



CallStash for On-Premise and Virtual PBX.

Admin Manual

V3 – 20.04.2022



1	SCOPE	3
2	OVERVIEW	3
3	NETWORK ACCESS	3
4	VIRTUAL MACHINE CONFIGURATION	3
5	CONSOLE ACCESS	4
6	INITIAL CALLSTASH CONFIGURATION	4
6.1	Network Configuration	5
6.2	Configuring server 'host name'	5
6.3	Setting a 'root' password	5
6.4	CallStash Disk Configuration	5
6.5	Making changes after initial deployment	6
7	SSL CERTIFICATES	7
7.1	Using Let's Encrypt	7
7.2	Installing your own certificates	8
8	PBX CONFIGURATION	10
8.1	CallStash User Creation and Permissions	10
8.2	API Access Token	11
9	SYSTEM MANAGEMENT	11
9.1	Licensing	11
9.2	Admin users	12
9.3	Log in to the Admin User Interface	12
9.4	Adding your PBX	14
9.5	PBX Status	15
9.6	Managing Companies	16
9.7	Company settings	18
9.8	Configuring an email server	18
9.9	Notifications and Email settings	19
9.10	System Backup and Resilience	20
9.11	Bulk export of a company's call recordings	24
9.12	On-Premise RAID Arrays	25
10	SUPPORT	27
10.1	Starting RST from the Web UI	27
10.2	Starting RST from the command line	27
11	SOFTWARE UPDATES	28
12	HOW TO	30

1 Scope

This document provides the information necessary to configure a new CallStash installation and then to manage the system on a day to day basis. The target audience for this document is CallStash system administrators. This document does not cover the general end user interface provided to users who are not administrators.

2 Overview

Your CallStash product will be delivered either as a physical appliance or as a virtual machine image (VM). The former is a standalone device that you connect into your network. The latter you install either on your internal VM infrastructure or on a third party hosting service such as AWS, Google Cloud or Azure.

Note: IPCortex provides a Virtual Machine as an OVA image and we are not involved with and are unable to provide support for installing that image with a cloud service provider.

Commissioning and managing a CallStash system involves:

1. Initial server configuration or a Virtual Machine (Section 4)
2. Initial product configuration, which is via a text-based configuration tool (Sections 5, 6)
3. SSL certificate installation for HTTPS (Section 7)
4. PBX Configuration (Section 8)
5. Ongoing application management provided via a web interface (Sections 9, 9.10.4)
6. Applying software upgrades (Section 11)

3 Network Access

All CallStash instances require Internet access via port 443 for licensing and also access to the PBX, again on port 443. If using Let's Encrypt for SSL certificates [§7.1] then external access through your firewall to port 80 will also be required for certificate installation and renewal.

4 Virtual Machine Configuration

The CallStash VM image includes a 30GB virtual disk containing a minimal Debian operating system and the CallStash operational software. This disk is sufficient to also contain the CallStash database. It is not however sufficient to store call recordings.

As part of your VM configuration **before first boot** you should attach an additional **un-partitioned** drive to the VM image. The size of this disk depends on the number of call recordings you expect to archive. As a rough calculation, CallStash archives approximately 1 second of recording in 8KB of disk space. So, for example:

- If you expect 500 calls per day, 5 days a week (52 x 5 days per year x 500 calls)

- With an average call duration of 4 minutes (240 seconds)
- And want to archive calls for 7 years.

This leads to a calculation of:

$6 \times (52 \times 5 \times 500 \times 240) \times 8000 \text{ bytes} = (\text{approximately}) 1.6\text{TB}$

Alternatively, an approximation can be made by understanding that one hour of recorded audio uses about 30MB of storage.

Note these figures exclude operating system overhead. Unless you have accurate call histories it is advised that you err very much on the side of caution.

The minimum size for the audio disk that will be accepted by CallStash is 50GB.

As stated, please ensure that this disk is attached to your VM configuration **before first boot**.

5 Console access

Initial configuration of a new CallStash installation is via a **console interface**. The console interface will be provided by your hypervisor in the case of a VM. If you are configuring a physical CallStash appliance, then you will need to connect a USB keyboard and a monitor to the product. No mouse is required.

6 Initial CallStash configuration

Once you have connected the console for the first time, you'll be presented with a system configuration tool as shown in Figure 1. The utility is simple and contains the minimum number of steps to get CallStash ready such that you can access the system across your network.

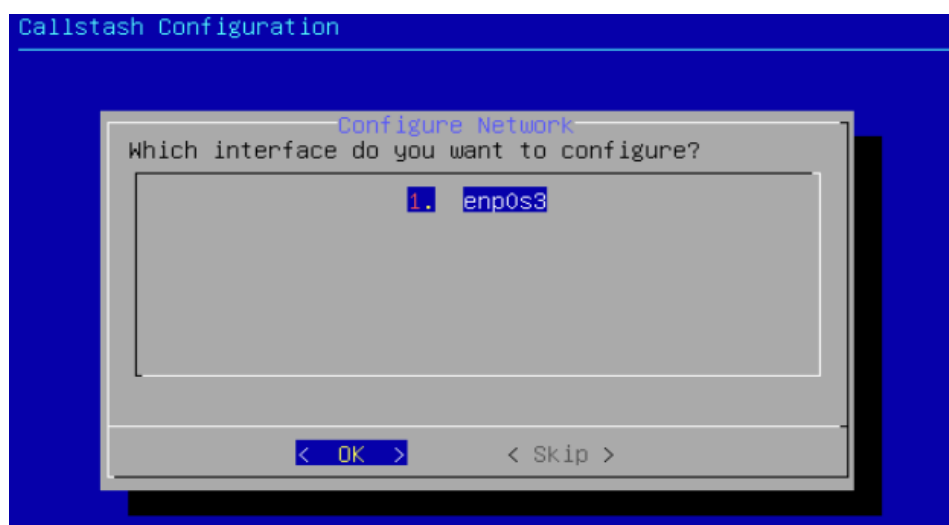


Figure 1: Configuration utility, first page

You will be guided through a short set of pages each dealing with a separate element of the configuration:

1. Selecting the network interface to use
2. Setting up the network parameters (DHCP or Manual)
3. Setting the host name
4. Configuring disk storage

Notes on using the configuration utility:

1. Use the **up** and **down arrows** to select from a list or type the number against the selection you want.
2. Press **Tab** to move between the fields
3. At any point press **Ctrl-C** to return to the start of the setup utility

6.1 Network Configuration

On the first page select the network interface to use for access to CallStash. If there is only one interface listed, then you can simply press enter. The next page will give you the option of using DHCP or manually configuring the interface. The latter allows you to set the IP Address, net mask, gateway, and a list of space separated DNS servers.

6.2 Configuring server 'host name'

After configuring the network you're offered the opportunity to set a device specific host name. By default, the server's internal host name will default to 'callstash'. If you wish to change this, then enter a valid name. The name may only comprise letters and numbers.

It is recommended that you leave the host name as 'callstash'.

6.3 Setting a 'root' password

You will be asked to provide a super user (root) password for your CallStash instance. This password is only for future console access. Remember to use the arrow keys to move between the two password fields!

Please carefully choose a secure password.

6.4 CallStash Disk Configuration

For a physical CallStash appliance your product will have been pre-configured before shipping so you can skip this page by pressing 'Enter'.

For a VM CallStash instance you should have configured and attached an unformatted raw drive to your VM to hold call recordings [§4]. At this stage you will be presented with a list of available

drives for storage. You will be told if there are no available drives in which case you may need to check your VM configuration.

Note: if the attached disk has partitioned drives, then it will not be presented as a candidate for CallStash. If the disk that you've attached is not recognised, continue with configuration. At the end of setup check the virtual disk configuration and if necessary, make changes and re-attach. Then run the CallStash configuration tool [§6.5]

If the drive you've attached to your VM is not shown as available, then check:

- That the drive has not been partitioned
- That the drive is **at least** 50GB in size

6.5 Making changes after initial deployment

You may need to change some of the above settings after you've deployed your CallStash instance, for example:

- if the appliance is moved to a new network location.
- if your disk configuration was not recognised during configuration and you've made changes.

Connect to the CallStash unit via the **console interface** [§5] (keyboard/screen or via your hypervisor). Log in with the user name 'root' and the password is as set above [§6.3].

From the command line run `callstash-config`. This will provide direct access to each of the steps above [Figure 2].

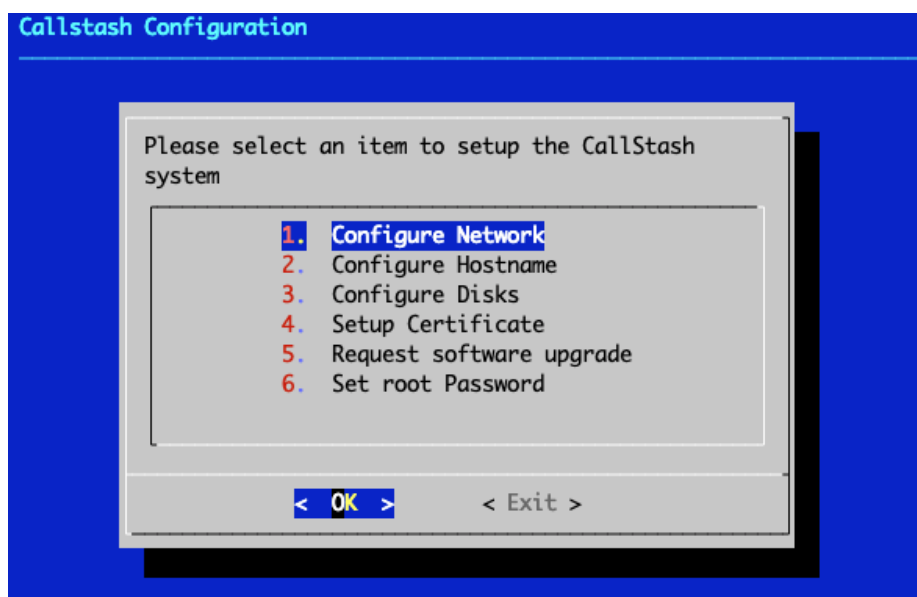


Figure 2 CallStash Configuration Tool

7 SSL certificates

SSL certificates are used to secure HTTPS communication, encrypting CallStash web traffic. CallStash is shipped with 'self-signed' certificates that need to be replaced with signed certificates in order to work efficiently with browsers.

Two options are available:

1. Use Let's Encrypt
2. Install your own certificates from your certificate authority (CA)

The first of these options requires external port 80 traffic to be forwarded to CallStash to complete the process but otherwise is the easier of the two options.

The second option doesn't require port 80 traffic forwarding and instead relies on you installing certificates directly onto the CallStash appliance.

7.1 Using Let's Encrypt

Let's Encrypt is a free, automated, and open certificate authority (CA), run for the public's benefit, details of which can be found on the following site: <https://letsencrypt.org>.

Certificates are issued with a three month lifetime and software installed on CallStash will automatically take care of renewal at the correct time. In broad terms CallStash will make a request to Let's Encrypt for a certificate for the domain server name you want to use for your CallStash instance. Let's Encrypt will then deliver the certificate by sending requests to port 80 (HTTP).

A prerequisite therefore is that requests received to port 80 on your public IP address must be correctly forwarded to CallStash. This may require firewall and/or router configuration.

Using Let's Encrypt to generate a certificate for **callstash.mydomain.com**:

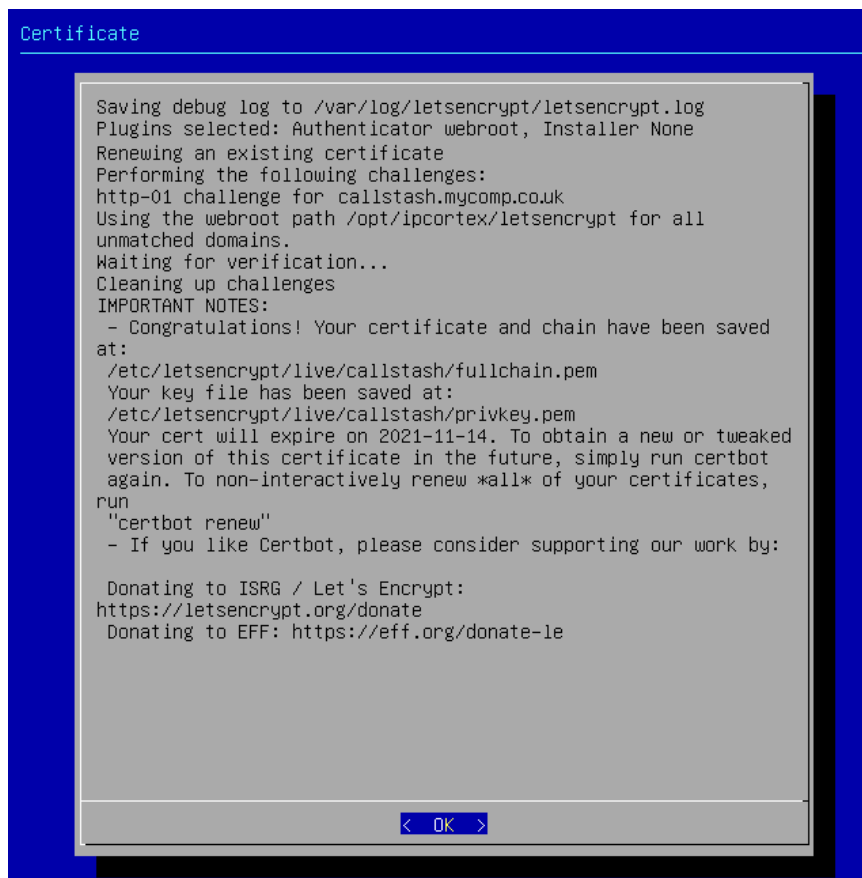
1. Configure your DNS server to point 'callstash.mydomain.com' to your CallStash device. Depending on your network configuration this may require DNS to point to your public IP address for your network with your router configured to forward traffic.
2. Ensure that your network and firewall configurations will correctly route traffic to your CallStash appliance on port 80.
3. Log into the **console interface** [5] and run `callstash-config` and select 'Setup Certificate'

The first two of these steps are entirely dependent on your network and firewall configurations and are outside of the scope of IPCortex and is not something for which IPCortex provides support.

Once your DNS and network are configured and you've run `callstash-config` you will be presented with the top level menu. Select 'Setup Certificate' and, from the next screen, 'Setup Let's Encrypt'. This will take you to a sequence of pages stepping you through the fairly straightforward process:

1. Confirm port 80 and DNS correctly configured
2. Agree to the Let's Encrypt Terms of Service
3. Set an admin email for certificate notifications
4. Enter the domains for which you want a certificate. Generally, this would be a single server name such as 'callstash.mycompany.co.uk'. This will match the DNS record that you confirmed that you set up in step 1 above.

Once you've completed these steps Let's Encrypt will be contacted to verify and issue your certificate which will be installed by CallStash, You'll see a log of the results similar to that shown in Figure 3. Carefully check the output for errors.



```
Certificate

Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator webroot, Installer None
Renewing an existing certificate
Performing the following challenges:
http-01 challenge for callstash.mycomp.co.uk
Using the webroot path /opt/ipcortex/letsencrypt for all
unmatched domains.
Waiting for verification...
Cleaning up challenges
IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved
at:
/etc/letsencrypt/live/callstash/fullchain.pem
Your key file has been saved at:
/etc/letsencrypt/live/callstash/privkey.pem
Your cert will expire on 2021-11-14. To obtain a new or tweaked
version of this certificate in the future, simply run certbot
again. To non-interactively renew *all* of your certificates,
run
"certbot renew"
 - If you like Certbot, please consider supporting our work by:

Donating to ISRG / Let's Encrypt:
https://letsencrypt.org/donate
Donating to EFF: https://eff.org/donate-le

< OK >
```

Figure 3 Let's Encrypt Successful installation

7.2 Installing your own certificates

If you are unable to or would prefer not to use Let's Encrypt you may alternatively install your own correctly signed certificates issued by an appropriate signing authority. This process is more manual:

1. Having decided on the fully qualified server name (e.g. callstash.mycomp.co.uk) use your chosen certifying authority to issue a certificate on your behalf. This will provide you with a certificate chain and a private key.

2. Copy the certificate chain and the private key onto the CallStash server [§7.2.1]
3. Log into the **console interface** [§5]
4. Run **callstash-set-cert** to tell CallStash how to find the files [§7.2.2]
5. Run **callstash-config** to install and activate the files.

Step one is outside the scope of IPCortex and is entirely dependent on your choice of certifying authority.

7.2.1 Copying the certificate and private key

The process of generating your certificate with your certifying authority will provide you with a combined certificate file and a private key file. The certificate file will be the one appropriate for most web servers.

Both of these files must be copied to your CallStash appliance.

You will need to have the files on a computer running an SSH server. Most Linux machines will have an SSH server active. You can enable the SSH Server on Windows as an “optional feature”.

Start up the **console interface** and log in as root [§5].

Use ‘scp’ to copy the two files to the /tmp/ directory:

```
root@callstash:~# cd /tmp
root@callstash:/tmp # scp user@other-server:/path/to/cert.pem .
root@callstash:/tmp # scp user@other-server:/path/to/priv.key .
root@callstash:/tmp # ls
cert.pem
priv.key
root@callstash:/tmp #
```

The names of the files are not significant and are likely to differ from this example.

7.2.2 Installing the certificates

Once copied to CallStash the files must be installed and activated. This is a two-step process.

First, again from the console interface, run the command **callstash-set-cert** and then start the configuration utility **callstash-config**:

```
root@callstash:/tmp # callstash-set-cert ./priv.key ./cert.pem
root@callstash:/tmp # callstash-config
```

From the **callstash-config** menu select the “Setup Certificate” option and from the next page “Use self installed cert” and then confirm your choice.

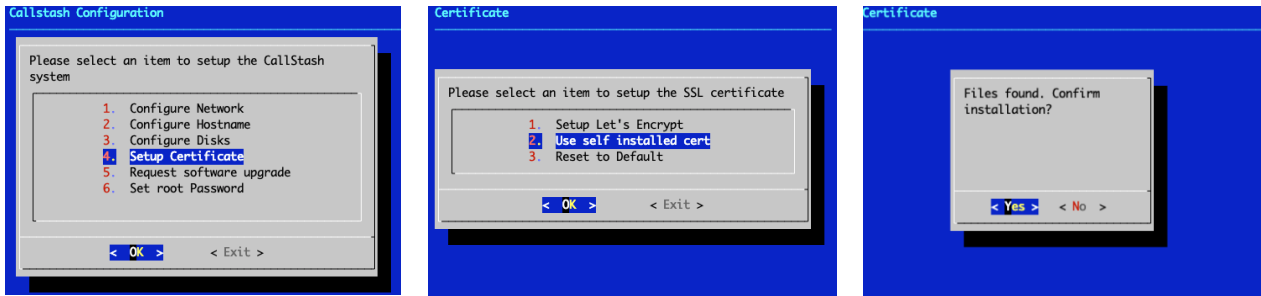


Figure 4 Install certificates

Note: if you are using your own certificates then it's your responsibility to renew those certificates before they expire. To install updated certificates reapply the instructions in this section.

8 PBX Configuration

CallStash archives call recordings from IPCortex PBX systems via the PBX API. Your PBX will first need to be configured to allow access from CallStash.

It is recommended that you create a new user on the PBX dedicated to CallStash.

8.1 CallStash User Creation and Permissions

1. Create a new user. On a multi-company PBX create this user in the **'default'** company.
2. Give the user the following permissions:
 - Billing/Call Reporting (cdr)
 - Billing/CallSummary (cdr_all)
 - Call-Recording download (callrec_dl)
 - Company Admin (comp)

In a multi company box you need to specify from which companies CallStash is to archive recordings. This is done simply by specifying which companies the new CallStash user can manage (Figure 5).

User is an Administrator for the following companies:

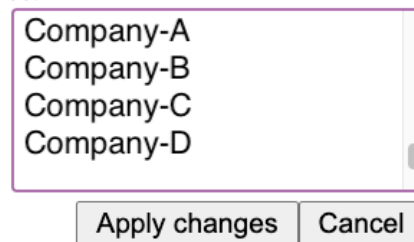



Figure 5: PBX admin company list

Note: you can change which companies are archived by CallStash at any time by changing the set of companies managed by the CallStash user on the PBX. CallStash will automatically update it's company list the **next time it polls the PBX for call recordings**.

8.2 API Access Token

CallStash needs an *access token* to securely access the call recordings on the target PBX. From the user management page on the PBX for the CallStash user click 'Edit user token(s)' [Figure 6] which will open the token management popup [Figure 7]. In the popup, click the 'add +' action and then remember to click the save icon  next to the new token. You will need to copy the new token value into the CallStash admin pages later [§9.4].

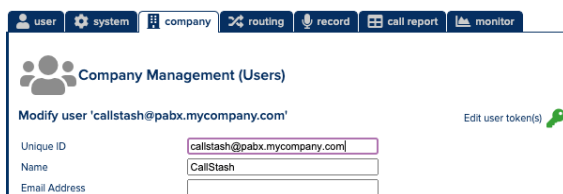


Figure 6: PBX User admin page



Figure 7: Adding an API token

9 System management

Once the steps above have been completed you will be able to access the CallStash web interface. The web interface is used to complete initial configuration and for ongoing system management. To proceed, open CallStash in a modern web browser.

9.1 Licensing

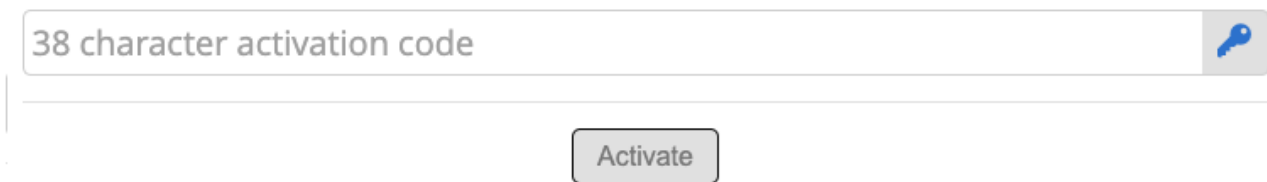
All CallStash products require a valid license. The first time you access an unlicensed CallStash instance you'll be presented with a licensing screen [Figure 8]. **Note that** an on-premise CallStash appliance may have been licensed before being shipped in which case skip straight to §9.2.

Licensing requires a 38 character '*activation code*'. This should have been provided to you with your virtual machine image or can be requested from your IPCortex sales partner.

Enter the 38 character code into the activation field and click "*Activate*". This will verify the code with the IPCortex license servers and, assuming the code is valid, apply the license to the CallStash unit.

CallStash - System Activation

This appliance needs to be activated before use.
Please enter the 38 character activation code supplied with your product



A screenshot of the CallStash licensing page. It features a large text input field with the placeholder text '38 character activation code'. To the right of the input field is a small blue key icon. Below the input field is a grey 'Activate' button.

Figure 8: CallStash licensing page

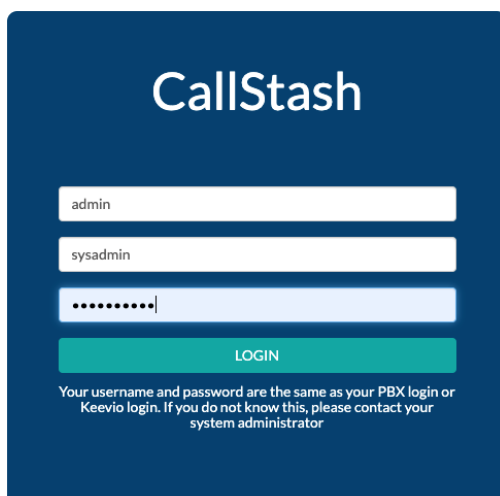
9.2 Admin users

CallStash is pre-configured with two web admin users: 'sysadmin' and 'admin':

- **'sysadmin'**: access to and used for all administrative tasks
- **'admin'**: read-only access to a subset of the CallStash configuration

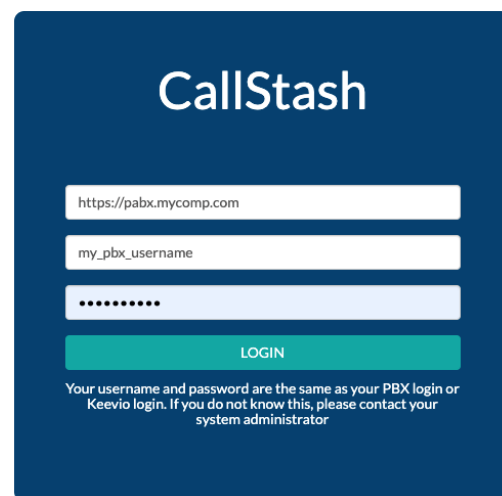
9.3 Log in to the Admin User Interface

Accessing the web interface on a licensed system presents the user with a login screen. To login as an administrator enter: 'admin' for the **PBX URL** (first field) then 'sysadmin' for the IPCortex user name and 'password' for the password [Figure 9]. For comparison Figure 10 shows a typical end-user login specifying the user's PBX.



A screenshot of the CallStash Admin Login screen. The background is dark blue. At the top, the word 'CallStash' is written in white. Below it are three white input fields. The first field contains 'admin', the second contains 'sysadmin', and the third contains a series of dots representing a password. Below the input fields is a green 'LOGIN' button. At the bottom, there is a small white text block that reads: 'Your username and password are the same as your PBX login or Keevio login. If you do not know this, please contact your system administrator'.

Figure 9 Admin Login



A screenshot of the CallStash End User Login screen. The background is dark blue. At the top, the word 'CallStash' is written in white. Below it are three white input fields. The first field contains 'https://pabx.mycomp.com', the second contains 'my_pbx_username', and the third contains a series of dots representing a password. Below the input fields is a green 'LOGIN' button. At the bottom, there is a small white text block that reads: 'Your username and password are the same as your PBX login or Keevio login. If you do not know this, please contact your system administrator'.

Figure 10 End User Login

When you first log in as the administrator, you'll be prompted to change the default password before accessing the management tools [Figure 11]. Once you've successfully changed the password, you'll be taken automatically to the main management screen shown in Figure 12.

Set Password

Please change the default password for user 'sysadmin'

*

*

Minimum password length is 8 characters, must contains at least one
uppercase, one lowercase and one numeric digit

Set password

Figure 11: Setting an initial password

Note: you should repeat this step by logging out and then logging in as user 'admin' to set that user's password.

This is the '**admin home page**' and will be referenced in future sections of this document. This is also the page you'll see as an administrator immediately after you successfully log in to CallStash.

CallStash - Admin

No PBXs

[Add PBX](#)

Warning: backups are not configured

[Configure backup service](#)

Disk usage

Name	Size	Available	Used
audio	1T bytes	867G bytes	13.30%
database	21G bytes	19G bytes	12.96%

System Information

Serial number	12100005
Activated	2021-09-13
Support expires	2021-10-14

[Update Licence](#)

[Check for Upgrades](#)

Scheduler running normally State: WAITING, next process scheduled: 2021-09-15 03:00:00
Next job: disk pruning

Figure 12: Admin home page

9.4 Adding your PBX

Click the 'Add PBX' button to show the new PBX screen [Figure 13]. Your licence will determine the number of PBX units that can be archived on a single CallStash instance. If you're going to archive calls from more than one PBX then please consider all when determining the amount of long term storage required for a VM installation [§4].

[Add new PBX](#)

Name

PBX URL

PBX API access token

API token used to poll PBX

Delete recordings?

☒ Never delete recordings
☐ Older than 5 years
☐ Older than 2 years
☐ Older than 1 year
☐ Older than 6 months
☐ Older than 3 months

Note: these values are defaults for companies hosted on this PBX. Each company can have a customised deletion policy.

Poll period

☐ 30 minutes
☐ 1 hour
☐ 6 hours
☒ 1 day

Time of day to run

[Add new PBX](#) [Finished](#)

Figure 13: Adding a PBX

The **PBX API access token** is the value that you created in [§7.2]. The easiest way to transfer to CallStash is to copy and paste from the PBX user interface. The token will be verified as part of adding the PBX.

By default CallStash will never delete recordings, however **if your archive disks become full, no further recordings will be saved by CallStash**. You can configure CallStash to email warnings when disk space becomes low [§9.9] and low disk status will also be highlighted on the admin home page [Figure 12].

It is recommended that a maximum age for archived recordings be set. The setting on this PBX management page **is a default value for every company on the PBX for which calls will be archived**. CallStash provides the option to set a maximum age on a per-PBX basis on the Company Management Page.

Note: If the maximum age for recordings is reduced then any recordings older than that limit will be deleted when the daily CallStash housekeeping tasks are run.

The default poll period is daily at 3am, which can be reduced to once every 30 minutes. With the default setting CallStash will only archive calls once a day out of normal office hours to reduce load on the PBX during busy periods. The disadvantage of polling once a day is that archived calls will not be available to users until the next day.

Once a new PBX has been added to the system, CallStash will schedule a first poll. If you've set polling for once a day then the first poll will happen at the specified time. For any other poll period the first poll will be scheduled immediately. The PBX will have saved recordings for up to 21 days and CallStash will download all of these on first poll. **For a high volume PBX with many call recordings this initial poll can take a significant amount of time, often measured in hours.**

Once the initial poll has completed subsequent CallStash will only download new recordings and so will complete significantly faster.

9.5 PBX Status

The new PBX will now show in the **admin home page** along with a '*manage*' and '*companies*' options, as shown in Figure 14. You can check the status of the PBX, suspend a PBX or change the poll frequency at any time via the '*manage*' option. 'Manage' also allows you to see the results of the most recent polls.

CallStash Enabled PBXs

ID	Name	URL	State	Actions
110	My Comp Ltd	pabx.mycompany.com	Active	manage companies

[Add PBX](#)

Figure 14: PBX admin list

Figure 15 shows the management page for a PBX and illustrates the status messages for polls.

As well as setting the poll period you can also request an *immediate poll*. Doing so will start the poll as soon as any current scheduled activity completes.

The ‘companies’ action will display a list of companies on the PBX for which CallStash will archive calls.

NOTE: CallStash determines which companies to poll by reading the PBX configuration. **See §8.1 for details on company selection.**

Manage PBX

Name

PBX URL

PBX API access token

Enter new value to change

State

☒ Active

☐ Suspended

Delete recordings?

☐ Never delete recordings

☒ Older than 5 years

☐ Older than 2 years

☐ Older than 1 year

☐ Older than 6 months

☐ Older than 3 months

Note: these values are defaults for companies hosted on this PBX. Each company can have a customised deletion policy.

Poll period

☒ 30 minutes

☐ 1 hour

☐ 6 hours

☐ 1 day

Recent Poll History

☐ Show all

2021-06-23 15:26:46		COMPLETE		
Company	Calls			
	Polled	New	Failed	
Default Company	0	0	0	
Demonstration	1164	1164	0	

* re-activated this poll, † new company added this poll

Figure 15: Poll status

9.6 Managing Companies

Clicking on the ‘companies’ action against a PBX [Figure 14] will display a list of all companies currently archived by CallStash [Figure 16]. As described in §8.1 this list of archived companies is managed by changing the managed companies on the PBX.

CallStash - Admin

My Comp Ltd

Monitored Companies

Label	Name	State	Last Poll	Call count	Storage	Actions
Company C	company_c_540	Active	2021-11-22 16:41:28	-	-	manage
Default Company	default	Active	2021-11-22 16:41:29	-	-	manage
Demonstration	demonstration	Active	2021-11-18 15:30:57	1,271	949K bytes	manage

[Refresh List](#)

[Finished](#)

Figure 16: Managed Company List

The company list will be update each time CallStash downloads the latest call recordings for that PBX. If you make changes to the company list on the PBX and don't wish to wait for the next poll cycle then click on the '*Refresh List*' button.

The state of a company will be 'Active' for companies that are being archived by CallStash. If a company is removed from the managed company list [§8.1] then they will appear in the company list as 'Suspended'.

Suspended companies may be *deleted* from CallStash.

Deleting a company from CallStash will delete ALL recordings archived for that company. These recordings cannot be subsequently recovered.

Label	Name	State	Last Poll	Call count	Storage	Actions
Company C	company_c_540	Suspended	2021-11-22 16:41:28	-	-	manage delete company
Default Company	default	Active	2021-11-22 16:41:29	-	-	manage
Demonstration	demonstration	Delete Pending	2021-11-18 15:30:57	1,271	949K bytes	cancel delete

Figure 17: Deleting companies

Figure 17 shows two inactive companies. The first, "Company C" is *suspended*, that is it has been removed from the set of companies archived by CallStash. Companies in this state have an additional action: "delete company". Clicking this link and acknowledging the various warnings will change the state of the company to *delete pending*.

Deleting companies does not happen immediately, instead they are 'marked', ready to be deleted, as can be seen in the 'demonstration' company above.

Marked companies are deleted as part of the overnight housekeeping activities carried out by CallStash. Up until those housekeeping tasks start to delete a company an administrator can click on "*cancel delete*" and revert the company back to 'suspended'.

9.7 Company settings

Use the 'manage' [Figure 16] action next to a company to access company settings. Figure 18 shows the settings for a company. The two key elements on this page are:

- How long CallStash should keep recordings for this company
- The directory on the server where this companies' recordings can be accessed.

The choice for how long to keep archived calls can be set per company or can be set (the default) to use the settings of the PBX.

Note that reducing the maximum age for recordings will cause any recordings older than that limit to be deleted.

The archive directory points to a location in the CallStash directory structure that provides access to this companies call recordings. This path is relevant if, for example, an organisation leaving a shared platform requires a copy of their archived calls. The calls can be retrieved via the console interface and using the 'scp' command to copy the calls to a remote server. Please note that these recording will be encrypted, see §9.11 for more information.

Company Settings

Name	Delete recordings?
demonstration	<input type="radio"/> Use PBX defaults (Never), <input type="radio"/> Never delete recordings <input type="radio"/> Older than 5 years <input type="radio"/> Older than 2 years <input type="radio"/> Older than 1 year <input type="radio"/> Older than 6 months <input type="radio"/> Older than 3 months
Label	
Demonstration	
State	
Active	

Call recordings for this company are available in the CallStash file system in the following directory:

/var/lib/callstash/companies/201

Save Changes

Cancel

Figure 18: Company settings

9.8 Configuring an email server

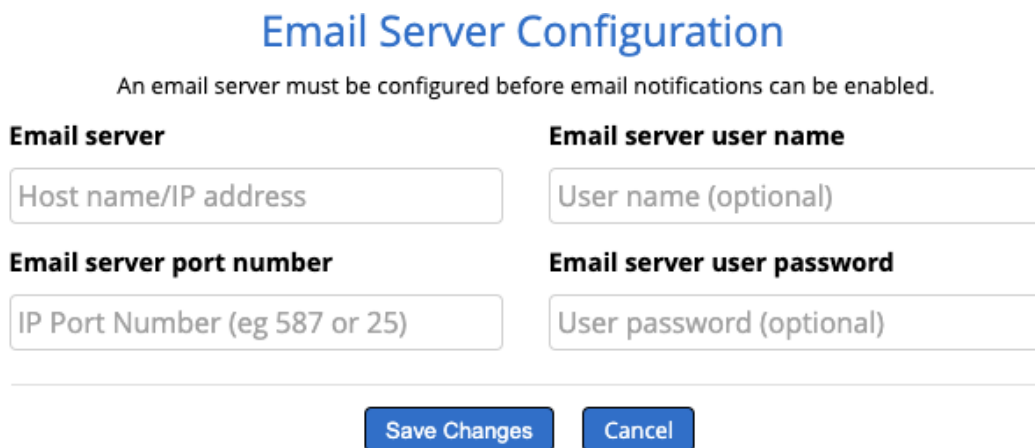
CallStash is able to send email notifications to administrators under certain circumstances:

- When disk space is low
- When archiving PBX call recordings fails

Email functionality can also be made available to end users to allow them to email time-limited links to recorded calls.

Before these services can be enabled, CallStash must be provided with access to an email service running the standard SMTP protocol. To configure the email service in CallStash click on the settings icon in the top right corner of the admin home page and from the drop down menu click on “Email Server” [Figure 19].

When you save the changes, CallStash will attempt to connect to the service. If this attempt fails then you will be shown an error message and you won’t be able to save the settings. Check that the user name and password, if required, are correct and that you have both the host name of the email service and the port number correct.



Email Server Configuration

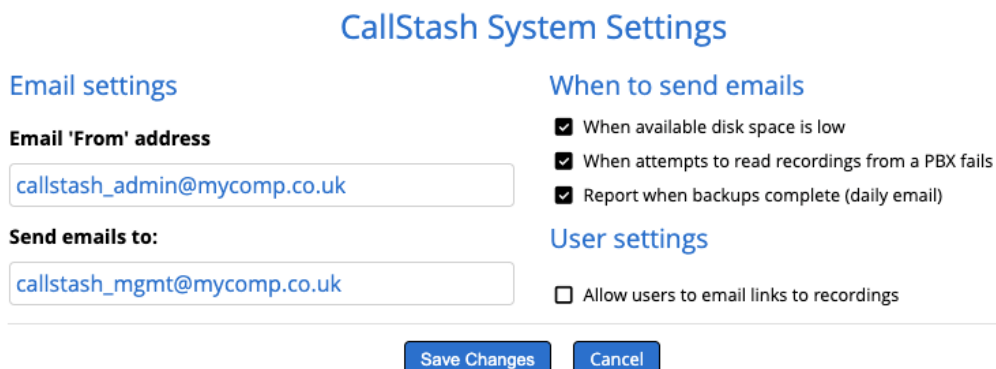
An email server must be configured before email notifications can be enabled.

Email server	Email server user name
<input type="text" value="Host name/IP address"/>	<input type="text" value="User name (optional)"/>
Email server port number	Email server user password
<input type="text" value="IP Port Number (eg 587 or 25)"/>	<input type="text" value="User password (optional)"/>

Figure 19: Adding an email service

9.9 Notifications and Email settings

Once you have correctly configured an email service, click on the cogs (settings) icon to the top right of the screen and select “General Settings” which will show the form in Figure 20. The fields are used as follows:



CallStash System Settings

Email settings	When to send emails
Email 'From' address	<input checked="" type="checkbox"/> When available disk space is low
<input type="text" value="callstash_admin@mycomp.co.uk"/>	<input checked="" type="checkbox"/> When attempts to read recordings from a PBX fails
Send emails to:	<input checked="" type="checkbox"/> Report when backups complete (daily email)
<input type="text" value="callstash_mgmt@mycomp.co.uk"/>	User settings
	<input type="checkbox"/> Allow users to email links to recordings

Figure 20: CallStash system settings

- **From Address:** this will appear in the 'from' field of emails sent from CallStash. **Note:** Some email services will restrict what values can be used in the 'from' field so please check with your email system administrator.
- **Send emails to:** This field only applies to the notifications and not to the emails that are sent by users containing recordings. You can include a list of email recipients, each separated with a comma.
- **When available disk space is low:** If enabled then an email will be sent if the available disk space for any of the monitored disks (audio, database or backup) falls below 10% capacity. This is a critical situation. If the audio storage runs out then CallStash will save no new recordings.
- **When attempts to read recordings from a PBX fails.** This can be for a number of reasons including network connectivity or if the audio disk is full. A failed poll is not generally a problem as long as the issue is resolved rapidly, CallStash will 'catch-up' with missed recordings on the next successful poll.
- **Report when backups complete.** If configured (see §9.10) backups happen every 24 hours. With this option selected CallStash will send an email after each backup cycle has completed. This email will either include statistics from a successful backup or errors if problems were encountered.
- **Allow users to email links to recordings.** With this box enabled end users will be able to send an email containing links to recordings. The links are time limited to a duration chosen by the user sending the email. By default links expire after 12 hours. The user can optionally increase link lifetime to a maximum of 72 hours. There is obviously a security issue around allowing users to email links to voice recordings and so administrators are advised to carry out an appropriate risk assessment before so doing.

9.10 System Backup and Resilience

Responsibility for backups lies with the client and it is highly recommended that a robust backup regime is put in place, especially in the case where call recordings are held for regulatory purposes.

Any backup of CallStash data will include potentially sensitive call recording data. It is important to secure the backup device and to ensure that access to that device is secure.

When installed on a VM infrastructure, clients *may* decide to rely on that infrastructure to replicate and/or backup the mounted VM storage completely independently of CallStash.

As an alternative, CallStash integrates its own backup tools. Two options are provided: Using the `rsync` protocol to backup data to an external storage system; mounting an NFS or iSCSI volume onto the CallStash instance. The latter is currently considered an advanced solution and requires knowledge on how to mount and persist volumes on the host operating system. If CallStash backups have not been configured then the *admin home page* will display a warning.

Backup configuration is available directly from the admin home page by clicking the ‘*Configure backup service*’ button [Figure 12] or via the drop-down settings menu (the *cogs* icon in the top-right of the page).

Choose your backup server carefully. The storage provided must be at least the size of the audio store (see §6.4 for VM installations). Because backup devices can also fail it’s recommended that you choose a product that is resilient to, for example, single disk failures by configuring RAID arrays. The backup system should ideally be located in a separate geographic location from the CallStash instance to prevent failure due to natural disasters such as flooding and fire.

9.10.1 Configuring rsync backups.

The *rsync* protocol is highly efficient, only transferring the minimum data to synchronise the source and target files. A number of NAS devices provide direct support for *rsync* including those from **Synology**, **Asustor** and **NetGear**. You can also backup to many Linux based servers.

CallStash supports only ‘*rsync over ssh*’, which is a secure encrypted backup protocol set.

Click the ‘*Configure backup service*’ button from the admin home page [Figure 12] to show the setup page and select “**Backup:** to remote server” as shown in Figure 21.

The fields in the left hand column identify the server, path and username on the remote system.

The right hand column allows you to choose how to authenticate with the remote server:

- **SSH Keys:** this is the most secure method and is the preferred option. Below the radio button is the CallStash public key. Your remote device will require you to add this key to enable CallStash access.

NOTE: Setup the public key on your NAS or other device *before* clicking ‘*Save*’ on this page. CallStash will attempt to write to the remote server as part of configuration and will report an error if access is not granted.

- **Password:** If you are unable to use public key authentication then you can use password authentication. Select the ‘password’ option on the settings page and enter the password you configured on your remote server.

CallStash - Backup

Configure backup of your call archive.

CallStash uses the common 'rsync' protocol to efficiently replicate the recordings and associated data onto a separate server. This backup can subsequently be used to restore your call archive after a serious system failure.

Backup: ☐ disabled ☐ to local mounted volume ☒ to remote server

Server Identification

Rsync server name. Either the IP address or the server domain name. eg
callstash_backup.mycomp.co.uk

Path on backup server. This path must exist.

User name

Server Authentication

Key authentication is recommended where possible.

Use ☒ SSH Keys ☐ Password

CallStash Public Key

Copy the following value into your NAS device.

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCyFB9egcL0bX0w
59eX8QKMpjslBssW9y40TE9tqkA3PjhRqlokopli1wu3O6W
CKDhIA98UMW+p3E8zNjdRFuaRZ9VaDgunv0ltPP/VoUHY2
OormCbv32Y40ljQcQagZ7CpYUnh+FKjIYdwb+q/zgCd+llfKH
MzhKCU9cULYF6zEnvaNnrPKszv6Xya0uRbCeEVSFivkkbur
ao2DMCl6GziffRU8EFjJbPqdoQ8qUs6G4dU/d2M2BzKQR
LPyMmysS5PvmDoC5bltLv0UMpbVzhH6/RcetDPGUvYj2
9YsqQ9sQYdzDV1AH78vivA8CY8eMogzFVKjJnVWF3+x8jvl
```



NOTE: please set up the above key on your backup device **before** confirming your changes here. CallStash will check access to the device before accepting these settings.

Figure 21: Configure remote server backup

9.10.2 Backup to a locally mounted NFS/iSCSI drive

Note: to use this feature will currently require expert Linux administrator skills. You will need to log in to the CallStash command line, mount your remote disk, create an EXT4 partition and correctly update system files. This manual does not cover that level of technical detail. IPCortex expect to simplify setup for this scenario in a future release.

You will need to correctly mount and persistently mount (via /etc/fstab) your remote disk partition onto the following path:

/var/lib/callstash/backup

Once you've done this reboot the device and then log in to the CallStash admin interface and return to the *backup configuration page* as shown in Figure 21. If you have correctly mounted the backup volume then you'll see "**Backup:** to local mounted volume" as an option which you should select.

If there is no option to use the local disk then the drive has not been correctly mounted.

Select the local mounted volume option and confirm by saving the settings. There are no additional settings required in this scenario.

9.10.3 Backup reporting

If CallStash is configured to run daily backups then the results of backups will be reported in the following ways:

- Via a summary on the admin home page. See Figure 22 for a sample report.
- For locally mounted volumes, the disk will be added to the monitored drives and reported on the admin home page and will generate low disk space email warnings [§9.9]
- If configured, send a daily backup report via email [§9.9]

Backup service operational

Method	Backup to remote rsync server using SSH key authentication
Last backup	2021-09-14 17:52:16
Elapsed time	0.745 seconds
Number of files	3 (reg: 1, dir: 2)
Number of created files	2 (dir: 2)
Number of regular files transferred	0
Total transferred file size	0 bytes
Literal data	0 bytes
Matched data	0 bytes
File list size	0
File list generation time	0.003 seconds
File list transfer time	0 seconds
Total bytes sent	151 bytes
Total bytes received	32 bytes

[Configure backup service](#)

Figure 22: Backup report, admin home page

9.10.4 Replacing the backup target

You may need to replace your backup system, for example for a system with more capacity, with more resilience or because the original system has failed.

Replacing the backup target is straightforward. Simply follow the instructions in the previous sections. The CallStash backup service will automatically copy the entire archive to the new target.

Note that in a system with a lot of archived calls the entire archive will be copied to the new backup. This may take a considerable time depending on your network capabilities and the location of the backup system. This can also place a considerable load on your network and on the CallStash system and so is best done outside of peak hours.

9.11 Bulk export of a company's call recordings

When managing a shared CallStash instance there may be times when one client company wishes to leave the service and obtain a copy of their calls. As outlined in §9.7, recordings for a particular client will be stored in a specific directory. You'll find the location of this on the company admin page, again referenced in §9.7.

Please note that from version 2.3 of the CallStash software, these recordings will be encrypted.

As such the recording files on their own are insufficient and the client will need the keys used to decrypt the recordings.

Call encryption in CallStash is a two part process:

1. Each recording is assigned a random "content encryption key" or CEK. This is used to encrypt the audio file itself using the AES256 algorithm.
2. The CEK is itself then encrypted using the public key of an asymmetric key pair assigned to the company. This yields an encrypted CEK, or eCEK.

To decrypt a recording it is therefore necessary to:

1. Find the eCEK for the call of interest
2. Find the private key for the company that owns the call
3. Decrypt the eCEK using that private key to get the CEK
4. Use the CEK to decrypt the call recording

The client must be provided with both the eCEK for each exported call *and* their private key.

CallStash provides a command line tool to export this additional information.

This is run twice, once to extract the eCEKs and once to extract the private key.

Log in to the CallStash console interface [§5] and then:

```
% cd /opt/ipcortex/callstash
% node ./tools/export-keys --company=target_comp https://my.pbx.com
Encrypted CEKs written to: /tmp/target_comp.keys.csv
% node ./tools/export-keys --mode=private -company=target_comp https://my.pbx.com
Company private key written to: /tmp/target_comp.private.key
% ls -lh /tmp/
total 1432
-rw-r--r--@ 1 root wheel   618K  1 Mar 14:43 target_comp.keys.csv
-rw-r--r--  1 root wheel    1.7K  1 Mar 14:44 target_comp.private.key
%
```

You can see that the two required files are in the 'tmp' directory. These should be given to the client along with the archived call recording files.

9.12 On-Premise RAID Arrays

Our on-premise hardware CallStash product includes a RAID Array for storing audio files. The array provides resiliency against disk failure and increases storage capacity. CallStash software monitors the state of the RAID array and can alert you to failures of any of the disks. A single disk failure will not result in the loss of data however such a disk should be replaced. A second disk failure before the first disk is replaced **will lead to data loss**.

Disk status is made available in two ways:

- Via the admin UI home page
- Through email notifications when disk errors are detected

Note that email notifications are crucial and rely on the correct configuration of the email service [§Error! Reference source not found.].

RAID Status

Disks	sdb	sdc	sdd
Position	0	1	2
Disk OK?	Yes	Yes	Yes

No errors

Figure 23: RAID status

Figure 23 is taken from the admin home page of an on-premise (hardware) CallStash unit. The three disks are shown, and all of the disks are 'OK'. This system is operating correctly.

RAID Status

Disks	sdb	sdc	sdd
Position	0	1	2
Disk OK?	Yes	No	Yes
Disk can be removed	No	Yes	No

The disk array is reporting errors

Please contact your support representative

Figure 24: RAID disk errors

CallStash periodically checks the state of the RAID array and will report errors on the admin home page. Figure 24 shows the case where disk 1 (sdc) is reporting errors. If CallStash has a valid email configuration, administrators will receive an email notification of the disk failure.

In this situation data is secure and there will be no data loss however the failure of another disk will cause loss of call recordings. The faulty disk **must be replaced as soon as possible**.

If disk errors are reported then immediately contact your support representative to arrange a replacement. Once the disk has been delivered contact support and you will be assisted in replacing the disk.

Once the faulty disk has been replaced there will be a period of recovery while the operating system builds the RAID information on the newly added disk. During this time the system will operate correctly, and the admin home page will report repair progress; this is shown in Figure 25.

RAID Status

Disks	sdb	sdc	sdd
Position	0	1	2
Disk OK?	Yes	Yes	Yes

Repair progress: 11%

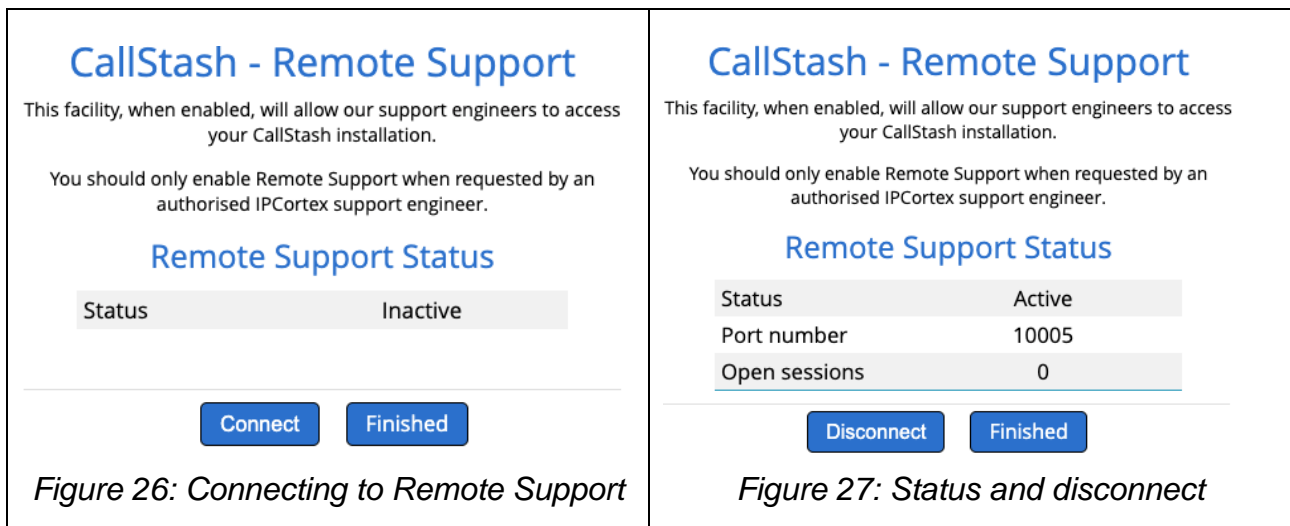
Figure 25: RAID array repair progress

10 Support

There may be times where IPCortex support staff need access to your CallStash instance. You will be asked to “Start the remote support service” or ‘RST’. RST opens a secure, encrypted ‘tunnel’ to IPCortex servers that we can use to access, diagnose and manage your system.

10.1 Starting RST from the Web UI

The usual way to start RST is to click on the ‘cogs’ icon on the Web interface and then click on “Remote Support”. From here [Figure 26] you can “Connect” [Figure 27], see the status and disconnect.



This page will continually update the status of the connection. Once our support staff have finished with the connection it can be closed down from this page.

10.2 Starting RST from the command line

Depending on the issue you’re experiencing it may not be possible to launch the remote support tool from the web UI. For example, if the web interface is unable to run. If this happens then our support engineers will ask you to start the tool from the command line. You will need to:

- Connect to your CallStash system via the console [§5]
- Log in using the root password you created during system configuration [§6.3].
- Run the commands:


```
cd /opt/ipcortex/callstash
sudo -u callstash node ./tools/rst.js connect
```

When it's time to disconnect simply run:

- `sudo -u callstash node ./tools/rst.js disconnect`

11 Software updates

NOTE: Upgrading CallStash will result in an interruption of service for both administrators and end users. It is highly recommended that upgrades are performed outside of core office hours.

IPCortex may periodically release updated CallStash software.

Software updates are available to CallStash customers with an active support contract.

A check for updates is made each day and if available will be displayed on the admin home page. A manual check for updates can be made from the same page. See Figure 28 for the standard admin home page. Click the “Check for Upgrades” button to force an immediate check.

CallStash - Admin

CallStash Enabled PBXs

ID	Name	URL	State	Actions
110	My Company Calls	pbx.mycompany.co.uk	Active	manage companies

Add PBX

Disk usage

Name	Size	Available	Used
audio	1T bytes	716G bytes	30.07%
database	30G bytes	24G bytes	20.25%

System Information

Serial number	12100006
Activated	2021-05-04
Support expires	2021-12-31

Check for Upgrades

Figure 28 Admin Home Page - no upgrade available

If there is an upgrade available then this will also be displayed on the admin home page along with a “Start Upgrade” button, as shown in Figure 29.

CallStash - Admin

CallStash Enabled PBXs

ID	Name	URL	State	Actions
110	My Company Calls	pbx.mycompany.co.uk	Active	manage companies

Add PBX

Disk usage

Name	Size	Available	Used
audio	1T bytes	716G bytes	30.07%
database	30G bytes	24G bytes	20.25%

System Information

Serial number	12100006
Activated	2021-05-04
Support expires	2021-12-31

Upgrade available: 2.0.25

Start Upgrade

Figure 29 Admin Home Page - upgrade ready to be installed

12 How To

This section summarises specific tasks and points you to the right section in this manual.

- **Add a new PBX**
From the Admin Home Page, click 'Add PBX' and reference section [§9.4]
- **Configure a PBX for CallStash**
See section [§8]
- **The storage volume attached to CallStash VM isn't recognised during configuration**
The volume will only be used if it has not already been partitioned. Complete the rest of setup, check the disk configuration and if necessary attach a new, unused/unpartitioned virtual disk. You can then attach this to CallStash using the `callstash-config` utility [§6.5]
- **Archive calls for an additional company in a multi-company PBX**
CallStash polls the companies that the configured PBX admin user can manage. To poll an additional company simply add that company to the managed list on the PBX [§8.1].
- **Stop archiving calls for one company in a multi-company PBX**
CallStash polls the companies that the configured PBX admin user can manage. To stop polling a company simply remove that company from the managed list on the PBX [§8.1].
- **Archive calls from more than one PBX**
CallStash can archive calls from more than one PBX subject to your purchased license. If your license permits you to archive an additional PBX click the 'Add PBX' button on the *admin home page* [§9.4].
- **Reset the system admin password**
Connect to CallStash via the console interface [§5] and run the commands:

```
cd /opt/ipcortex/callstash  
node ./tools/resetpwd.js sysadmin
```


This will reset the web UI password to 'password'. The next time you try to log as 'sysadmin' you will need to set an appropriate password [§9.2]
- **Upgrading CallStash**
Software upgrades, either for new features or to fix bugs, are made available over the Internet and can be installed from the web admin interface [§11].
- **My SSL certificates are about to expire**
Let's Encrypt certificates should automatically renew however ensure that port 80 on CallStash is accessible from the Internet. Self-installed certificates can be updated in the same way they are initially installed [§7.2].
- **Limit how long calls are archived for an individual company**
You can set this value on a per company basis from the company management page. See §9.7
- **Delete all recordings for a company** (multi-company configuration)
For example when a client leaves a partner's hosted service and a copy of archived calls are required. See §9.7
- **How to delete a company** (multi-company configuration)

This might be because a client is leaving a hosted service and all calls and associated data must be deleted from the system. To delete a company it must first **be suspended** by removing it from the managed company list [§8.1] and then marking it for deletion [§9.6]

- **My on-premise CallStash is reporting disk errors**

Your CallStash hardware maintains a RAID array for data storage. This distributes data across a set of three disks such that the failure of an individual disk will not cause loss of data. If you receive an email warning of a faulty disk, or notice such a status on the admin home page **contact your support representative at your earliest opportunity** [§9.12].