Linux Forwarder Release Notes

Downloads

Package	Kernel Version	Download URL
Rocky Linux 9	5.14.0	stairwell-2.4.6-1.el9.amd64.rpm 🔗 8efcdd84d894e7a85a9299b69cf75b5f55e39fe2c10f71f90fce33d405a541e4
RHEL9	5.14.0	stairwell-2.4.6-1.el9.amd64.rpm 🔗 8efcdd84d894e7a85a9299b69cf75b5f55e39fe2c10f71f90fce33d405a541e4
RHEL8	4.18.0-80	stairwell-2.4.6-1.el8.amd64.rpm 🔗 737c00a8e5c2c322311debf601f753f8d5acdbbc07a7491656a1b0e83b897273
RHEL7	3.10.0-1160	stairwell-2.4.6-1.el7.amd64.rpm 🔗 4a4fd1971e7913b3a5b0f29dba86a09a5b5f9a905dafaa00ed7dd168fe735945
RHEL6	2.6.32	stairwell-2.4.6-1.el6.amd64.rpm 🔗 861acb3ae4638b41314428971c1dbda22cec80ee50c164991b110f7173fee444
Ubuntu 20.04	5.15	stairwell-2.4.6-1.amd64.deb 🔗 7079ec5d10e7c897c566fb2b821b5df5e5813e5d88bfa0f1eb67bcbda32f1542
Ubuntu 22.04	6.5	stairwell-2.4.6-1.amd64.deb 🔗 7079ec5d10e7c897c566fb2b821b5df5e5813e5d88bfa0f1eb67bcbda32f1542
Ubuntu 24.04	6.8	stairwell-2.4.6-1.amd64.deb 🔗 7079ec5d10e7c897c566fb2b821b5df5e5813e5d88bfa0f1eb67bcbda32f1542
Debian		stairwell-2.4.6-1.amd64.deb 🔗 7079ec5d10e7c897c566fb2b821b5df5e5813e5d88bfa0f1eb67bcbda32f1542
Checksums		checksums.txt 🔗

Changes

FIX **Fix A Bug Where The Forwarder Would Not Receive The Configured 'Glob' Policy Exclusions During Initial Backscan.**

The Forwarder will now send a metadata request to the Stairwell backend during startup before requesting policies. This ensures the backend has sufficient information to generate correct policies for that Forwarder.

FIX **Fix A Bug Where An Uninstalled Forwarder Would Still Show As 'Installed' In The Stairwell Web Console.**

The Forwarder would not always be able to send a metadata update during un-installation. This is now fixed.

IMPROVED **Backscan Stats Now Include Files That Were Seen But Did Not Require Uploading.**

Files that are succesfully reported during pre-intake, but not requested to be uploaded, are now included in the backscan stats.

Package Installation

To install or upgrade the stairwell forwarder service, you will need to download the appropriate package and install it with your distribution's package management software.

Note: the audit service will need to be enabled for realtime events. See the section on enabling audit 🔗 below.

Rocky Linux 9

New Installation

```
$>
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.el9.amd64.rpm
sudo rpm -i stairwell-2.4.6-1.el9.amd64.rpm
```

Upgrade

```
$>
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.el9.amd64.rpm
sudo rpm -U stairwell-2.4.6-1.el9.amd64.rpm
```

RHEL9

New Installation

```
$>
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.el9.amd64.rpm
sudo rpm -i stairwell-2.4.6-1.el9.amd64.rpm
```

Upgrade

```
$>
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.el9.amd64.rpm
sudo rpm -U stairwell-2.4.6-1.el9.amd64.rpm
```

RHEL8

New Installation

```
$>
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.el8.amd64.rpm
sudo rpm -i stairwell-2.4.6-1.el8.amd64.rpm
```

Upgrade

```
$>
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.el8.amd64.rpm
sudo rpm -U stairwell-2.4.6-1.el8.amd64.rpm
```

RHEL7

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.el7.amd64.rpm
sudo rpm -i stairwell-2.4.6-1.el7.amd64.rpm
```
$>

Upgrade

```
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.el7.amd64.rpm
sudo rpm -U stairwell-2.4.6-1.el7.amd64.rpm
```
$>

RHEL6

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.el6.amd64.rpm
sudo rpm -i stairwell-2.4.6-1.el6.amd64.rpm
```
$>

Upgrade

```
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.el6.amd64.rpm
sudo rpm -U stairwell-2.4.6-1.el6.amd64.rpm
```
$>

Ubuntu 20.04

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.amd64.deb
sudo apt-get install ./stairwell-2.4.6-1.amd64.deb
```
$>

Ubuntu 22.04

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.amd64.deb
sudo apt-get install ./stairwell-2.4.6-1.amd64.deb
```
$>

Ubuntu 24.04

New Installation

```
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.amd64.deb
sudo apt-get install ./stairwell-2.4.6-1.amd64.deb
```
$>

Debian

New Installation

```
$>
curl -LO https://downloads.stairwell.com/linux/2.4.6/stairwell-2.4.6-1.amd64.deb
sudo apt-get install ./stairwell-2.4.6-1.amd64.deb
```

Forwarder Configuration

If this is the first time installing the forwarder on this machine, the service will need to be configured before it will activate. To configure the service, edit the configuration file in **/etc/stairwell/config.json** with <u>vim</u> or another editor of your choice, such as <u>nano</u>.

```
$>
sudo vim /etc/stairwell/config.json
```

You will need your Environment ID along with your Deployment Token, which should be placed in the **EnvId** and **Token** fields, respectively

```
/etc/stairwell/config.json
{
    "logger": {
        "loglevel": "error"
    },
    "asset": {
        "idempotencyKey": "",
        "EnvId": "ABCDEF-ABCDEF-123ABC-ABCD1234",
        "Token": "ABCDEFG1234567HIJKLMNOP789012QRSTUVW345678XYZABCD901"
    },
    "interpreters": [
        "sh",
        "bash",
        "python",
        "python3",
        "go",
        "ruby",
        "perl",
        "lua",
        "Rscript"
    ],
    "ostype": "server",
    "proxyURL": "http://your.proxy.host",
    "enableEvents": true
}
```

Using a Proxy

If your environment requires a proxy, you may also set the **proxyURL** value to the appropriate URL:

```
/etc/stairwell/config.json
    "ostype": "server",
    "proxyURL": "http://your.proxy.host",
    "enableEvents": true
}
```

Enabling Audit

For realtime event support, the auditd service needs be enabled so that the stairwell forwarder can set rules and read events via domain socket or kernel multicast. Most distributions will have this enabled by default and will

require no other special configuration, but if it is disabled on your system for some reason, you will need to enable it.

The commands to do this will differ depending on your distribution, so follow the instructions listed in the correct section below to check if auditd is enabled, and re-enable if necessary.

Enabling Audit on systemd-managed distributions

More recent distributions, such as RHEL7 and above, use Systemd, which manages services using the `systemctl` command.

To check if auditd is enabled, you can run the following command

```
$>
sudo systemctl status auditd
```

If the service is running, you will see a status message containing **Active: active**.

```
● auditd.service - Security Auditing Service
  ...
    Active: active (running) since ...
```

If you see this, you should be good to go.

If the service is not running, it will say something like **Active: inactive** instead:

```
● auditd.service - Security Auditing Service
  ...
    Active: inactive (dead) since ...
```

If the service is inactive, you can enable the service and start it immediately with:

```
$>
sudo systemctl enable --now
```

Enabling audit on sysvinit-managed distributions

Older systems may require the `service` and `chkconfig` commands to start and enable the service, respectively.

To see if auditd is running, run the following command:

```
$>
sudo service auditd status
```

If the service is running, you will see somthing like the following:

```
auditd (pid  1009) is running...
```

Otherwise you will see:

```
auditd is stopped
```

If the service is stopped, you can start it and enable it on reboot with the following two commands:

```
$>
sudo service auditd start # start the auditd service
sudo chkconfig auditd on  # enable auditd on reboot
```