Configuring built-in firewall rules

In this article

You can view default firewall rules and customize rules for your GitHub Enterprise Server instance.

About your GitHub Enterprise Server instance's firewall

GitHub Enterprise Server uses Ubuntu's Uncomplicated Firewall (UFW) on the virtual appliance. For more information see "UFW" in the Ubuntu documentation. GitHub Enterprise Server automatically updates the firewall allowlist of allowed services with each release.

After you install GitHub Enterprise Server, all required network ports are automatically opened to accept connections. Every non-required port is automatically configured as `deny`, and the default outgoing policy is configured as `allow`. Stateful tracking is enabled for any new connections; these are typically network packets with the `SYN` bit set. For more information, see "Network ports."

The UFW firewall also opens several other ports that are required for GitHub Enterprise Server to operate properly. For more information on the UFW rule set, see the UFW README.

We do not recommend customizing UFW as it can complicate some troubleshooting issues.

Viewing the default firewall rules

1. SSH into your GitHub Enterprise Server instance. If your instance comprises multiple nodes, for example if high availability or geo-replication are configured, SSH into the primary node. If you use a cluster, you can SSH into any node. For more information about SSH access, see "Accessing the administrative shell (SSH)."

   ```
   ssh -p 122 admin@HOSTNAME
   ```

2. To view the default firewall rules, use the `sudo ufw status` command. You should see output similar to this:

   ```
   $ sudo ufw status
   > Status: active
   > To                            Action      From
   > --                            ------      ----
   ```

```
> ghe-1194                   ALLOW       Anywhere
> ghe-122                    ALLOW       Anywhere
> ghe-161                    ALLOW       Anywhere
> ghe-22                     ALLOW       Anywhere
> ghe-25                     ALLOW       Anywhere
> ghe-443                    ALLOW       Anywhere
> ghe-80                     ALLOW       Anywhere
> ghe-8080                   ALLOW       Anywhere
> ghe-8443                   ALLOW       Anywhere
> ghe-9418                   ALLOW       Anywhere
> ghe-1194 (v6)              ALLOW       Anywhere (v6)
> ghe-122 (v6)               ALLOW       Anywhere (v6)
> ghe-161 (v6)               ALLOW       Anywhere (v6)
> ghe-22 (v6)                ALLOW       Anywhere (v6)
> ghe-25 (v6)                ALLOW       Anywhere (v6)
> ghe-443 (v6)               ALLOW       Anywhere (v6)
> ghe-80 (v6)                ALLOW       Anywhere (v6)
> ghe-8080 (v6)              ALLOW       Anywhere (v6)
> ghe-8443 (v6)              ALLOW       Anywhere (v6)
> ghe-9418 (v6)              ALLOW       Anywhere (v6)
```

Adding custom firewall rules

Warning: Before you add custom firewall rules, back up your current rules in case you need to reset to a known working state. If you're locked out of your server, visit GitHub Enterprise Support and contact us to reconfigure the original firewall rules. Restoring the original firewall rules involves downtime for your server.

1. Configure a custom firewall rule.
2. Check the status of each new rule with the `status numbered` command.

   ```
   sudo ufw status numbered
   ```

3. To back up your custom firewall rules, use the `cp` command to move the rules to a new file.

   ```
   sudo cp -r /etc/ufw ~/ufw.backup
   ```

After you upgrade your GitHub Enterprise Server instance, you must reapply your custom firewall rules. We recommend that you create a script to reapply your firewall custom rules.

Restoring the default firewall rules

If something goes wrong after you change the firewall rules, you can reset the rules from your original backup.

Warning: If you didn't back up the original rules before making changes to the firewall, visit GitHub Enterprise Support and contact us for further assistance.

1. SSH into your GitHub Enterprise Server instance. If your instance comprises multiple nodes, for example if high availability or geo-replication are configured, SSH into the primary node. If you use a cluster, you can SSH into any node. For more information

about SSH access, see "Accessing the administrative shell (SSH)."

```
ssh -p 122 admin@HOSTNAME
```

2. To restore the previous backup rules, copy them back to the firewall with the `cp` command.

```
sudo cp -f ~/ufw.backup/*rules /etc/ufw
```

3. Restart the firewall with the `systemctl` command.

```
sudo systemctl restart ufw
```

4. Confirm that the rules are back to their defaults with the `ufw status` command.

```
$ sudo ufw status
> Status: active
> To                         Action      From
> --                         ------      ----
> ghe-1194                   ALLOW       Anywhere
> ghe-122                    ALLOW       Anywhere
> ghe-161                    ALLOW       Anywhere
> ghe-22                     ALLOW       Anywhere
> ghe-25                     ALLOW       Anywhere
> ghe-443                    ALLOW       Anywhere
> ghe-80                     ALLOW       Anywhere
> ghe-8080                   ALLOW       Anywhere
> ghe-8443                   ALLOW       Anywhere
> ghe-9418                   ALLOW       Anywhere
> ghe-1194 (v6)              ALLOW       Anywhere (v6)
> ghe-122 (v6)               ALLOW       Anywhere (v6)
> ghe-161 (v6)               ALLOW       Anywhere (v6)
> ghe-22 (v6)                ALLOW       Anywhere (v6)
> ghe-25 (v6)                ALLOW       Anywhere (v6)
> ghe-443 (v6)               ALLOW       Anywhere (v6)
> ghe-80 (v6)                ALLOW       Anywhere (v6)
> ghe-8080 (v6)              ALLOW       Anywhere (v6)
> ghe-8443 (v6)              ALLOW       Anywhere (v6)
> ghe-9418 (v6)              ALLOW       Anywhere (v6)
```