	ami-06a8f34d84291850f
eu-central-1	ami-0ec5d2daef260b97b
ap-southeast-1	ami-095befc85f01e1371
ap-southeast-2	ami-00cc5ada8ec74507d
ap-northeast-1	ami-096962faf5fa8f6d1
ap-northeast-2	ami-06b657393ec04128b
ap-south-1	ami-01a44302d25d6252f
sa-east-1	ami-0d35335e686ec307c
ca-central-1	ami-06ae36902a8ac1502

How to find the appropriate ZenHub Enterprise AMI for your region:

Select **My AMIs** (on the left) -> Check on “**Shared with me**” checkbox -> Search “**ZenHub**” -> Click **Select**.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI) [Cancel and Exit](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

My AMIs

AWS Marketplace

Community AMIs

▼ **Ownership**

☒ Owned by me

☒ **Shared with me**

▼ **Architecture**

☐ 32-bit

☐ 64-bit

Q ZenHub

ZenHub Enterprise 1.5 - ami-02f3c56a

ZenHub Enterprise --Version 1.5

Root device type: ebs Virtualization type: hvm Owner: 427746948829

64-bit

Select

Choose instance type

Select your preferred instance type. Then click **Next: Configure Instance Details**.

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Tag Instance
6. Configure Security Group
7. Review

Step 2: Choose an Instance Type

<input type="checkbox"/>	Compute optimized	c4.xlarge	36	60	EBS only	Yes	10 Gigabit
<input type="checkbox"/>	Compute optimized	c3.large	2	3.75	2 x 16 (SSD)	-	Moderate
<input type="checkbox"/>	Compute optimized	c3.xlarge	4	7.5	2 x 40 (SSD)	Yes	Moderate
<input checked="" type="checkbox"/>	Compute optimized	c3.2xlarge	8	15	2 x 80 (SSD)	Yes	High
<input type="checkbox"/>	Compute optimized	c3.4xlarge	16	30	2 x 160 (SSD)	Yes	High
<input type="checkbox"/>	Compute optimized	c3.8xlarge	32	60	2 x 320 (SSD)	-	10 Gigabit
<input type="checkbox"/>	GPU instances	g2.2xlarge	8	15	1 x 60 (SSD)	Yes	High

Cancel
Previous
Review and Launch
Next: Configure Instance Details

Note: ZenHub Enterprise is only supported on the following instance types:

Instance Type	CPU Cores	Memory	Disk
c3.2xlarge **	8	15GB	160GB (SSD)
m3.2xlarge **	8	30GB	850GB
r3.xlarge *	4	30.5GB	80GB (SSD)
m3.xlarge	4	15GB	80GB (SSD)
c3.xlarge	4	7.5GB	80GB (SSD)

* Denotes a recommended instance type

** Denotes a recommended instance type, if you plan on uploading large files

Configure networking for your instance

On the **Configure Instance Details** page, select the network configuration that will allow **ZenHub Enterprise** to communicate with **Github Enterprise** on the same network.

If **Github Enterprise** is in VPC, then select the associated **Network** (VPC), **Subnet**, and ensure **Auto-assign Public IP** is set to **Enable**. Otherwise, select **Launch into EC2 Classic**.

The screenshot shows the 'Configure Instance Details' page with the following settings:

- Network:** vpc-9dacddf5 (172.31.0.0/16) (default) [Create new VPC]
- Subnet:** [No preference (default subnet in any Availability Zone) subnet-9facddf7(172.31.0.0/20) | Default in us-west-1c subnet-90acddf8(172.31.16.0/20) | Default in us-west-1a] [Create new subnet]
- Auto-assign Public IP:** [Enable]
- Placement group:** [No placement group]

Click **Next: Add Storage**

Remove any other volumes except **Root** (if applicable). Ensure **General Purpose (SSD)** is selected under **Volume Type** and that you have at least **30 GB** of storage size:

Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Delete on Termination ⓘ	Encrypted ⓘ
Root	/dev/sda1	snap-c0be3981	30	General Purpose (SSD) [v]	24 / 3000	<input checked="" type="checkbox"/>	Not Encrypted
Add New Volume							

Click **Next: Tag Instance**

Name your instance (example: **ZenHub Enterprise**) for easier identification.

Key (127 characters maximum)	Value (255 characters maximum)
Name	ZenHub Enterprise

Click **Next: Configure Security Group**

Click **Select an existing security group** and find the security group you configured in Step 1, then click **Review and Launch**.

 sg-d9fb5cbc	Enterprise	Github & Zenhub Enterprise
---	------------	----------------------------

Type ⁱ	Protocol ⁱ	Port Range ⁱ	Source ⁱ
HTTPS	TCP	443	Github and Zenhub Enterprise Security Group
SSH	TCP	22	Office IP Range
HTTP	TCP	80	Office IP Range
HTTP	TCP	80	Github and Zenhub Enterprise Security Group
HTTPS	TCP	443	Office IP Range

Launch ZenHub Enterprise

Review the configuration for accuracy. Click **Launch**.

Select **Proceed without a key pair**, click the checkbox, then click **Launch Instances**.

Select an existing key pair or create a new key pair ×

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.


Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

⌵

☒ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

Cancel Launch Instances

Note: The instance may take up to 10 minutes to boot. It is recommended to wait for the instance to boot before proceeding to Step 6.

▼ AMI Details						
 Zenhub Enterprise - ami-04190241 Zenhub Enterprise - Version 1.1.0 Root Device Type: ebs Virtualization type: hvm						
▼ Instance Type						
Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
r3.xlarge	13	4	30.5	1 x 80	Yes	Moderate
▼ Security Groups						
Security Group ID	Name	Description				
sg-d9fb5cbc	Enterprise	Github & Zenhub Enterprise				

[Cancel](#)[Previous](#)[Launch](#)

Optional: Allocate an Elastic IP and associate it with the instance

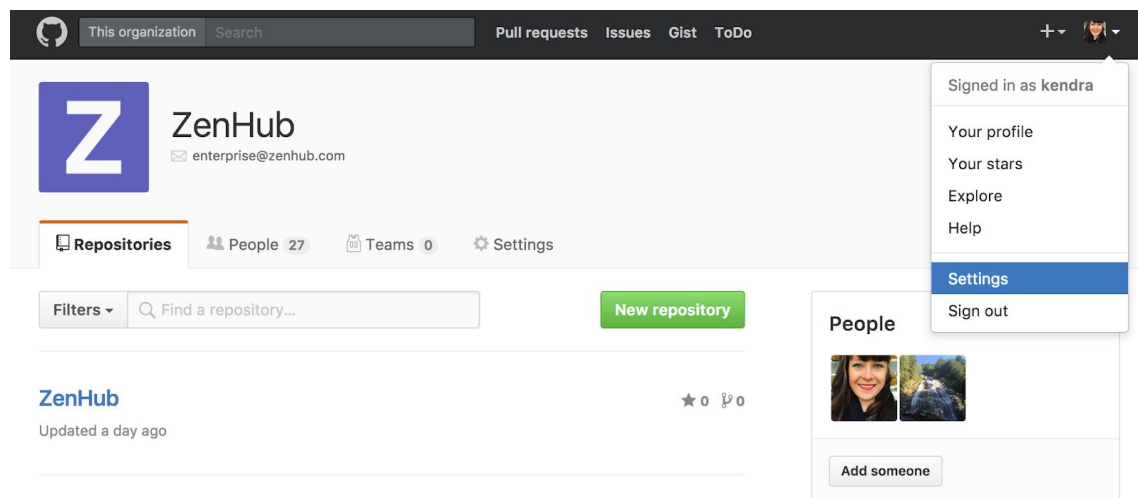
We recommend using an Elastic IP with your instance, which is useful if you wish to move instances, or stop and start your instance. For more, see Amazon's AWS guide [here](#).

Register ZenHub Enterprise on GitHub Enterprise

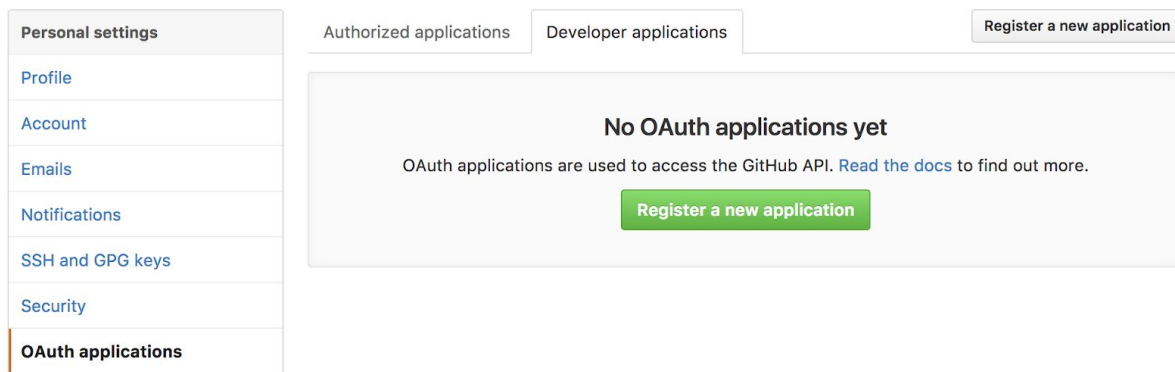
Next, you will configure ZenHub Enterprise on GitHub Enterprise.

ZenHub Enterprise must be registered as an application on GitHub Enterprise. Log in to GitHub Enterprise as a site administrator, and then:

Navigate to the Account Settings page by clicking **Settings**:



On the **Settings** page, select the **OAuth Applications** tab from the sub-navigation bar on your left. Click **Developer Applications**, and finally, select **Register New Application** on the top-right corner.



Fill in the registration form with the following information.

- **Application name:** ZenHub Enterprise
- **Homepage URL:** <https://zenhub.com>
- **Application description:** (optional)
- **Authorization callback URL:** <https://> + [Your ZenHub Enterprise address] + /auth/github/callback.

For example, if your ZenHub Enterprise IP address is **192.168.10.7**, then the authorization callback URL becomes **<https://192.168.10.7/auth/github/callback>**.

Personal settings

Profile

Account

Emails

Notifications

SSH and GPG keys

Security

OAuth applications


Personal access tokens

Repositories

Organizations

Saved replies

Organization settings

 zenhub

Register a new OAuth application

Application name

ZenHub Enterprise

Something users will recognize and trust

Homepage URL

<https://zenhub.com>

The full URL to your application homepage

Application description

Project management for innovative organizations

This is displayed to all potential users of your application

Authorization callback URL

<https://zenhub.com.company.com/auth/github/callback>

Your application's callback URL. Read our [OAuth documentation](#) for more information.

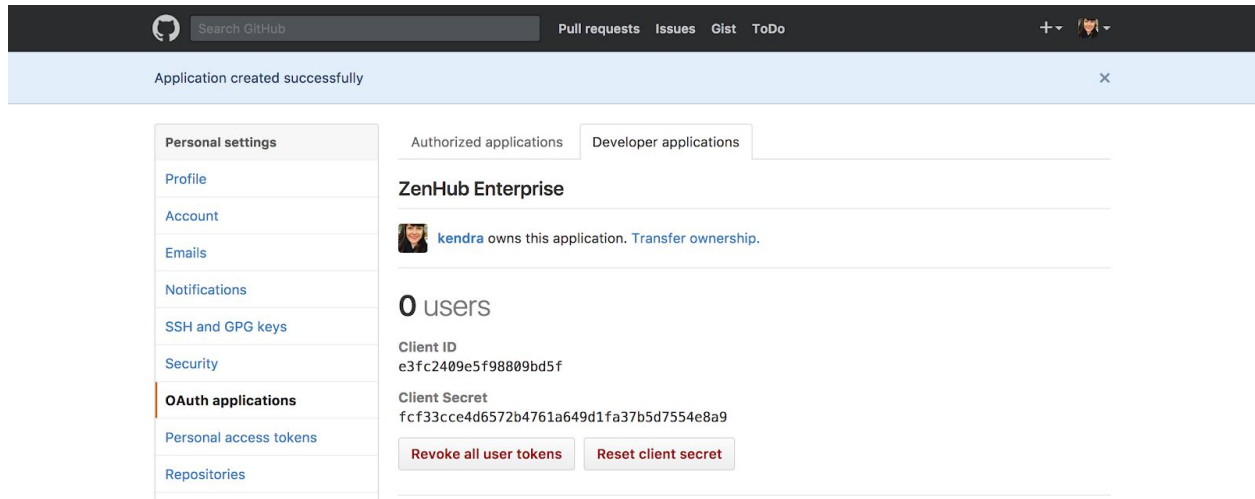
Register application

Cancel

Note: If you choose to use a domain (Ex. zenhub.company.com) instead of an IP address, then the callback URL should be <https://zenhub.company.com/auth/github/callback>.

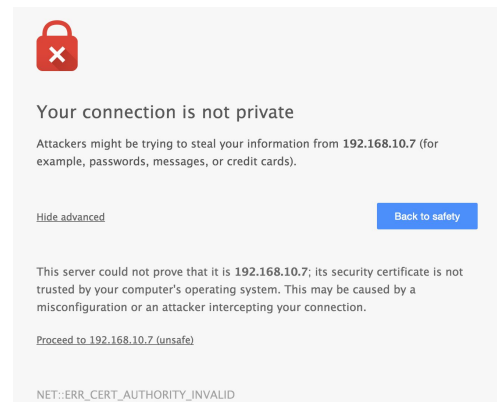
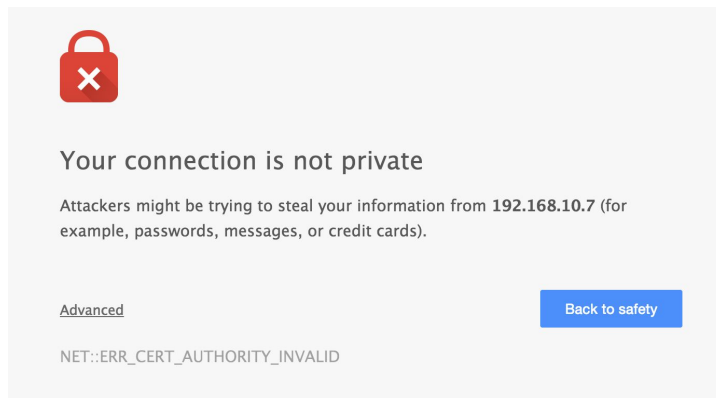
You must ensure your DNS server points that domain (zenhub.company.com) to your ZenHub Enterprise IP address. You can also **upload an image** to make finding your OAuth application easier. You can download the image [here](#).

Once you register the application, you will see a page similar to the one below. Take note of the **Client ID** and **Client Secret** as you will need them later.



Configure Your ZenHub Enterprise Instance

Access the ZenHub Enterprise **Settings** page via the URL provided in Step 4. You will see the following image:



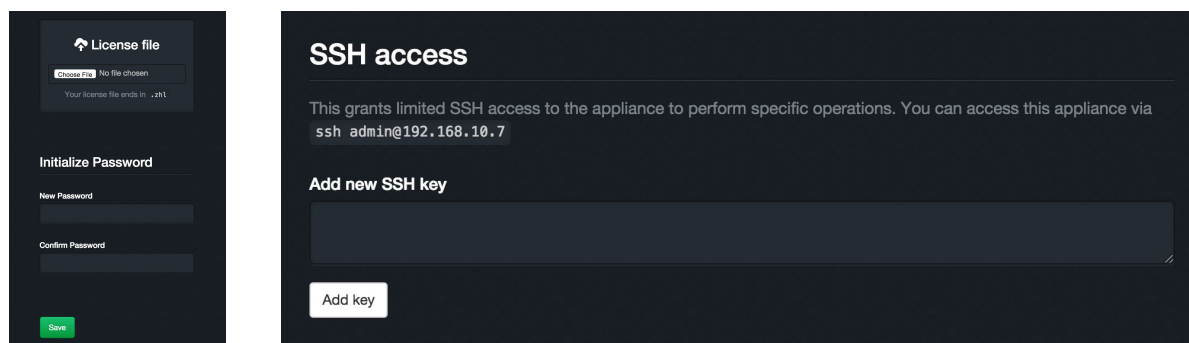
This warning is displayed because a self-signed certificate is being used in order to establish a SSL connection. Once SSL settings are configured, this warning will no longer appear.

For now, click on **Advanced**, and then click on **Proceed to appliance_ip_address (unsafe)**.

You will be redirected to the ZenHub Enterprise **License** page. Here, you will be prompted to upload a valid license file (.zhl) and initialize a password for the Settings page. Click **Save** to proceed.

Note: The password will be required for login when accessing the **Settings** page, **Change Password** page, and **User Report** page. You can share the **Extension Download** page with your team, as it does **not** require authentication.

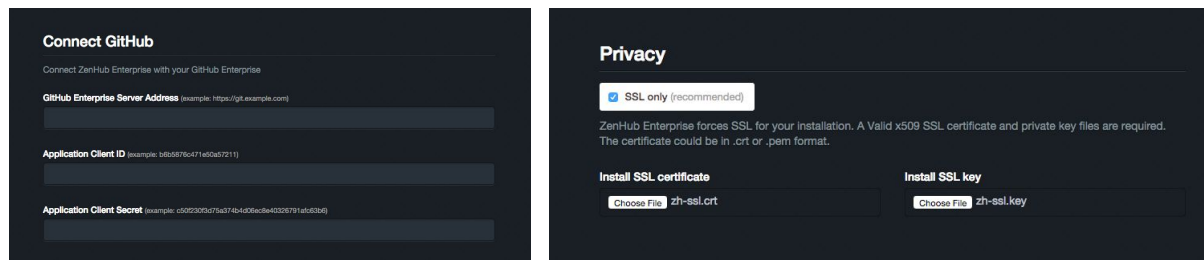
Optional: In the **SSH access** section, add your ssh key to the textbox and click **Add key**. Adding the ssh here will allow you to ssh into the ZenHub Enterprise Appliance. This is useful if you forget your Settings page password.



The image shows two side-by-side screenshots of the ZenHub Enterprise installation interface. The left screenshot is the 'License file' section, featuring a 'Choose file' button, a note 'No file chosen', and a text indicator 'Your license file ends in .zhl'. Below this is the 'Initialize Password' section with 'New Password' and 'Confirm Password' input fields, and a 'Save' button at the bottom. The right screenshot is the 'SSH access' section, which includes a text block explaining limited SSH access to the appliance. It shows a terminal-style command 'ssh admin@192.168.10.7'. Below is the 'Add new SSH key' section with a large text area for the key and an 'Add key' button.

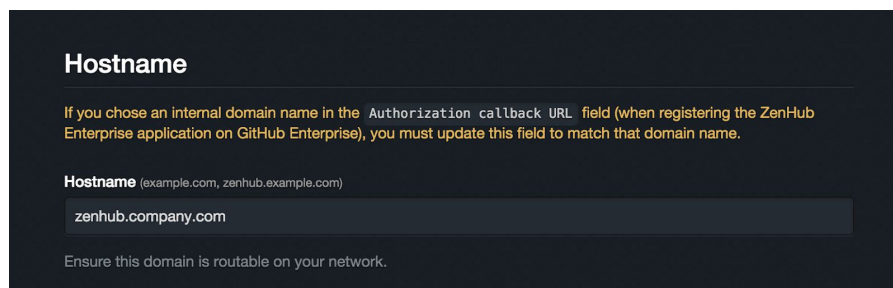
Navigate to the **Connect GitHub** section. You will see a form like the image below. Enter the homepage address of your GitHub Enterprise instance. Also enter the **Client ID** and **Client Secret** (generated from the previous step). Under the **Privacy** header, you will see **SSL only** is enabled by default.

Click **Choose File** to install your SSL Certificate (in PEM format.) This file will usually have a **.pem**, **.crt**, or **.cer** extension. Then click **Choose file** to install your SSL Key. This file will usually have a **.key** extension. The private key **must not** have a passphrase. To enable SSL, you must configure the Hostname and DNS.



The image shows two side-by-side screenshots of the ZenHub Enterprise installation interface. The left screenshot is the 'Connect GitHub' section, with a subtitle 'Connect ZenHub Enterprise with your GitHub Enterprise'. It contains three input fields: 'GitHub Enterprise Server Address' (with an example URL), 'Application Client ID' (with a long alphanumeric string), and 'Application Client Secret' (with another long alphanumeric string). The right screenshot is the 'Privacy' section. It features a toggle switch for 'SSL only (recommended)' which is turned on. Below this is a text block stating that ZenHub Enterprise forces SSL and requires valid x509 SSL certificate and private key files. At the bottom, there are two sections: 'Install SSL certificate' and 'Install SSL key', each with a 'Choose File' button and a text input field containing 'zh-ssl.crt' and 'zh-ssl.key' respectively.

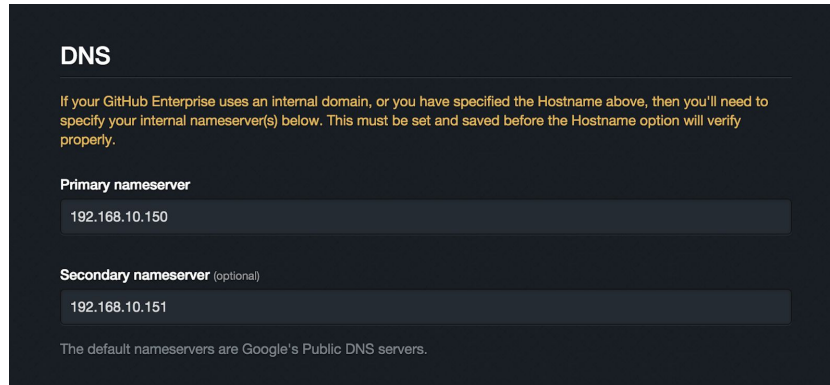
Note: The **Hostname** will automatically appear as the ZenHub Enterprise IP address. If you chose an internal domain name in the **Authorization callback URL** field (when registering the **ZenHub Enterprise** application on **GitHub Enterprise**) in step 5.3, you must update this field to match that domain name.



The image shows a screenshot of the 'Hostname' configuration screen. It has a title 'Hostname' and a text block explaining that if an internal domain name was chosen in the 'Authorization callback URL' field, it must be updated here. Below this is an input field for the 'Hostname' with the example '(example.com, zenhub.example.com)' and the value 'zenhub.company.com'. At the bottom, there is a note: 'Ensure this domain is routable on your network.'

If your **GitHub Enterprise** instance uses an internal domain (for example: git.company.com) or you have specified the Hostname above, you must specify the Primary and Secondary DNS nameservers below.

This will enable **ZenHub Enterprise** to sign in the user with **GitHub Enterprise** OAuth.



DNS

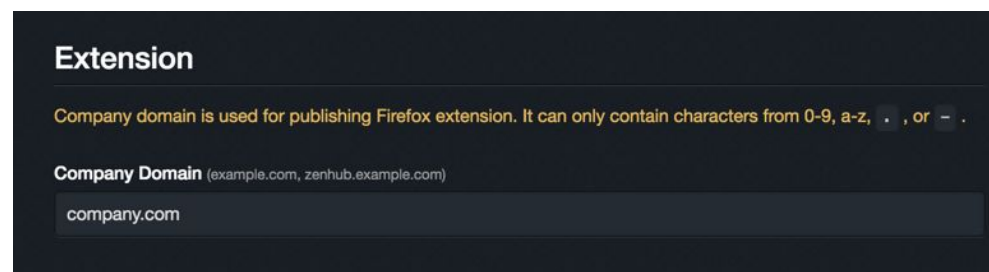
If your GitHub Enterprise uses an internal domain, or you have specified the Hostname above, then you'll need to specify your internal nameserver(s) below. This must be set and saved before the Hostname option will verify properly.

Primary nameserver

Secondary nameserver (optional)

The default nameservers are Google's Public DNS servers.

Note: If, when a user signs into the **ZenHub Enterprise** extension, a “*Fail to sign in ZenHub*” error message appears, check your **GitHub Enterprise** server address in Step 6.1. Also check the **DNS settings** above to ensure the nameservers are able to point your **GitHub Enterprise** server address to the correct IP address. **Enter your Company Domain.** This will be used when we are publishing the Extensions.

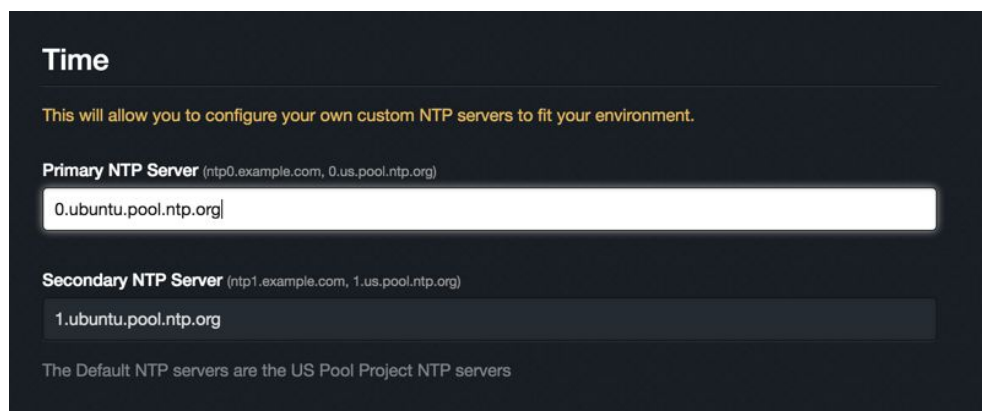


Extension

Company domain is used for publishing Firefox extension. It can only contain characters from 0-9, a-z, ., or -.

Company Domain (example.com, zenhub.example.com)

To configure a custom NTP Server for the ZenHub Enterprise Appliance, add a NTP server address to the Primary and Secondary NTP Server fields. ZenHub Enterprise Appliances use the US Ubuntu NTP Pool Servers by default.



Time

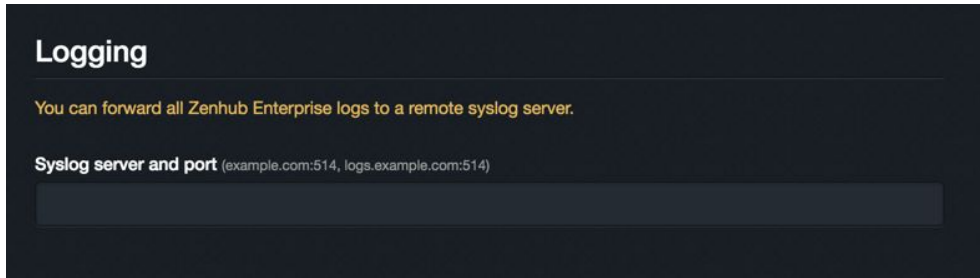
This will allow you to configure your own custom NTP servers to fit your environment.

Primary NTP Server (ntp0.example.com, 0.us.pool.ntp.org)

Secondary NTP Server (ntp1.example.com, 1.us.pool.ntp.org)

The Default NTP servers are the US Pool Project NTP servers

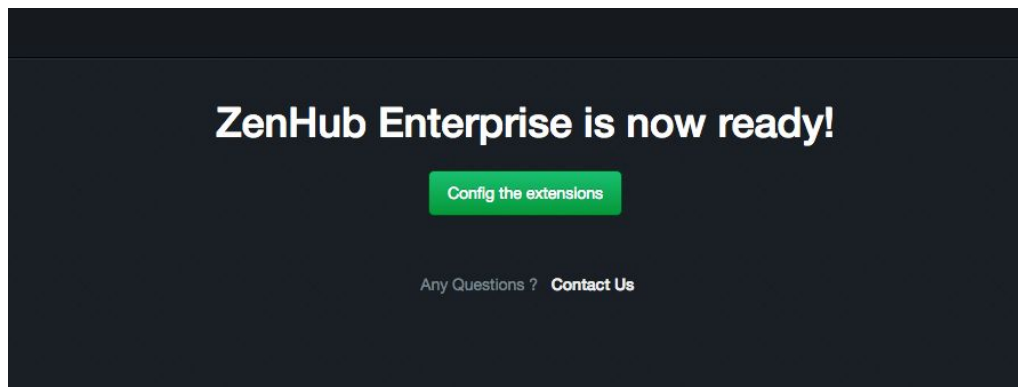
Optional: Configure the Appliance to forward its logs to a remote syslog server.



The screenshot shows a dark-themed configuration window titled "Logging". Below the title, a yellow text line states: "You can forward all Zenhub Enterprise logs to a remote syslog server." Underneath, there is a label "Syslog server and port" followed by a small example "(example.com:514, logs.example.com:514)". Below this label is a long, empty text input field.

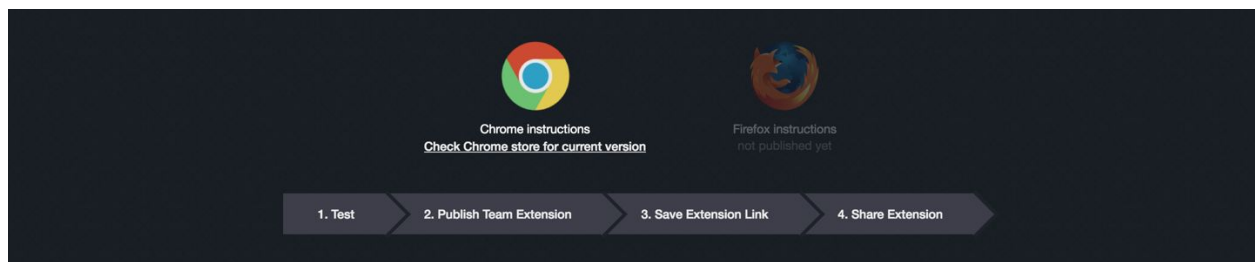
Click **Save settings**. This process can take up to 10 minutes.

When the settings are saved, you will see a button prompting you to **Config the Extension**. It will redirect you to the extension configuration page



Configure the ZenHub extension

The extension page explains how to publish the extensions for Chrome and Firefox. Follow the instructions for each browser to configure and publish the extension, and make the extension link available to users.



Distribute the Extension

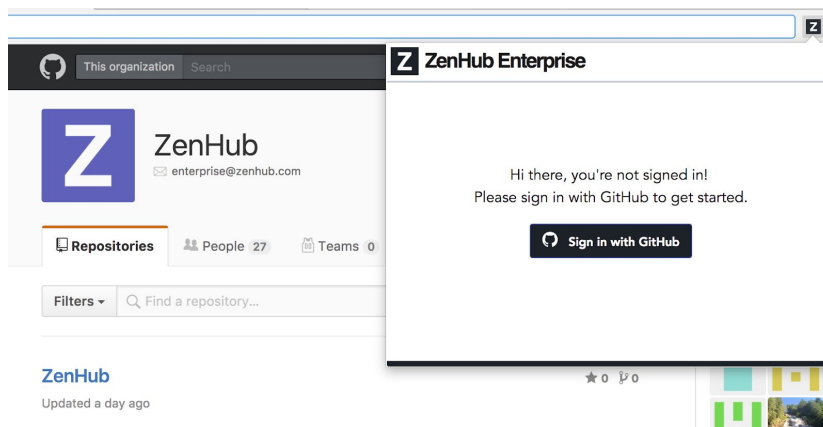
ZenHub Enterprise is now ready to be shared with your team. To install ZenHub Enterprise on Chrome or Firefox, new users can visit the following URL:

<https://<zenhub-enterprise-hostname>/setup/download>

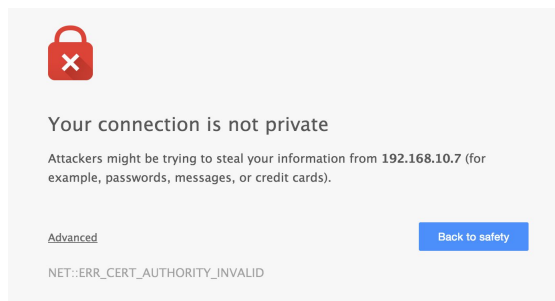
Note: You may wish to copy this URL to an internal wiki or support page so new users can easily download the ZenHub Enterprise extension.

Sign in to ZenHub Enterprise

Sign in to ZenHub Enterprise through the black icon to the right of your address bar.



Note: If you do not have SSL enabled you may see this error screen. Click **Advanced** and **Proceed** to continue.



Sign in using your GitHub credentials, and you're ready to roll! Your version of ZenHub Enterprise is ready! If you have any questions regarding your ZenHub Enterprise installation, we are happy to assist you.

Primary contact: enterprise@zenhub.com