

Hiptest on-premises - Installation guide

Owner: Hiptest	Version: 1.4.3	Released: 2017-01-27
Author: Hiptest	Contributors:	
Module: Hiptest enterprise	ID:	Link:

Summary

This guide details the installation and administration of Hiptest Enterprise solution for a single server installation with internet access. It applies to Hiptest Enterprise 1.1.1.0 and beyond.

© 2017 [Hiptest](#)

Created by DocGen 2.1.3 on 27/01/2017 at 10:51:39.

Table of Contents

Table of Contents	2
Overview	6
Requirements	7
Hardware	7
Operating system	7
Network configuration	7
License file (.rli)	7
Easy Installation with Internet Access	8
Install the on-premises solution	8
Access the on-premises administration console	8
Provide a hostname and an SSL certificate	9
Upload your Hiptest license	9
Secure the administration console	10
Preflight checks	11
Configure your Hiptest instance	12
Hostname	12
Default account	12
Email Server Settings	13
Advanced settings	14
Boot Hiptest	15
Open Hiptest	16
Airgap Installation without Internet Access	17
Prepare the environment	17
Install Replicated	17
Download Hiptest Airgap Package	17
Access the on-premises administration console	18
Provide a hostname and an SSL certificate	19
Use airgap package and upload your Hiptest license	19
Secure the administration console	20
Preflight checks	21
Configure your Hiptest instance	22
Hostname	22
Default account	22
Email Server Settings	23
Advanced settings	24
Boot Hiptest	25
Open Hiptest	26
Licensing	27
View License information	27
Synchronizing license	27
Configuration	28
SSL certificates	28
Browser warning about SSL certificates	28

Certificates during installation	28
Certificates and private keys format	29
Modify the certificate of the administration console	29
Self-signed (generated)	29
Server path	29
Upload files	29
Save	29
Modify the certificate of the Hiptest application	29
Use same certificate as the console	30
Use custom certificate	30
Linking JIRA instance to Hiptest	31
Operations	32
Restarting Hiptest on-premises	32
Stopping, starting and getting status	32
Updating server IP address for Replicated 1.2	32
1. Stop all replicated services	33
2. Change IP address in config files	33
3. Regenerate replicated certificate information	34
4. Start replicated service	34
5. Copy replicated certificate to replicated-agent	34
6. Start replicated-agent service	34
7. Start replicated-ui service	34
8. Check that IP address changed in web administration console	34
9. Update IP address of Hiptest service in settings	35
Updating server IP address for Replicated 2.x	36
1. Stop all replicated services	36
2. Change IP address in config files	36
3. Start all replicated services	37
4. Check that IP address changed in web administration console	37
5. Update IP address of Hiptest service in settings	37
Update HTTP Proxy / set HTTP Proxy after install	38
Upgrade	39
Upgrading Replicated	39
Which Replicated version do I use?	39
Upgrade from Replicated v1.2 to Replicated 2.x	39
Upgrade to latest Replicated v2.0	39
Upgrading Hiptest application	40
Upgrading to latest Hiptest application version	40
Airgap Upgrade	42
Download the airgap package	42
Copy the airgap package onto the server	42
Set the path to the airgap package	43
Perform the upgrade	43
Backup & Restore	45
Backup	45

Automatic snapshots	45
Starting a snapshot	46
List snapshots	46
Restore	46
Migrating from Hiptest Cloud	49
Troubleshooting	51
I lost the password of the Hiptest on-premises administration console	51
It hangs when creating a new snapshot.	51
I restored from a snapshot but I lost my data.	51
One user lost his/her password	52
I want to set the password of one user	52
Release notes	53
[1.1.1.0] - 2017-01-04	53
Fixed	53
[1.1.0.0] - 2016-12-27	53
Added	53
Updated	53
Fixed	53
[1.0.0.0] - 2016-10-19	53
Added	53
Fixed	54
Removed	54
[0.9.62.0] - 2016-10-05	54
Added	54
[0.9.61.0] - 2016-09-16	54
Added	54
[0.9.60.1] - 2016-09-14	54
Fixed	54
[0.9.60.0] - 2016-09-14	54
Added	54
[0.9.59.0] - 2016-08-24	54
Added	54
Fixed	54
[0.9.58.0] - 2016-07-22	54
Added	54
Fixed	55
Removed	55
[0.9.57.4] - 2016-07-13	55
Added	55
[0.9.57.3] - 2016-07-11	55
Fixed	55
[0.9.57.2] - 2016-06-24	55
Fixed	55
[0.9.57.0] - 2016-06-02	55
Added	55

Changed	55
Fixed	56
[0.9.56.0] - 2016-05-06	56
Added	56
Changed	56
[0.9.55.0] - 2016-04-22	56
Added	56
Changed	56
[0.9.53.0] - 2016-04-01	56
Added	56

Overview

This guide details the installation and administration of Hiptest Enterprise solution for a single server installation with or without internet access. It applies to Hiptest Enterprise 1.1.1.0 and beyond.

An installation without internet connectivity is called **airgap installation**.

It covers:

- Installation of Hiptest Enterprise,
- Upgrade to newer versions of Hiptest Enterprise,
- Backup & Restore of Hiptest Enterprise data,
- Configuration and troubleshooting,
- Release notes of Hiptest Enterprise.

Requirements

Hardware

The recommended minimum resources of the linux server are:

- 4 cores with minimum 2,4 GHz per core
- 8 GiB of RAM
- Primary disk with minimum 50 GiB

Operating system

The Linux server must run a 64-bits distribution able to run Docker engine 1.12.3. The minimum kernel version is 3.10. Well supported distributions include, but are not limited to:

- Debian 7.7+
- Ubuntu 14.04 / 15.10 / 16.04
- Fedora 21 / 22
- Red Hat Enterprise Linux 6.5+
- CentOS 6+
- Amazon AMI 2014.03 / 2014.09 / 2015.03 / 2015.09 / 2016.03 / 2016.09
- Oracle Linux 6.5+

Network configuration

Firewall/Security settings must allow:

- Inbound traffic for the following TCP ports:
 - 80 Hiptest app interface access, redirects to HTTPS
 - 443 Hiptest app interface access over SSL
 - 8800 Administration console access
- Inbound/Outbound traffic from docker0 interface to the host interface for the following TCP ports:
 - 9870-9880 container orchestration and administration console API

Non-airgap installation requires outbound HTTP/HTTPS Internet access to these domains and subdomains:

- replicated.com for license validation and release update checks
- docker.io for pulling containers from the Docker hub registry

Installation also require following elements:

- DNS hostname where your instance of Hiptest can be reached by your organization. Typically your hostname will look something like `hiptest.YOURCOMPANY.com`.
- SSL certificate matching the chosen DNS hostname. Either provide a PEM encoded certificate file and private key file, or use the provided self-signed certificate. The self-signed certificate is not recommended as browsers will display a security warning.
- SMTP server settings. This includes the type of authentication, the server name and credentials.

License file (.rli)

This license file will be provided by a Hiptest representative prior to installation. If you need a Hiptest license, please contact us at contact@hiptest.net.

Easy Installation with Internet Access

Install the on-premises solution

1. Create a server instance from a supported OS with the resources recommended above.
2. Open an SSH session and login into your new server.
3. Run the following command to download and install the application with an easy installation wizard:

```
curl -sSL https://get.replicated.com/docker | sudo bash
```

If you are installing Hiptest behind a proxy, modify the install commands to export `http_proxy` environment variable as below:

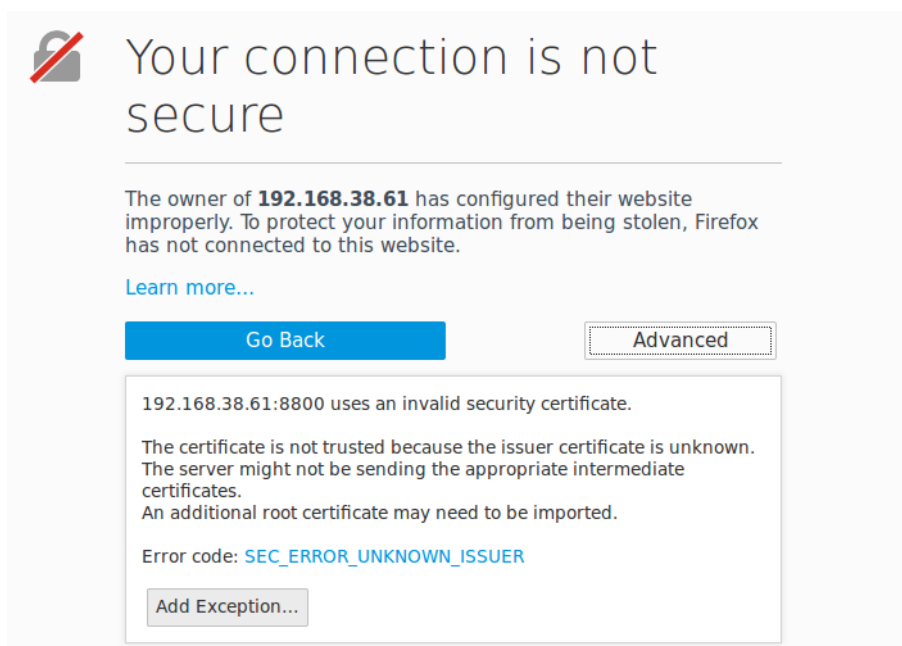
```
export http_proxy=http://login:password@proxy.you-company.com:port/
curl -sSL https://get.replicated.com/docker | sudo -E bash
```

You will be prompted for simple questions through out the installation process if it cannot guess the settings automatically. It will ask for the networking interface to use and the proxy settings. It will then start downloading and installing the administration console application. Then it asks for the service IP address and prompts you to go to the administration console web interface.

Access the on-premises administration console

Open a browser and navigate to the administration console at `https://<server_address>:8800` where `<server_address>` is the name or IP address of the newly created Hiptest server.

The browser will display a security warning because Hiptest on-premises initially uses a self-signed certificate.



Proceed past the HTTPS connection security warning.

Provide a hostname and an SSL certificate

On the presented screen, supply the hostname and a custom SSL certificate for the administration console.

You can choose 'Use Self-Signed Cert' and use the generated self-signed certificate or select 'Upload and Continue' after supplying your own SSL certificate. The certificate and key files must be PEM encoded.

HTTPS for admin console

We're currently using a self-signed TLS certificate to secure the communication between your browser & the management console. If you don't upload your own TLS cert, you'll see a warning about this in your browser every time you access the management console.

Provide Custom SSL Certificate

Hostname (Ensure this domain name resolves to this server & is routable on your network)

Private Key

Certificate

Files will be uploaded directly to the management server & will never leave.
If your private key and cert are already on this server, click [here](#).

Upload your Hiptest license

The Hiptest license file (.rli) has been provided by a Hiptest representative prior to installation.

Upload your license

Click the button below to find and upload your license file.
The file will have a **.rli** extension.

If this server cannot access the internet, you can [install from a local package](#).

Click here →

[Restore from a snapshot](#)

Once uploaded, the license will be validated.

Upload your license

Validating license file...

Secure the administration console

After the license validation is complete, secure the administration console access using a local password, an LDAP user account, or anonymous access (insecure).

Secure the admin console

Keeping this admin console secure is important.

You can create a shared password that will be required to access the settings, or you can connect it to your existing directory based authentication system.

☐ Anonymous ☒ Password ☐ LDAP

Password

Confirm Password

Continue

Local password or LDAP user account is highly recommended.

Preflight checks

The installer will perform some checks to ensure that Hiptest on-premises can be run on this server. Once completed, proceed to next screen by clicking 'Continue'.

Preflight Checks

- ✓ **OS linux is supported**
The operating system must be linux
- ✖ **Linux distribution is supported**
The linux distribution must be one of amzn, centos, debian, fedora, rhel, ubuntu
- ✖ **Kernel version is supported**
Kernel version must be at least 3.10
- ✖ **Memory meets minimum requirement**
Server must have at least 1G total memory
- ✓ **Total space requirement met for directory /tmp**
Directory must have at least 1G total space
- ✓ **Total space requirement met for directory /var/lib/replicated**
Directory must have at least 250M total space
- ✓ **Docker server version requirement met**
Docker server version must be at least 1.7.1 and no greater than 1.11.1
- ✓ **Total space requirement met for directory /var/lib/docker/aufs**
Directory must have at least 10G total space
- ✓ **Successful connection**
Can connect to 192.168.38.200 address
- ✖ **Can connect to address**
Can connect to docker0 address
- ✖ **Can access HTTP address**
Can access api.replicated.com
- ✖ **Can access Docker registry**
Can access registry index.docker.io
- ✓ **Successful Docker registry ping**
Can access registry registry.replicated.com

Node: cfbe7f0f720547...

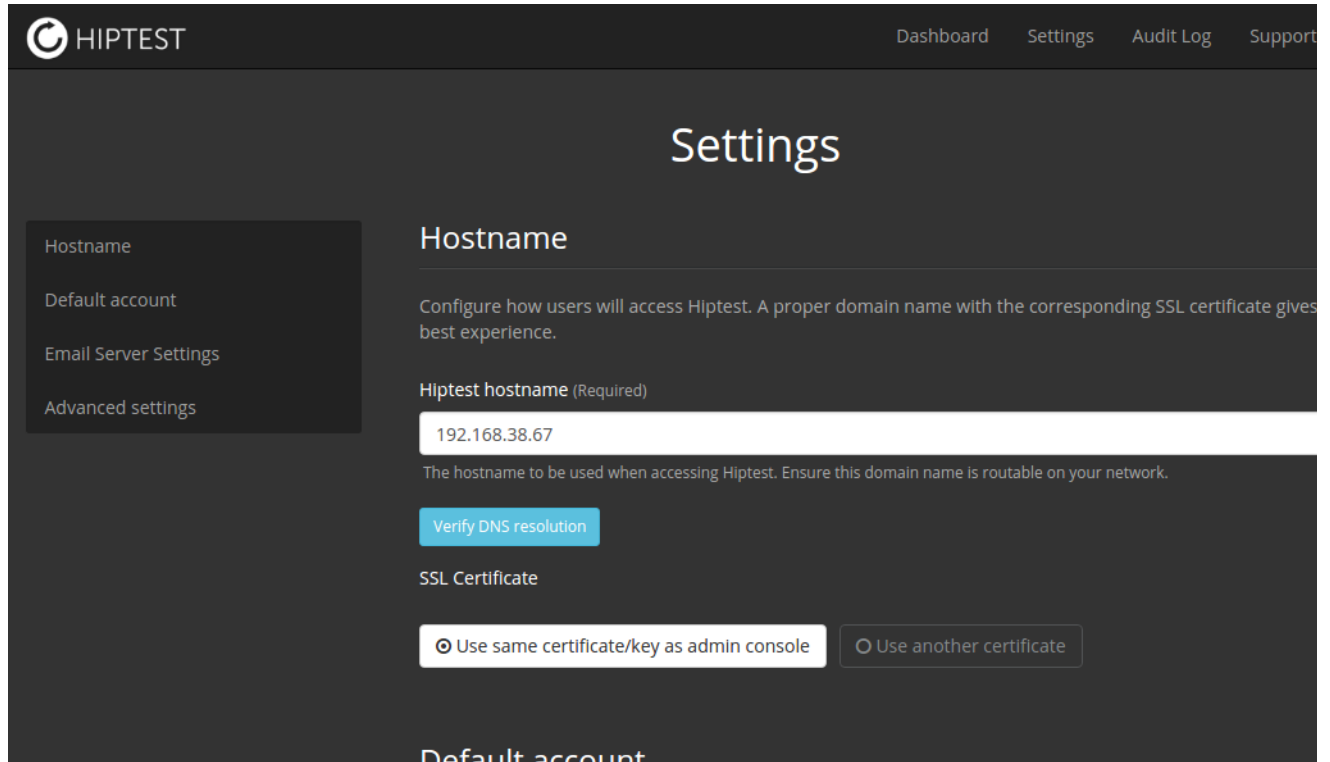
- ✓ **Docker server version requirement met**
Docker server version must be at least 1.7.1 and no greater than 1.11.1

Configure your Hiptest instance

Fill in required settings parameters in the Settings panel. Provide the requested information requested and click "Save" to continue.

Hostname

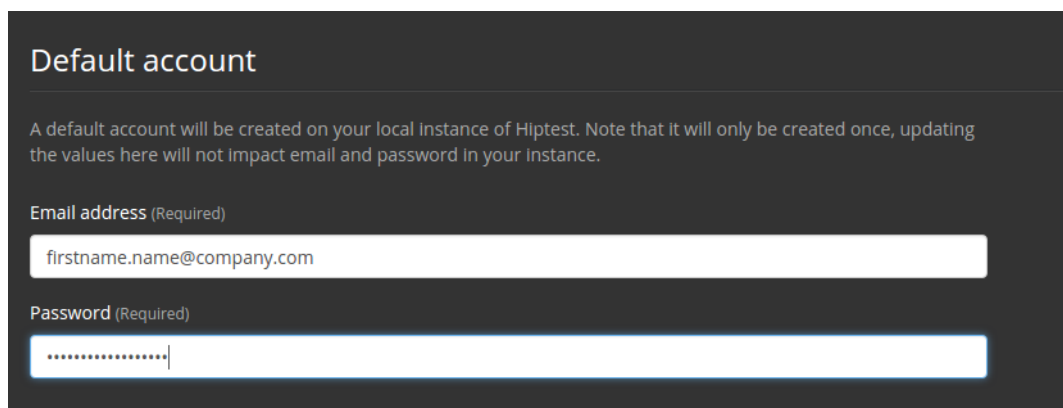
You can use the same hostname and certificate as the administration console, or use a custom one.



The screenshot shows the Hiptest Settings page. The top navigation bar includes the Hiptest logo and links for Dashboard, Settings, Audit Log, and Support. The main heading is "Settings". On the left, there is a sidebar with links for Hostname, Default account, Email Server Settings, and Advanced settings. The "Hostname" section is active. It contains a description: "Configure how users will access Hiptest. A proper domain name with the corresponding SSL certificate gives best experience." Below this, there is a field for "Hiptest hostname (Required)" with the value "192.168.38.67". A note states: "The hostname to be used when accessing Hiptest. Ensure this domain name is routable on your network." There is a "Verify DNS resolution" button. Below that, the "SSL Certificate" section has two radio buttons: "Use same certificate/key as admin console" (which is selected) and "Use another certificate".

Default account

The default account will be the first account created on Hiptest. You will use this account the first time you login to Hiptest.



The screenshot shows the "Default account" settings page. It has a heading "Default account" and a description: "A default account will be created on your local instance of Hiptest. Note that it will only be created once, updating the values here will not impact email and password in your instance." Below this, there are two fields: "Email address (Required)" with the value "firstname.name@company.com" and "Password (Required)" with a masked password ".....".

Email Server Settings

This section allows to configure the email server. If you skip this step, the users won't receive notifications and invitation by email.

Email Server Settings

Define outgoing email settings to be able to send invitations email from Hiptest.

☒ Configure outgoing email server settings

SMTP Host Address and Port (Required)

The hostname and port of your SMTP server, like so: `server:port`

From Address (Required)

The from address that will be used in Hiptest outgoing emails

SMTP Authentication Type

☒ None
 ☐ CRAM-MD5
 ☐ Login
 ☐ Plain

SMTP Encryption

☒ Enable STARTTLS (Recommended)
 ☐ Disable STARTTLS

Please note that the "Verify SMTP Authentication Settings" check does not work when SMTP Authentication is set to "None"

Advanced settings

If you check the box "Display internal settings", you will be able to modify the internal settings. You may only need to change them for troubleshooting. Be sure to know what you are doing.

You can change:

- Frontend HTTP port
- Frontend HTTPS port
- Database port

You can also disable SSL. By default, Hiptest will always enforce SSL and https usage, but the SSL handling can be offloaded to your own SSL terminator proxy. The proxy must be in front of Hiptest, handle the SSL connections and forward them to Hiptest. To use this configuration, uncheck this setting so that Hiptest only listens for connections on its frontend http port and does not listen on https port. In this case, be sure to have HTTP header "X-Forwarded-Proto: https" in forwarded HTTP requests.

By default, Hiptest binds http and https to all interfaces of the server. When adding a reverse proxy in front of Hiptest, you might want to bind these ports on the docker0 interface so they can only be reached locally.

Advanced settings

These settings are set upon installation. You may only need to change them for troubleshooting.

☒ Display internal settings

You have to check this box to display the internal settings and modify them. Be sure to know what you are doing.

Frontend HTTP port

The port used by Hiptest to serve HTTP requests. Defaults to 80. Change it if it conflicts with other services installed on the server.

Frontend HTTPS port

The port used by Hiptest to serve HTTPS requests using SSL. Defaults to

1. Change it if it conflicts with other services installed on the server.

☒ Enable SSL for Hiptest

Hiptest will always enforce SSL and https usage, but the SSL handling can be offloaded to your own SSL terminator proxy. The proxy must be in front of Hiptest, handle the SSL connections and forward them to Hiptest. To use this configuration, uncheck this setting so that Hiptest only listens for connections on its frontend http port and does not listen on https port.

Be sure to have HTTP header `X-Forwarded-Proto: https` in forwarded HTTP requests.

Database port

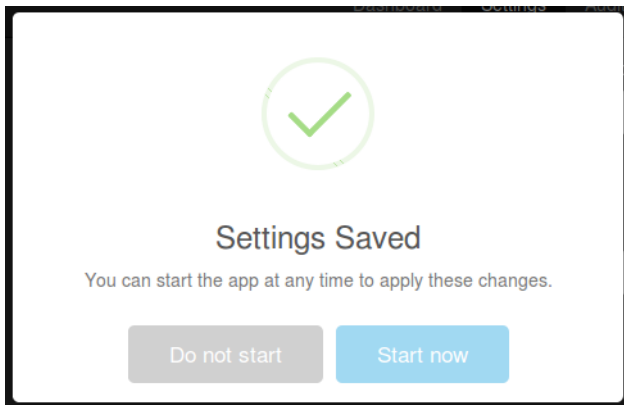
The port used by the PostgreSQL database used by Hiptest. Defaults to 5432. Change it if it conflicts with other services installed on the server.

☐ Bind frontend ports to docker0 interface

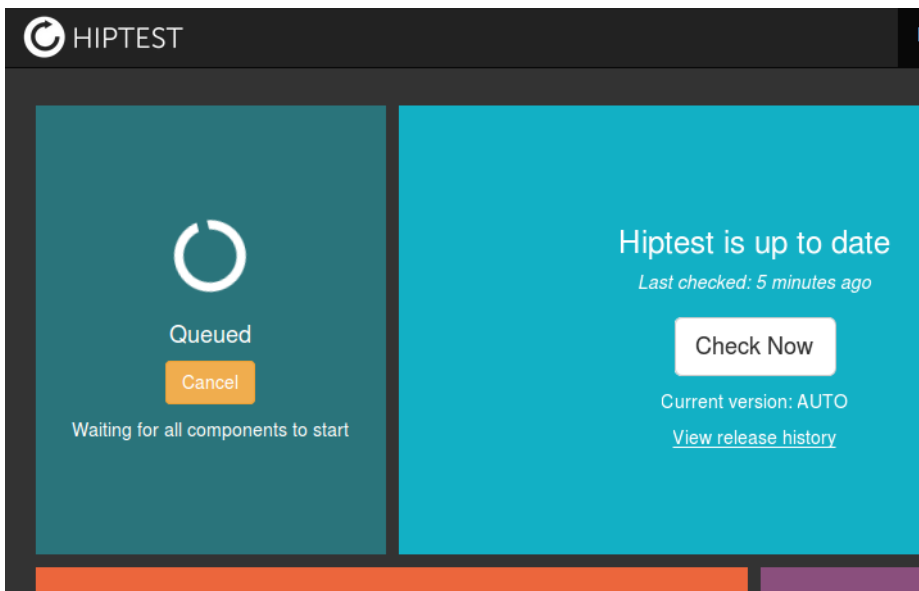
Hiptest binds http and https to all interfaces of the server by default. When adding a reverse proxy in front of Hiptest, you might want to bind these ports on the docker0 interface so they can only be reached locally.

Next, click "Save" to continue.

Boot Hiptest



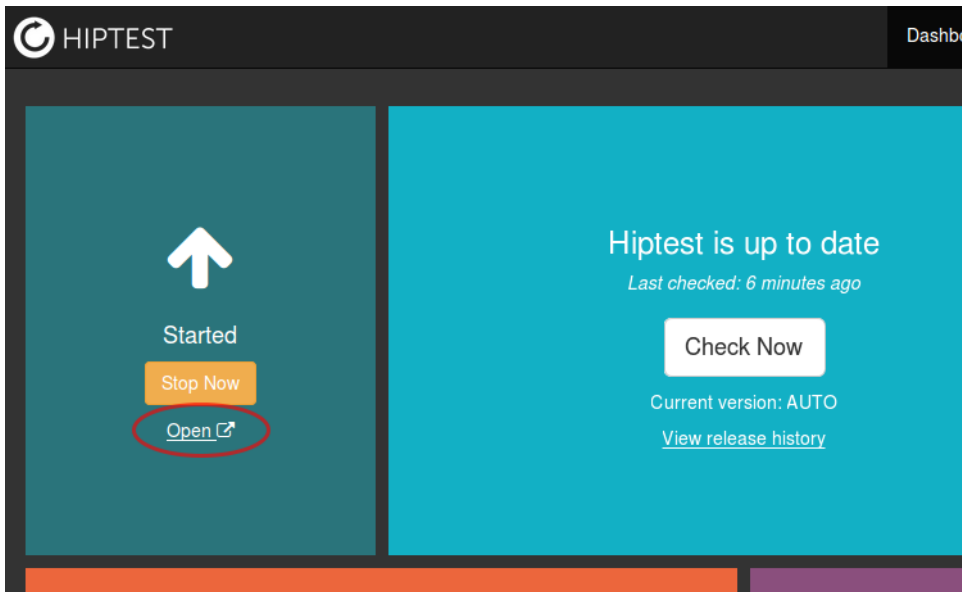
Once settings are saved, click "Start Now" to boot Hiptest. You will be taken to the dashboard of the Hiptest Management Interface while the instance boots up.



While booting, containers must be downloaded and it can take some time to complete depending on your connection speed. Please be patient.

Open Hiptest

Once the instance has finished booting, an "open" link will appear on the far left side. Click "open" to launch Hiptest in a new browser window.



Airgap Installation without Internet Access

Prepare the environment

Create a server instance from a supported OS with the resources recommended above.

Install a supported version of Docker. Installing a supported version of Docker on a server that does not have any internet access is a simple process, but it can require you to install a few dependencies. Most airgapped environments will still have access to yum and apt, but they will be pointing to local mirrors.

The supported Docker versions range from 1.7.1 to 1.10.3. We recommend that you use the latest version of Docker available in this range for your operating system. Locate and download the desired package of Docker from one of the official repositories:

OS	Repository location	Highest Docker Version Supported
CentOS 7 / RHEL 7	http://yum.dockerproject.org/repo/main/centos/7/Packages/	1.11.1
Ubuntu 12.04 (precise) / 14.04 (trusty) / 15.10 (wily)	https://apt.dockerproject.org/repo/pool/main/d/docker-engine/	1.11.1
Fedora 22	http://yum.dockerproject.org/repo/main/fedora/22/Packages/	1.11.1
Debian 7 (Wheezy) / 8 (Jessie)	https://apt.dockerproject.org/repo/pool/main/d/docker-engine/	1.11.1
Ubuntu 15.04 (vivid)	https://apt.dockerproject.org/repo/pool/main/d/docker-engine/	1.9.1
Fedora 21	http://yum.dockerproject.org/repo/main/fedora/21/Packages/	1.9.1
CentOS 6 / RHEL 6	http://yum.dockerproject.org/repo/main/centos/6/Packages/	1.7.1
Ubuntu 14.10 (utopic)	https://apt.dockerproject.org/repo/pool/main/d/docker-engine/	1.7.1

Once the correct package has been downloaded and transferred to the airgapped machine you need to install it using one of the following commands:

rpm:

```
# CentOS/RHEL/Fedora
$ sudo rpm -ivh <package_name>.rpm
```

dpkg:

```
# Ubuntu / Debian
$ sudo dpkg --install <package_name>.deb
```

Different versions of Docker require different dependencies that may have to be manually downloaded/transferred/installed to the airgapped machine. You will have to follow the same procedure for each one of those dependencies.

Install Replicated

Hiptest on-premises is provided through Replicated technology. Replicated software must be downloaded and installed on the server.

Download latest Replicated release from <https://s3.amazonaws.com/replicated-airgap-work/replicated.tar.gz> and run the following commands:

```
tar xzvf replicated.tar.gz
cat ./install.sh | sudo bash -s airgap
```

Installer will ask if the machine requires a proxy to access the internet. You can safely ignore the question and press Enter. The installer will proceed and prompt you to visit the address `https://<this_server_address>:8800`. We will download the Hiptest airgap package first, and then go back to this URL to go on with installation.

Download Hiptest Airgap Package

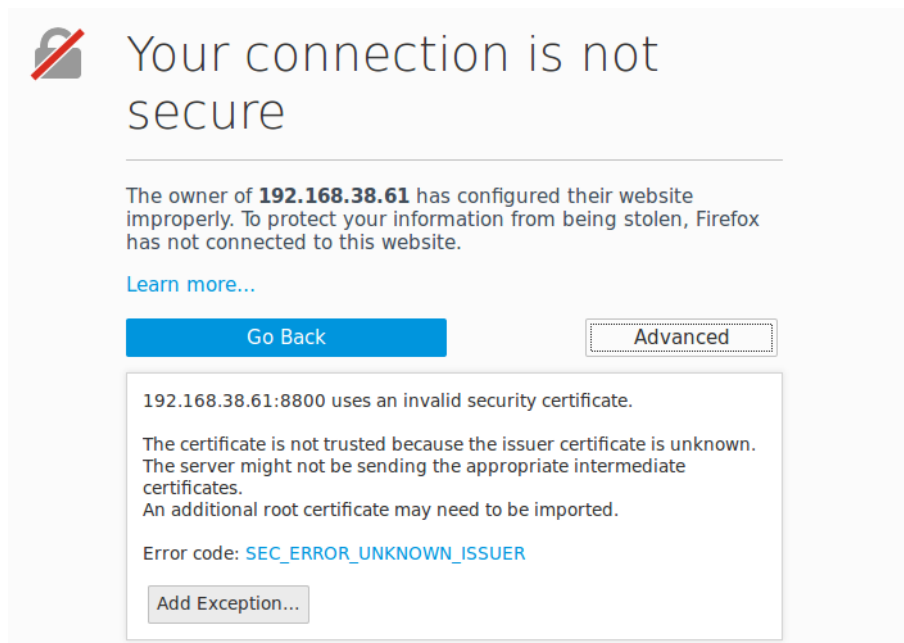
You have been provided a download link and a password to access Hiptest airgap packages. Use the download link to access a password protected page. Enter the provided password to see a page listing Hiptest releases. Choose the latest release and click its download icon to download it. Package size is around 1.5 GiB.

Copy this package on your server, it will be needed in further steps.

Access the on-premises administration console

Open a browser and navigate to the administration console at `https://<server_address>:8800` where `<server_address>` is the name or IP address of the newly created Hiptest server.

The browser will display a security warning because Hiptest on-premises initially uses a self-signed certificate.

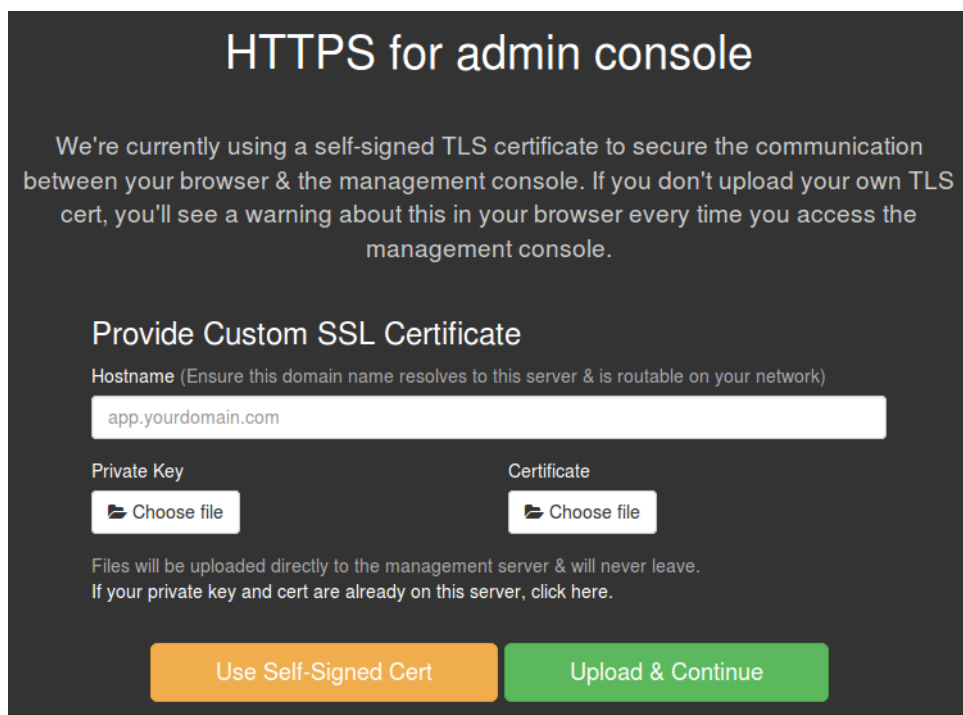


Proceed past the HTTPS connection security warning.

Provide a hostname and an SSL certificate

On the presented screen, supply the hostname and a custom SSL certificate for the administration console.

You can choose 'Use Self-Signed Cert' and use the generated self-signed certificate or select 'Upload and Continue' after supplying your own SSL certificate. The certificate and key files must be PEM encoded.



HTTPS for admin console

We're currently using a self-signed TLS certificate to secure the communication between your browser & the management console. If you don't upload your own TLS cert, you'll see a warning about this in your browser every time you access the management console.

Provide Custom SSL Certificate

Hostname (Ensure this domain name resolves to this server & is routable on your network)

app.yourdomain.com

Private Key Choose file

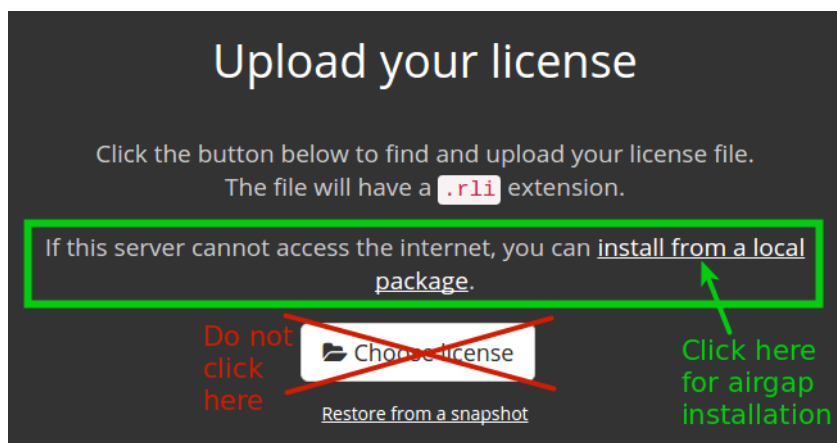
Certificate Choose file

Files will be uploaded directly to the management server & will never leave.
If your private key and cert are already on this server, click here.

Use Self-Signed Cert Upload & Continue

Use airgap package and upload your Hiptest license

On next screen, you are prompted to upload your license file or to install from a local package if the server cannot access the internet.



Upload your license

Click the button below to find and upload your license file.
The file will have a **.rli** extension.

If this server cannot access the internet, you can install from a local package.

Do not click here ~~Choose license~~ Restore from a snapshot Click here for airgap installation

Click on the 'install from a local package' link. You are prompted to specify the absolute path to the airgap package you saved on this server earlier. You must also upload the license file that Hiptest provided you.

Install from local package

To install from an offline package, you will need to specify a path (from this server) to the downloaded installer, and also your license file.

[< Back](#)

Supply the requested information and click 'Continue'. The airgap package will be extracted and validated.

Install from local package

Extracting and validating the archive. This may take a minute.

Secure the administration console

After the airgap package is extracted and the license validation is complete, secure the administration console access using a local password, an LDAP user account, or anonymous access (insecure).

Secure the admin console

Keeping this admin console secure is important.

You can create a shared password that will be required to access the settings, or you can connect it to your existing directory based authentication system.

☐ Anonymous
 ☒ Password
 ☐ LDAP

Password

Confirm Password

Local password or LDAP user account is highly recommended.

Preflight checks

The installer will perform some checks to ensure that Hiptest on-premises can be run on this server. Once completed, proceed to next screen by clicking 'Continue'.

Preflight Checks

- ✓ **OS linux is supported**
The operating system must be linux
- ✓ **Distribution Ubuntu is supported**
The linux distribution must be one of amzn, centos, debian, fedora, rhel, ubuntu
- ✓ **Kernel version requirement met**
Kernel version must be at least 3.10
- ✓ **Memory requirement met**
Server must have at least 1G total memory
- ✓ **Total space requirement met for directory /tmp**
Directory must have at least 1G total space
- ✓ **Total space requirement met for directory /var/lib/replicated**
Directory must have at least 250M total space
- ✓ **Docker server version requirement met**
Docker server version must be at least 1.7.1 and no greater than 1.11.1
- ✓ **Total space requirement met for directory /var/lib/docker/aufs**
Directory must have at least 10G total space
- ✓ **Successful connection**
Can connect to 192.168.38.67 address
- ✓ **Successful connection**
Can connect to docker0 address

Node: 8818f9b455514...

- ✓ **Docker server version requirement met**
Docker server version must be at least 1.7.1 and no greater than 1.11.1

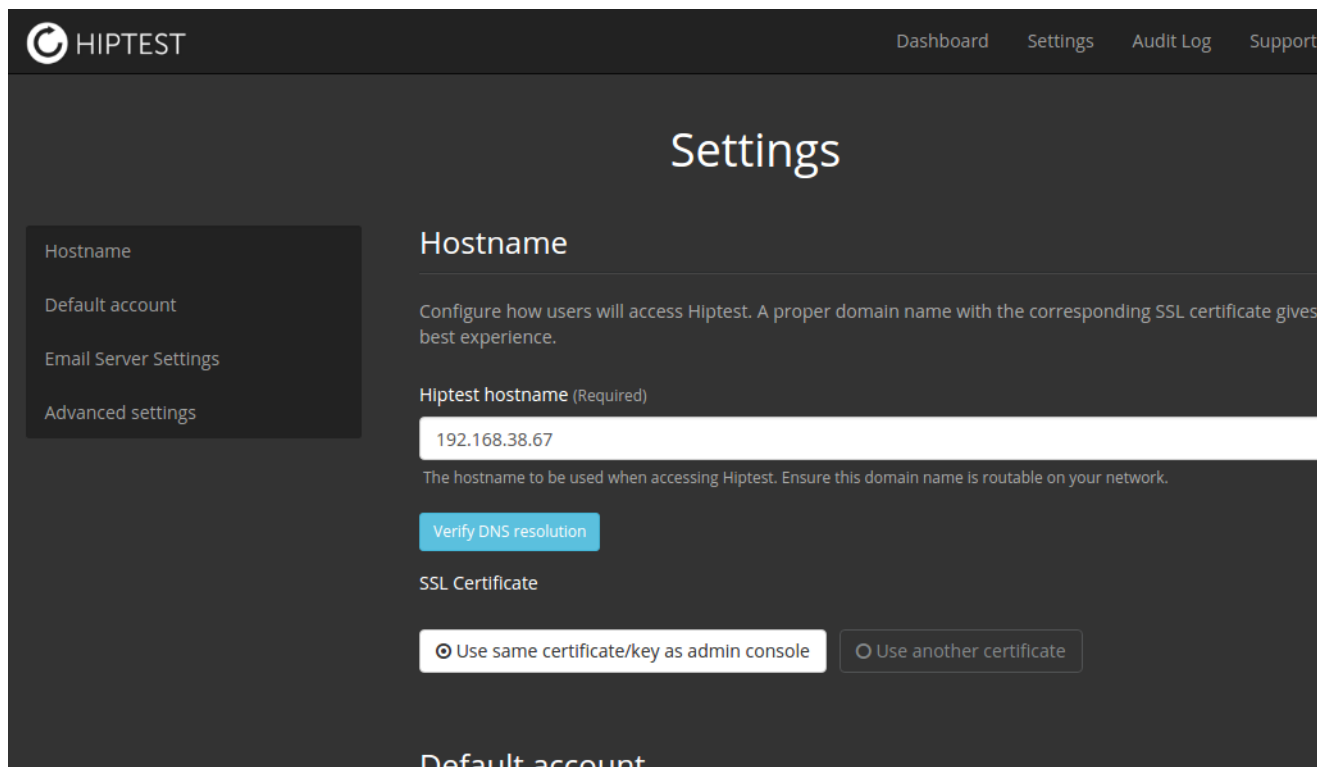
Continue

Configure your Hiptest instance

Fill in required settings parameters in the Settings panel. Provide the requested information requested and click "Save" to continue.

Hostname

You can use the same hostname and certificate as the administration console, or use a custom one.

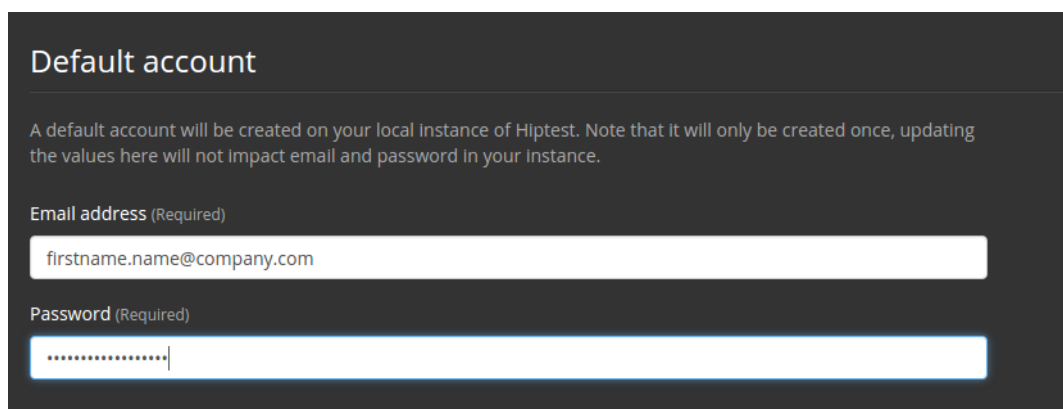


The screenshot shows the Hiptest Settings page. The top navigation bar includes the Hiptest logo and links for Dashboard, Settings, Audit Log, and Support. The main heading is "Settings". On the left, there is a sidebar with links for Hostname, Default account, Email Server Settings, and Advanced settings. The "Hostname" section is active. It contains a description: "Configure how users will access Hiptest. A proper domain name with the corresponding SSL certificate gives best experience." Below this, there is a field for "Hiptest hostname (Required)" with the value "192.168.38.67". A note states: "The hostname to be used when accessing Hiptest. Ensure this domain name is routable on your network." There is a "Verify DNS resolution" button. Below that, the "SSL Certificate" section has two radio buttons: "Use same certificate/key as admin console" (which is selected) and "Use another certificate".

Provide the requested information requested and click "Save" to continue.

Default account

The default account will be the first account created on Hiptest. You will use this account the first time you login to Hiptest.



The screenshot shows the "Default account" settings page. It has a heading "Default account" and a description: "A default account will be created on your local instance of Hiptest. Note that it will only be created once, updating the values here will not impact email and password in your instance." Below this, there are two required fields: "Email address (Required)" with the value "firstname.name@company.com" and "Password (Required)" with a masked password ".....".

Email Server Settings

This section allows to configure the email server. If you skip this step, the users won't receive notifications and invitation by email.

Email Server Settings

Define outgoing email settings to be able to send invitations email from Hiptest.

☒ Configure outgoing email server settings

SMTP Host Address and Port (Required)

The hostname and port of your SMTP server, like so: `server:port`

From Address (Required)

The from address that will be used in Hiptest outgoing emails

SMTP Authentication Type

☒ None
 ☐ CRAM-MD5
 ☐ Login
 ☐ Plain

SMTP Encryption

☒ Enable STARTTLS (Recommended)
 ☐ Disable STARTTLS

Please note that the "Verify SMTP Authentication Settings" check does not work when SMTP Authentication is set to "None"

Advanced settings

If you check the box "Display internal settings", you will be able to modify the internal settings. You may only need to change them for troubleshooting. Be sure to know what you are doing.

You can change:

- Frontend HTTP port
- Frontend HTTPS port
- Database port

You can also disable SSL. By default, Hiptest will always enforce SSL and https usage, but the SSL handling can be offloaded to your own SSL terminator proxy. The proxy must be in front of Hiptest, handle the SSL connections and forward them to Hiptest. To use this configuration, uncheck this setting so that Hiptest only listens for connections on its frontend http port and does not listen on https port. In this case, be sure to have HTTP header "X-Forwarded-Proto: https" in forwarded HTTP requests.

By default, Hiptest binds http and https to all interfaces of the server. When adding a reverse proxy in front of Hiptest, you might want to bind these ports on the docker0 interface so they can only be reached locally.

Advanced settings

These settings are set upon installation. You may only need to change them for troubleshooting.

☒ Display internal settings

You have to check this box to display the internal settings and modify them. Be sure to know what you are doing.

Frontend HTTP port

The port used by Hiptest to serve HTTP requests. Defaults to 80. Change it if it conflicts with other services installed on the server.

Frontend HTTPS port

The port used by Hiptest to serve HTTPS requests using SSL. Defaults to

1. Change it if it conflicts with other services installed on the server.

☒ Enable SSL for Hiptest

Hiptest will always enforce SSL and https usage, but the SSL handling can be offloaded to your own SSL terminator proxy. The proxy must be in front of Hiptest, handle the SSL connections and forward them to Hiptest. To use this configuration, uncheck this setting so that Hiptest only listens for connections on its frontend http port and does not listen on https port.

Be sure to have HTTP header `X-Forwarded-Proto: https` in forwarded HTTP requests.

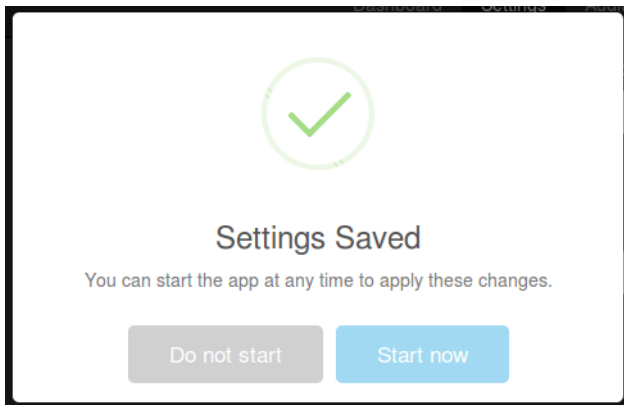
Database port

The port used by the PostgreSQL database used by Hiptest. Defaults to 5432. Change it if it conflicts with other services installed on the server.

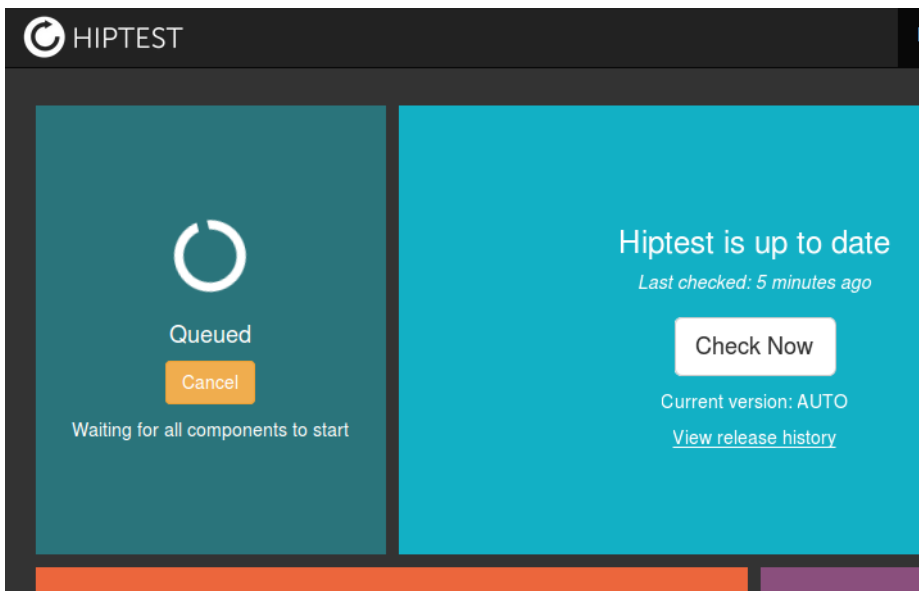
☐ Bind frontend ports to docker0 interface

Hiptest binds http and https to all interfaces of the server by default. When adding a reverse proxy in front of Hiptest, you might want to bind these ports on the docker0 interface so they can only be reached locally.

Boot Hiptest



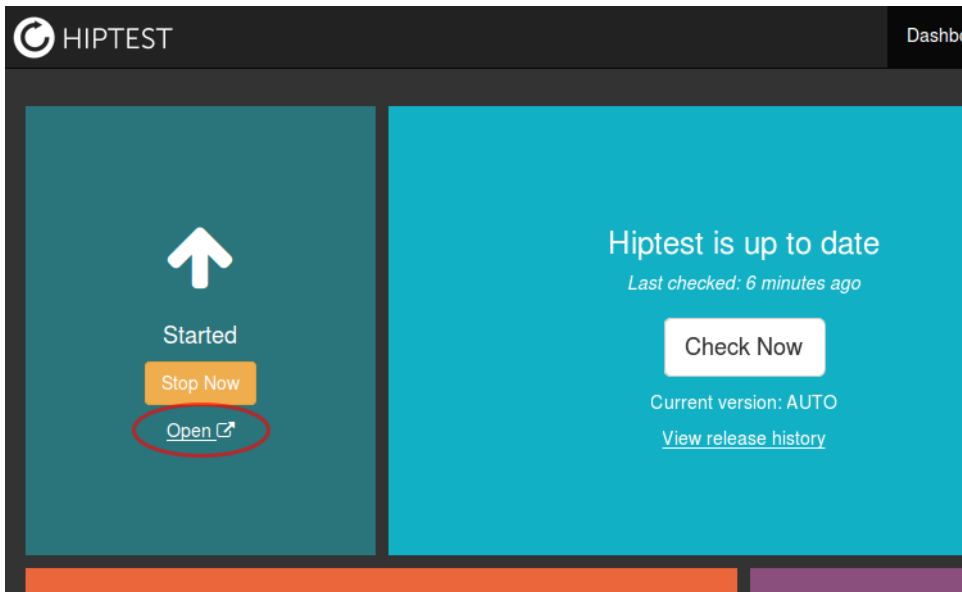
Once settings are saved, click "Start Now" to boot Hiptest. You will be taken to the dashboard of the Hiptest Management Interface while the instance boots up.



Note that features to check for Hiptest updates or to synchronize licence are inoperant as this is an airgap installation.

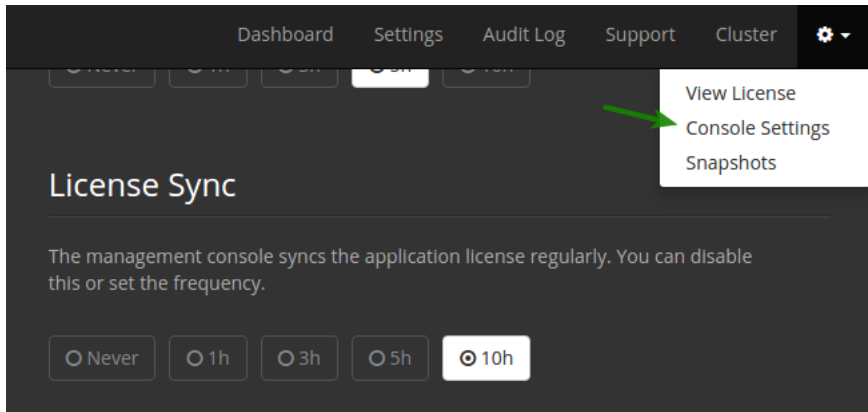
Open Hiptest

Once the instance has finished booting, an "open" link will appear on the far left side. Click "open" to launch Hiptest in a new browser window.



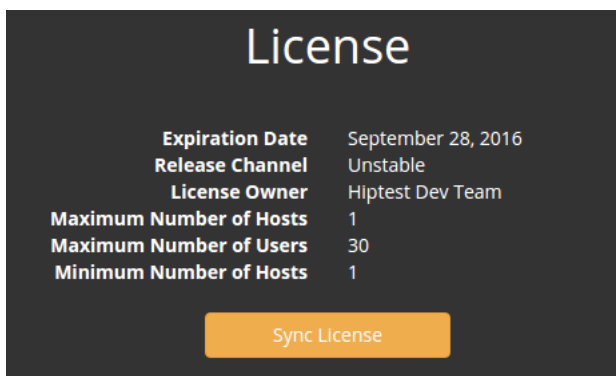
Licensing

The license for Hiptest on-premises usage is automatically synchronized online on a regular basis. This is set to synchronize every 10 hours by default. This can be changed in the console settings:



View License information

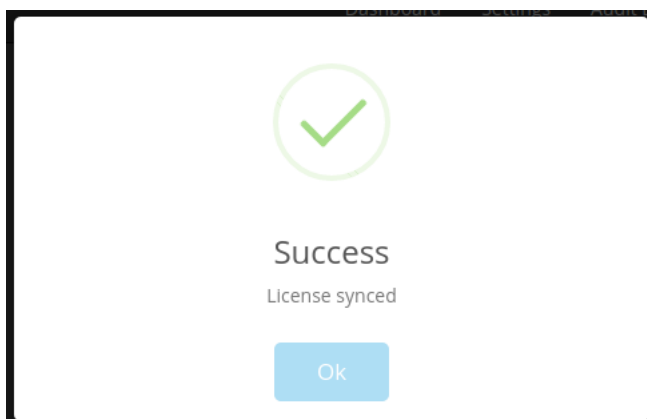
You can view license information from the cog menu, under the "View License" menu item.



The license defines the maximum number of users you can have on Hiptest, and also the period of validity of the license. When the license expires, the service stops and can not be restarted. The administration console is still available. After a payment, the license gets updated and you can start Hiptest again.

Synchronizing license

To update your license information immediately, you can click the "Sync License" button. It will connect to our backend and retrieve the license information defined for you. A message is displayed once the license is updated.



Configuration

SSL certificates

SSL certificates are used to secure the connection when accessing to the administration console or the Hiptest application.

Browser warning about SSL certificates

In the case of web http servers, SSL Certificates are small data files that binds a cryptographic key to one or multiple hostnames. It enables the use of the https protocol and allow secure connections.

These certificates are signed by a certificate authority (CA) that guarantees the link between the issued certificate, the owner of the certificate and the hostname. Each CA has its own certificate which can be signed by another CA certificate. The top-most CA is called the Root CA. The certificate of a Root CA is self-signed.

All browsers have a list of trusted certificate authorities and they will trust the information contained in any certificate issued by these trusted certificate authorities.

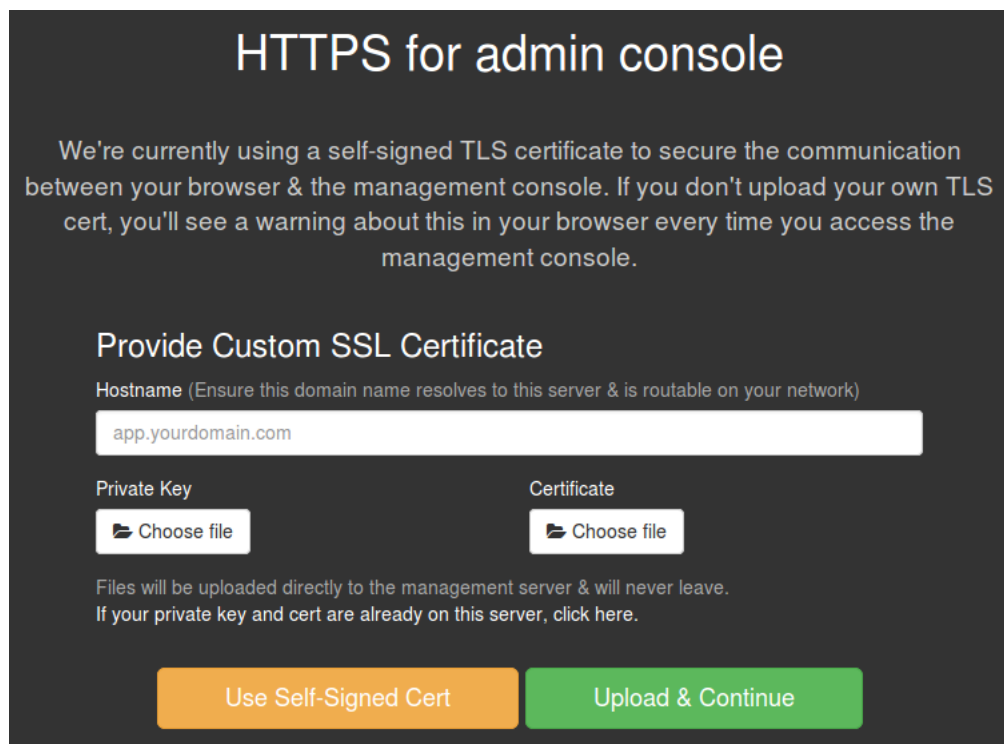
In the case of self-signed certificates, there is no CA to be trusted, so the browser displays a warning because it can't trust the connection.

Also if the hostname from the certificate does not match the hostname the browser is connecting to, the browser will display a warning too.

So to prevent browser warnings, you must use a certificate issued by a certificate authority trusted by your browser and having a hostname that matches your server hostname.

Certificates during installation

At installation, a local certificate authority is created and a certificate signed by this authority is issued. This self-signed certificate is valid for the public IP address prompted on the console during installation. Then this certificate is used on the first web console page:



On this screen, you can choose to use your own certificate or generate a self-signed one. The hostname must be entered and must resolve to the same IP address you are using to access the administration console. This hostname must also be routable on your network.

If you click "Use Self-Signed Cert", then a new certificate will be issued from the local certificate authority with the given hostname and the browser page will be refreshed to use this new certificate.

Note: if you use the IP address as hostname, then no new certificate will be issued.

You can also provide your own certificate and key pair. They can be uploaded to the server or you can specify the full path if they are already stored on the server. In any case, the CN of the uploaded certificate must match the hostname specified. Click "Upload & Continue" button and the browser

page will be refreshed to use the provided certificate.

Certificates and private keys format

The format used must be PEM. This is a Base64-encoded structure starting and ending with a header, like so:

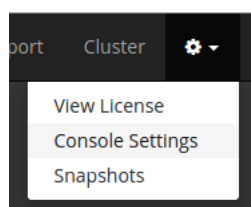
```
-----BEGIN CERTIFICATE-----
MIIFmzCCA40gAwIBAgIJAMprPVN0fZbHMA0GCSqGSIb3DQEBCwUAMGQxCzAJBgNV
BAYTAkZSMQ8wDQYDVQQIDAZGcmFuY2UxETAPBgNVBACMCEJlc2FuY29uMRAdBgYD
[...]
+89xL5jL/WctokA9TLqQ1rr68U2erk6PYZMFndI+CqKEPp9CCChHxIA6yrTo3Fwo2
r2WnBStgRQNK5FNT7p1aaEECH8fke41KLrntuFGHo35YS4mSFDZtqw87+7VkhY=
-----END CERTIFICATE-----
```

The header is -----BEGIN CERTIFICATE----- for a certificate, and -----BEGIN PRIVATE KEY----- for a private key.

The certificate file should also contain the CA certificate chain used to sign the certificate. The server certificate should come first, followed by the issuing CA certificate until the last certificate issued by a Root CA.

The private key file must not be protected with a passphrase. A passphrase would prevent the web server to load it.

Modify the certificate of the administration console



The certificate used when accessing the administration console can be changed in the console settings, in "TLS Key & Cert" section. Three options are proposed: "Self-signed (generated)", "Server path", "Upload files"

The certificate Common Name (CN) must match the value of the "Management Console Hostname" parameter.

Self-signed (generated)

Select this option to let the system generate a certificate using its local Certificate Authority. The issued certificate will be self-signed and browsers will display a warning when connecting. This is a good choice for testing a setup without bothering with certificate generation.

Server path

Select this option if the key and certificate is already stored on the server. Enter the absolute path to get them on the server.

Upload files

Select this option to upload the certificate and the key to the server.

Save

Click save button to confirm your choice and start using the certificate. You may need to reload your browser.

Modify the certificate of the Hiptest application

When accessing the Hiptest application, you can choose to use the same certificate for both the hiptest app and the administration console, or use separate certificates and hostname.

This can be set in the Settings tab of the administration console

Hostname

Configure how users will access Hiptest. A proper domain name with the corresponding SSL certificate gives the best experience.

Hiptest hostname (Required)

The hostname to be used when accessing Hiptest. Ensure this domain name is routable on your network.

SSL Certificate

☒ Use same certificate/key as admin console

☐ Use another certificate

Use same certificate as the console

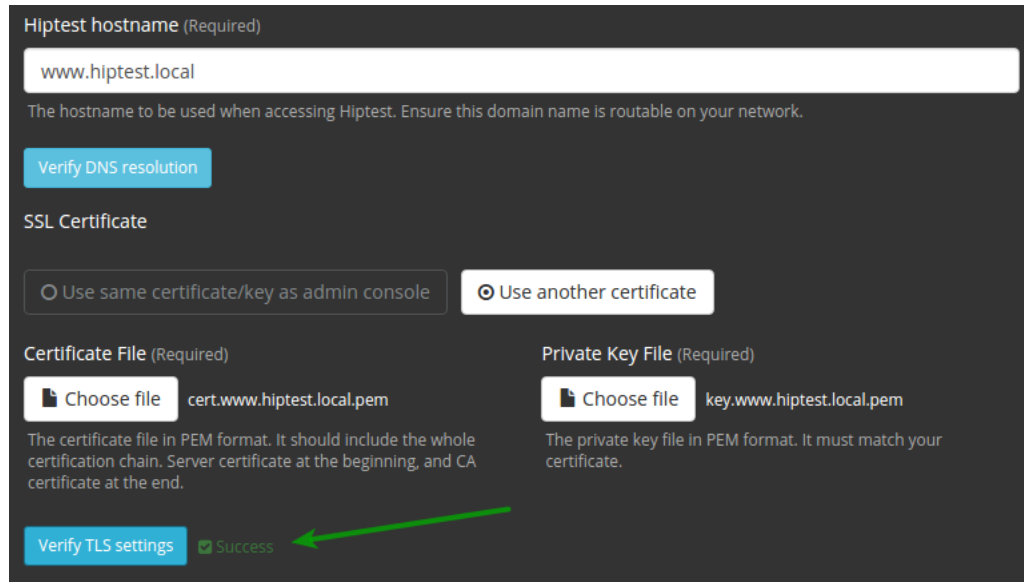
When selecting "Use same certificate/key as admin console" then the certificate used to access the console will be used to access Hiptest too. That means that the Hiptest hostname and the console administration hostname must be the same, or the certificate must handle both hostnames if they are different.

This is the default setting after a Hiptest installation.

Use custom certificate

If you choose to use different certificates for both Hiptest and the administration console, you should use separate hostnames. Then upload the certificate file and the private key file and click "Verify TLS settings" button to ensure the uploaded files are valid and that they match the hostname.

Valid:



Hiptest hostname (Required)

The hostname to be used when accessing Hiptest. Ensure this domain name is routable on your network.

SSL Certificate

☐ Use same certificate/key as admin console ☒ Use another certificate

Certificate File (Required)

cert.www.hiptest.local.pem

The certificate file in PEM format. It should include the whole certification chain. Server certificate at the beginning, and CA certificate at the end.

Private Key File (Required)

key.www.hiptest.local.pem

The private key file in PEM format. It must match your certificate.

✔ Success

Invalid because the hostname does not match:

Hiptest hostname (Required)

my.hiptest.local

The hostname to be used when accessing Hiptest. Ensure this domain name is routable on your network.

[Verify DNS resolution](#)

SSL Certificate

☐ Use same certificate/key as admin console ☒ Use another certificate

Certificate File (Required)

[Choose file](#) cert.www.hiptest.local.pem

The certificate file in PEM format. It should include the whole certification chain. Server certificate at the beginning, and CA certificate at the end.

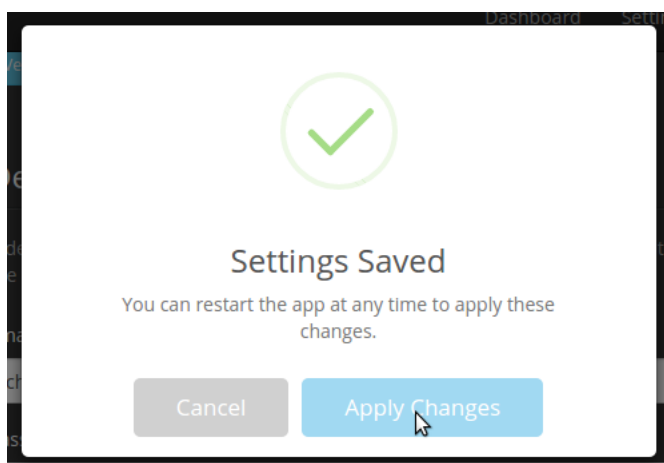
Private Key File (Required)

[Choose file](#) key.www.hiptest.local.pem

The private key file in PEM format. It must match your certificate.

[Verify TLS settings](#) Certificate verification failure: x509: certificate is valid for www.hiptest.local, not my.hiptest.local

Once the certificate is valid, press "Save" button at the bottom of the page to apply changes and restart Hiptest and use the given certificate.



Linking JIRA instance to Hiptest

If using the Hiptest add-on for JIRA, you will have to configure it to contact you Hiptest instance instead of <https://hiptest.net>. The detailed instructions can be found on <http://docs.hiptest.net/configure-jira-with-hiptest-on-premises/>.

Operations

Restarting Hiptest on-premises

To restart the Hiptest service, you have to restart all Replicated services on the server. The replicated services depend on the version installed:

- For Replicated 1.2, services are replicated, replicated-agent and replicated-ui.
- For Replicated 2.x services are replicated, replicated-operator and replicated-ui.

N.B: For RHEL based distributions, this guide will assume you are using **systemd** as the default init system

The supported init systems are: **systemd**, **upstart** and **sysvinit**. To find out which init system is used by Replicated services, you can use the following script

```
if [[ "`/sbin/init --version 2>/dev/null`" =~ upstart ]]; then
  INIT_SYSTEM=upstart
  echo >&2 "upstart will be used as the init system"
elif [[ "`systemctl 2>/dev/null`" =~ -\..mount ]]; then
  INIT_SYSTEM=systemd
  echo >&2 "systemd will be used as the init system"
elif [ -f /etc/init.d/cron ] && [ ! -h /etc/init.d/cron ]; then
  INIT_SYSTEM=sysvinit
  echo >&2 "sysvinit will be used as the init system"
else
  echo >&2 "Error: failed to detect init system or unsupported."
fi
```

And here are the commands to use depending on the init system

For systemd

```
systemctl restart replicated replicated-agent replicated-ui # or replicated-operator depending on replicated version
```

For upstart

```
restart replicated
restart replicated-agent # or replicated-operator depending on replicated version
restart replicated-ui
```

For sysvinit

```
service replicated restart
service replicated-agent restart # or replicated-operator depending on replicated version
service replicated-ui restart
```

Stopping, starting and getting status

To stop, start or getting status of the services, use `start`, `stop` or `status` command in place of the `restart` command.

For example, to stop the replicated service on RedHat Enterprise Linux:

```
systemctl stop replicated
```

Updating server IP address for Replicated 1.2

When the IP address of the host changes, the replicated services are a little lost because they still rely on the previous IP address to contact each other. Here is a summary of the steps to perform. They will be detailed in next sections.

1. Stop all replicated services
2. Change IP address in config files
3. Regenerate replicated certificate information
4. Start replicated service
5. Copy replicated certificate to replicated-agent
6. Start replicated-agent service
7. Start replicated-ui service

8. Check that IP address changed in web administration console
9. Update IP address of Hiptest service in settings

These instructions are valid for a Replicated 1.2 installation. All commands must be run as root user.

During all the process you can check the last lines of replicated services log files located in the `/var/log/replicated/` directory.

1. Stop all replicated services

For **Debian/Ubuntu**

```
service replicated stop
service replicated-agent stop
service replicated-ui stop
```

For **CentOS/RedHat Enterprise Linux/Fedora**

```
systemctl stop replicated replicated-agent replicated-ui
```

Then ensure that services are fully stopped:

```
ps -ef | grep replicated
```

This should yield no results.

2. Change IP address in config files

The IP address is stored in 3 different places:

- `/etc/replicated.conf`
- `/etc/replicated-agent.conf`
- `/etc/replicated-agent/autoconfig.conf`

It must be updated in all files. To edit the files, you can use the `nano` command:

```
nano /etc/replicated.conf
nano /etc/replicated-agent.conf
nano /etc/replicated-agent/autoconfig.conf
```

Here is how the files should look like if the IP address was `192.168.38.248`:

`/etc/replicated.conf`

```
{
  "LocalAddress": "192.168.38.248",
  "ReleaseChannel": "stable"
}
```

`/etc/replicated-agent.conf`

```
{
  "BootstrapInstallsDocker": false,
  "ConfigDir": "/etc/replicated-agent",
  "DataDirectory": "/etc/replicated-agent",
  "HostId": "c053156446b44ed2b427f99410d6ba17",
  "LocalAddress": "192.168.38.248",
  "ReplicatedHostCert": "/etc/replicated-agent/host.crt",
  "ReplicatedHostKey": "/etc/replicated-agent/host.key",
  "ReplicatedTlsCertPath": "/etc/replicated-agent/ca.crt"
}
```

`/etc/replicated-agent/autoconfig.conf`

```
{"ReplicatedDaemonIp":"192.168.38.248","EventsourcePort":"9875","PatchServerPort":"9873","RegistryPort":"9874","...":"..."}
```

3. Regenerate replicated certificate information

Replicated stores certificate information in `/var/lib/replicated/secrets` directory. It contains the certificates and keys used for SSL communications. As these certificates have been generated for the old IP address, this information is obsolete. We will move this directory to another place to get them regenerated by replicated.

Enter the following command:

```
mv /var/lib/replicated/secrets/ /var/lib/replicated/secrets.bak/
```

We could delete the directory, but it's safer to move it to another place to achieve the same goal.

4. Start replicated service

We only start the replicated service. This will regenerate new certificates and keys in the `/var/lib/replicated/secrets` directory. replicated-agent and replicated-ui will be started later.

For **Debian/Ubuntu**

```
service replicated start
```

For **CentOS/RedHat Enterprise Linux/Fedora**

```
systemctl start replicated
```

5. Copy replicated certificate to replicated-agent

Now that the certificates have been regenerated, they must be copied to the replicated-agent config files using the following commands:

```
cp /var/lib/replicated/secrets/ca.crt /etc/replicated-agent/ca.crt
cp /var/lib/replicated/secrets/*.host.crt /etc/replicated-agent/host.crt
cp /var/lib/replicated/secrets/*.host.key /etc/replicated-agent/host.key
```

6. Start replicated-agent service

For **Debian/Ubuntu**

```
service replicated-agent start
```

For **CentOS/RedHat Enterprise Linux/Fedora**

```
systemctl start replicated-agent
```

7. Start replicated-ui service

For **Debian/Ubuntu**

```
service replicated-ui start
```

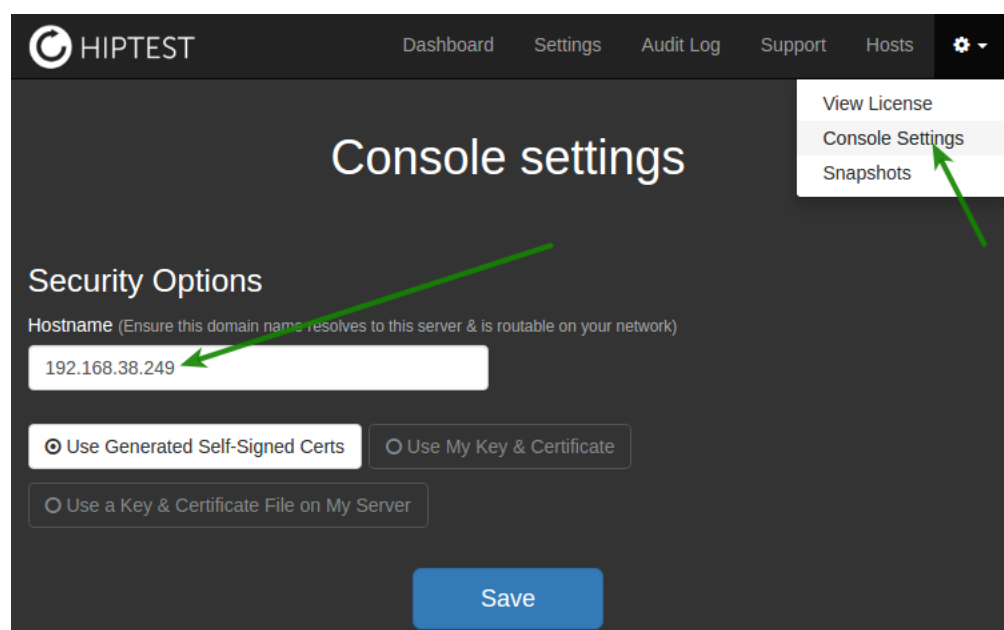
For **CentOS/RedHat Enterprise Linux/Fedora**

```
systemctl start replicated-ui
```

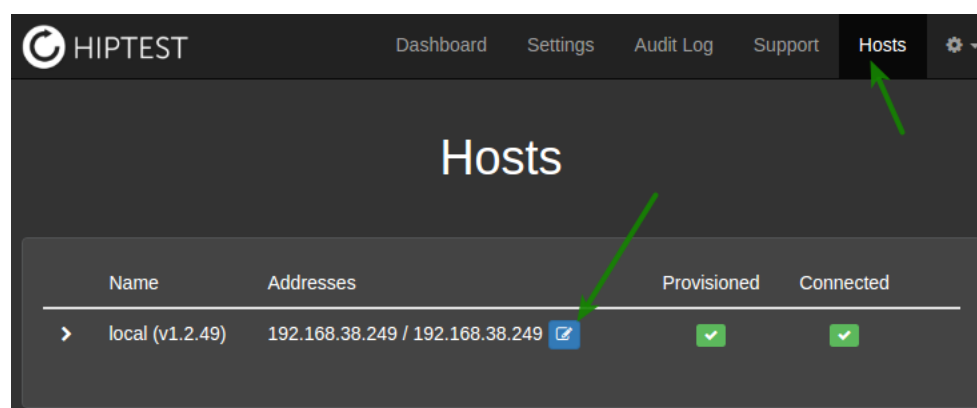
8. Check that IP address changed in web administration console

Now that all replicated services are up and running, you can go to the web administration console to check that the IP address has been updated. 2 places must be checked.

First one is the console settings, from the cog menu.



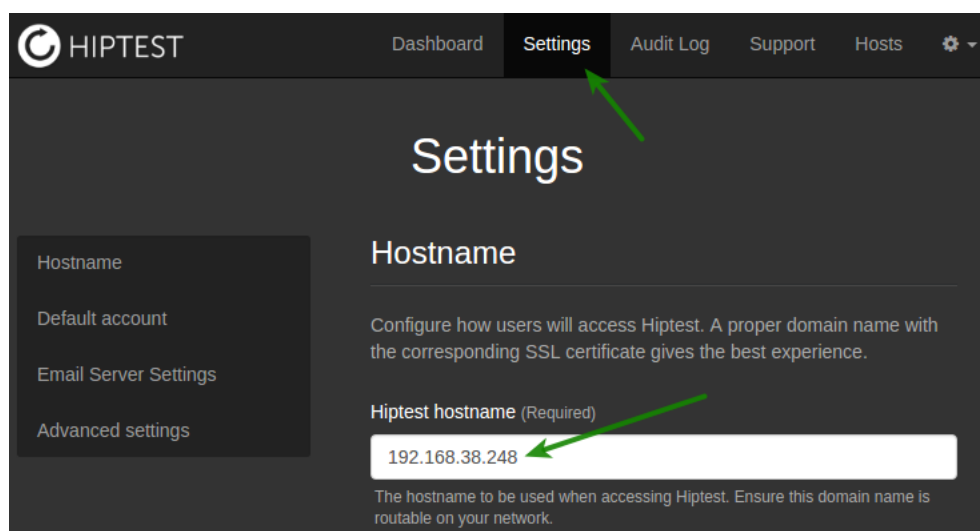
Second one is in the Hosts page.



If the IP address did not update automatically, carefully review the performed steps to ensure they all have been performed. If it still not updates, grab the support bundle and send it to support@hiptest.net. We'll help you fix it.

9. Update IP address of Hiptest service in settings

In the web console, go to the Setting page. From there, update the Hiptest hostname to match your IP address. Of course, you do not need to modify it if you are using a hostname to access the service (like hiptest.mycompany.com).



Updating server IP address for Replicated 2.x

If you need to update the server IP address you will need to manually edit Replicated config files.

1. Stop all replicated services
2. Change IP address in config files
3. Start all replicated services
4. Check that IP address changed in web administration console
5. Update IP address of Hiptest service in settings

1. Stop all replicated services

For **Debian/Ubuntu**

```
service replicated stop
service replicated-operator stop
service replicated-ui stop
```

For **CentOS/RedHat Enterprise Linux/Fedora**

```
systemctl stop replicated replicated-operator replicated-ui
```

Then ensure that services are fully stopped:

```
docker ps | grep replicated
```

This should yield no results, except replicated-statsd and replicated-premkit.

2. Change IP address in config files

The IP address is stored in 2 different places:

- /etc/default/replicated
- /etc/default/replicated-operator

It must be updated in all files. To edit the files, you can use the `nano` command:

```
nano /etc/default/replicated
nano /etc/default/replicated-operator
```

Here is how the files should look like if the IP address was 192.168.38.248:

/etc/default/replicated

```
RELEASE_CHANNEL=stable
PRIVATE_ADDRESS=192.168.38.248
SKIP_OPERATOR_INSTALL=0
REPLICATED_OPTS="-e LOG_LEVEL=info -e DAEMON_TOKEN=Wu39SFBB0Qn5GD5iMdVRPhs7EsMZWdc -e NODENAME=tom"
```

/etc/replicated-agent.conf

```
RELEASE_CHANNEL=stable
DAEMON_ENDPOINT=[192.168.38.248]:9879
DAEMON_TOKEN=Wu39SFBB0Qn5GD5iMdVRPhs7EsMZWdc
DAEMON_HOST=[192.168.38.248]
PRIVATE_ADDRESS=192.168.38.248
REPLICATED_OPERATOR_OPTS="-e LOG_LEVEL=info -e PUBLIC_ADDRESS=192.168.38.248 -e TAGS=local -e NODENAME=tom"
```

3. Start all replicated services

For **Debian/Ubuntu**

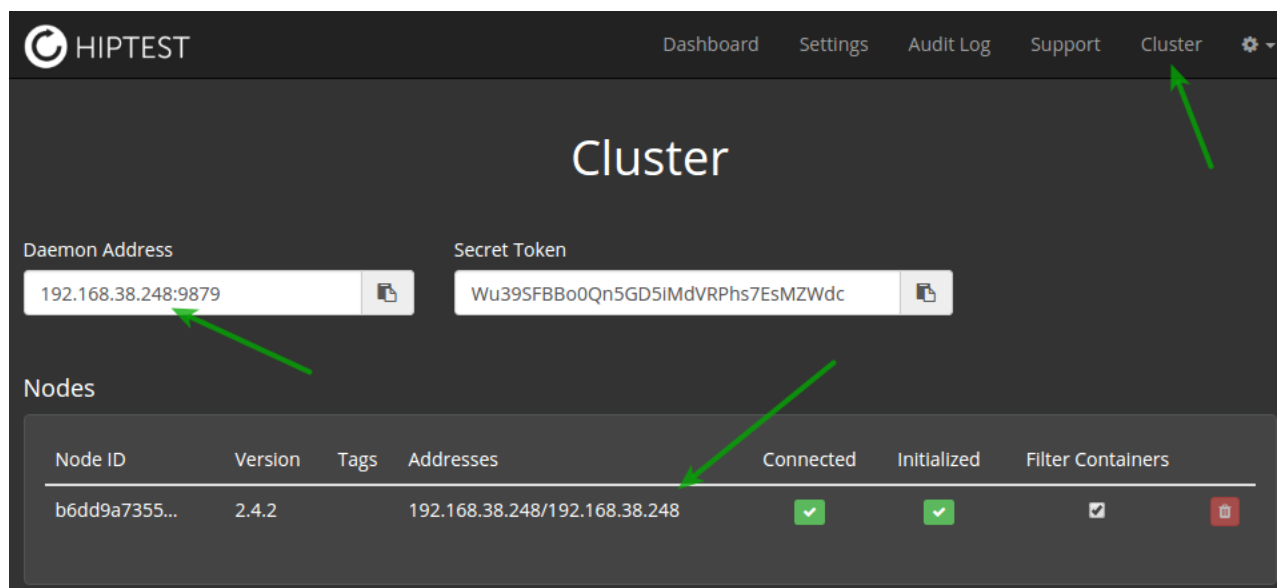
```
service replicated start
service replicated-operator start
service replicated-ui start
```

For **CentOS/RedHat Enterprise Linux/Fedora**

```
systemctl start replicated replicated-operator replicated-ui
```

4. Check that IP address changed in web administration console

Now that all replicated services are up and running, you can go to the web administration console to check that the IP address has been updated on the Cluster page



Cluster

Daemon Address: 192.168.38.248:9879

Secret Token: Wu39SFBB0Qn5GD5iMdVRPhs7EsMZWdc

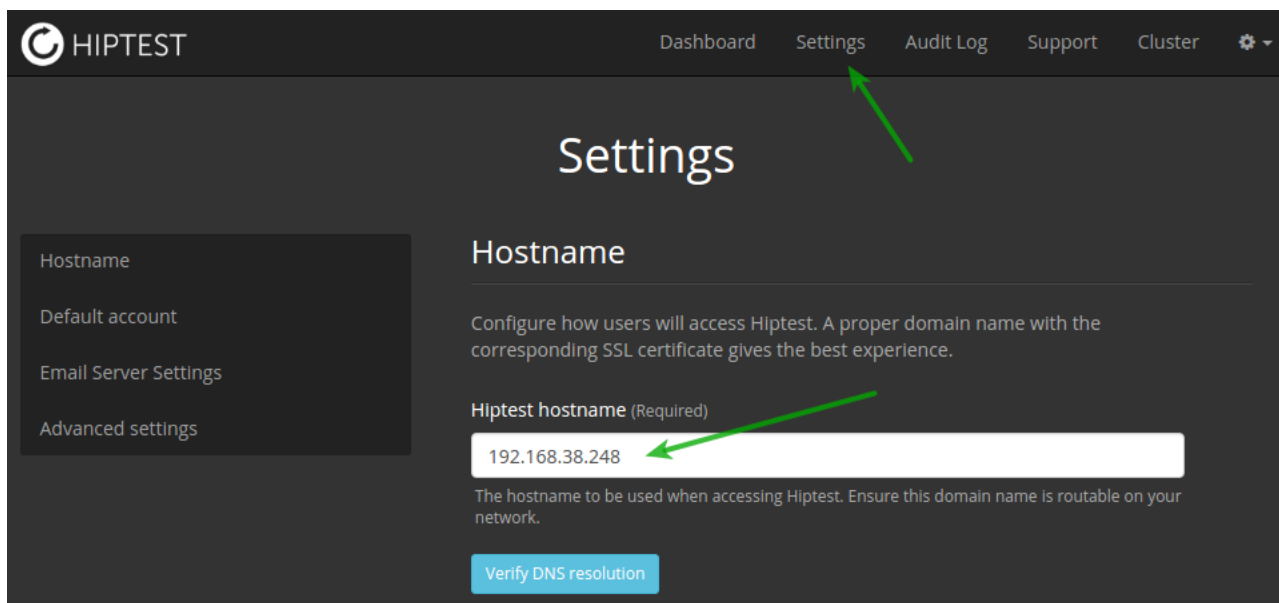
Nodes

Node ID	Version	Tags	Addresses	Connected	Initialized	Filter Containers
b6dd9a7355...	2.4.2		192.168.38.248/192.168.38.248	✓	✓	☑

If the IP address did not update automatically, carefully review the performed steps to ensure they all have been performed. If it still not updates, grab the support bundle and send it to support@hiptest.net. We'll help you fix it.

5. Update IP address of Hiptest service in settings

In the web console, go to the Setting page. From there, update the Hiptest hostname to match your IP address. Of course, you do not need to modify it if you are using a hostname to access the service (like hiptest.mycompany.com).



Update HTTP Proxy / set HTTP Proxy after install

There are several files that need to be modified, depending on the service manager.

Upstart

- Update the file `/etc/default/docker` with updated `http_proxy` environment variable.
- Update the file `/etc/default/replicated` with updated `HTTP_PROXY` variable.
- Restart docker

```
restart docker
```

Systemd

- Follow instructions here <https://docs.docker.com/engine/admin/systemd/#/http-proxy>
- Update the file `/etc/sysconfig/replicated` with updated `HTTP_PROXY` variable.
- Restart docker

```
systemctl restart docker
```

Upgrade

Hiptest Enterprise is composed of two parts: the Hiptest application and the technology to provide the application as an installable package. Both can be upgraded independently.

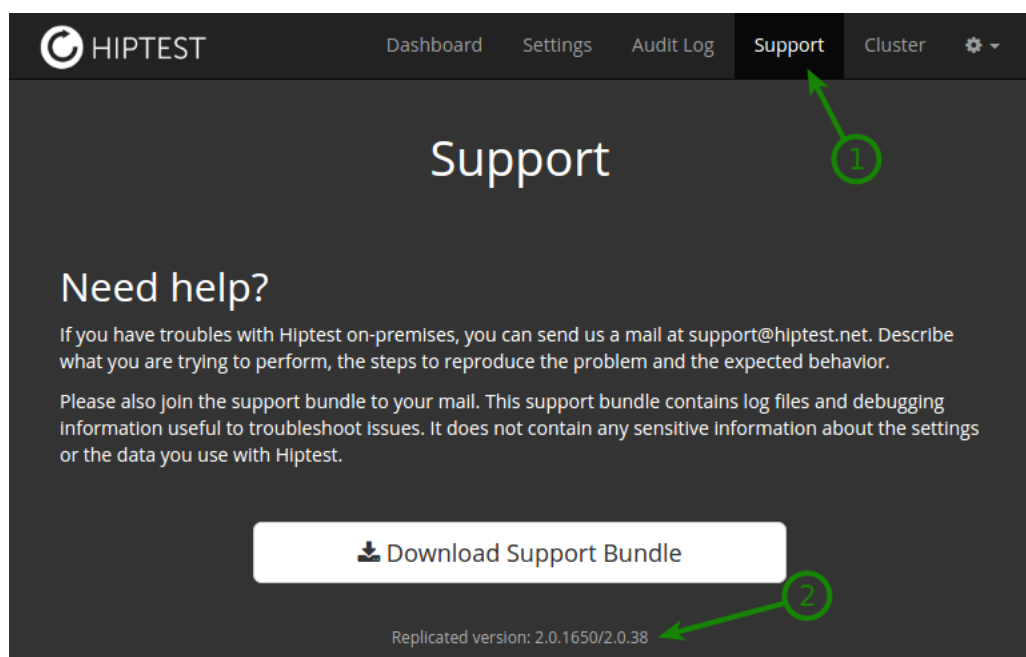
Upgrading Replicated

Replicated is the technology making it possible to ship Hiptest Enterprise as a package easy to install and administer. Key features include one-click updates, audit logging, snapshot and restore utilities, friendly interface and so on.

Which Replicated version do I use?

To know your replicated version:

1. Go to the Support section from the administration console.
2. The Replicated version is the first number. On the screenshot, it is 2.0.1650.



Upgrade from Replicated v1.2 to Replicated 2.x

Replicated 2.x offers more options and control, especially the snapshotting feature which enables backup & restore.

Before upgrading to 2.x, you should make a backup of your files using the following commands as root user:

```
mkdir -p /backup
docker run --rm --volume /backup:/backup --link $(docker ps | grep postgres | awk '{print $NF}'):postgres postgres:9.3 bash -c '\
echo "postgres:5432:*:hiptest:$POSTGRES_ENV_POSTGRES_PASSWORD" > $HOME/.pgpass ; \
chmod 0600 $HOME/.pgpass ; \
exec pg_dump --format=custom --username $POSTGRES_ENV_POSTGRES_USER --host postgres hiptest > /backup/db.dump'
tar czf /backup/attachments.tar.gz /var/lib/hiptest/shared/attachments
```

Copy the files from the /backup directory in a safe place before continuing, in the case where the upgrade would fail.

Replicated provides a one line migration script to upgrade your v1 installation to v2. The script will first stop your app and backup all Replicated internal data in case there is a need for a restore. To invoke the migration script all you have to do is run the script below and follow the prompts.

```
curl -sSL https://get.replicated.com/migrate-v2 | sudo bash
```

Upgrade to latest Replicated v2.0

You can update all Replicated component versions to latest by re-running the installation script command:

```
curl -sSL https://get.replicated.com/docker | sudo bash
```

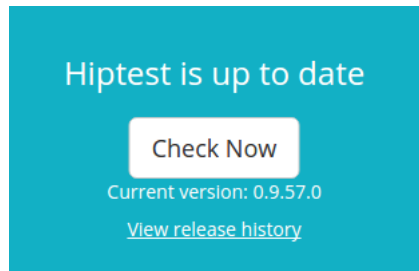
Upgrading Hiptest application

Upgrading the application is done from the administration console dashboard.

Note that during upgrade, Hiptest will not be available to users until the upgrade completes.

Upgrading to latest Hiptest application version

From the dashboard, the current version of Hiptest is displayed.



You can check for new versions by clicking on the "Check Now" button. If an update is available, the following message will be displayed:



Update Available

An update is now available. Click the button below for detailed release notes.

[View Update](#)

Click on the "View Update" button to go to the release history screen.

Release History

There is an update available for Hiptest.

[Install Update](#)

Status	Version	Date Released	Date Installed	
New	0.9.57.3 (182)	Jul 11, 2016 5:38 PM	Never	Release Notes Install
Current	0.9.57.0 (166)	Jun 2, 2016 4:20 PM	Jul 12, 2016 2:27 PM	Release Notes

On this screen, you can see all available versions and their related release notes. Click on "Install Update" button to perform the upgrade to the latest Hiptest software. Note that during upgrade, the service is down until it finishes.

Now on the dashboard, you should see the service is up and running.

Hiptest is up to date

Check Now

Current version: 0.9.57.3

[View release history](#)

Congratulations, you have just upgraded Hiptest!

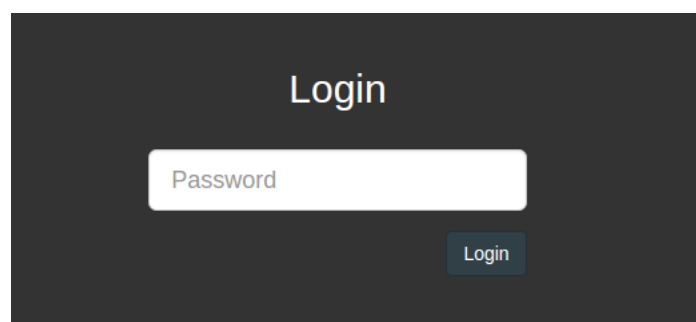
Airgap Upgrade

Upgrading requires to download the new airgap package, to copy it onto the Hiptest server and to run the upgrade from the administration console.

Note that during upgrade, Hiptest will not be available to users until the upgrade completes.

Download the airgap package

Use the Hiptest airgap download link provided by Hiptest. A password is prompted:



Use the password that Hiptest provided you to access the list of available Hiptest releases.

Release History				
	Date Released	Version	Release Notes	Download
Optional	Yesterday at 5:38 PM	0.9.57.3	### Fixed - On-premises platform - Fix an issue preventing Hiptest to start on servers having IPV6 disabled.	Get Download Link
Optional	06/24/2016	0.9.57.2	### Fixed - On-premises platform - Fix start order of components. Previously it could lead to not receiving finished background jobs notifications (for example, at test run creation, the user could need to refresh the browser to see test run creation completion).	Get Download Link
Required	06/02/2016	0.9.57.0	## Hiptest - Add badges for integration in any web-based tool - Add scenario filtering based on tags for test run creation page - Add quick folder access in test run creation page - Enhance Behave, Robot and CucumberJS	Get Download Link

Download the desired airgap package. The top one is the most recent release. Click on the "Download" button to reveal the download link.

If you are downloading from the command line using `curl` or `wget`, the filename will look gibberish. To save the airgap package with a proper filename, you have to use some options to use the filename specified in the Content- Disposition HTTP header:

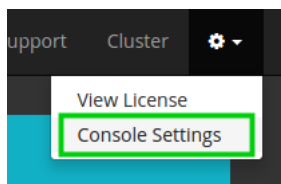
```
# with curl, short options is curl -O -J
curl --remote-name --remote-header-name <download-link>
# with wget
wget --content-disposition <download-link>
```

Copy the airgap package onto the server

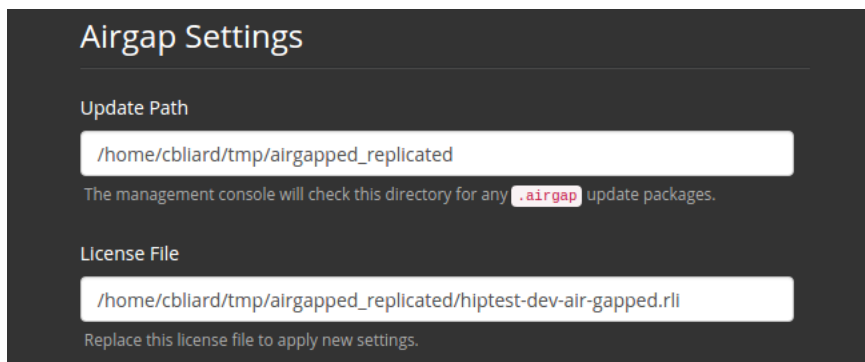
Copy the airgap package to a location on your Hiptest server. Using the same path you used for the installation is fine.

Set the path to the airgap package

From the web administration console, go to the console settings using the cog menu in the top bar



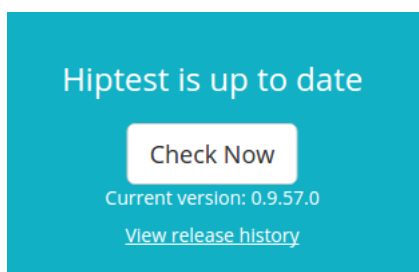
The "Airgap Settings" section defines the "Update Path" where the airgap packages should be searched for. Ensure that this settings matches the path where you copied the airgap package you want to install.



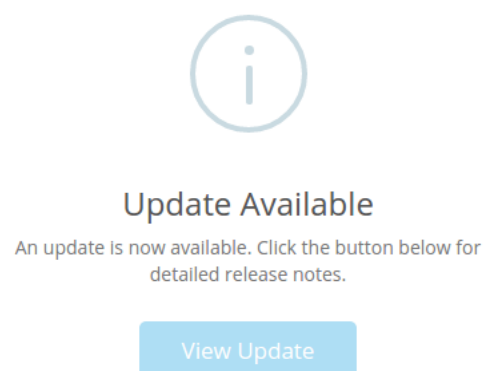
Note that you can also update the licence file from this section.

Perform the upgrade

From the dashboard, there is a button to check for updates. Click the "Check Now" button to search for new airgap packages from the "Update Path" configured before.



When a more recent airgap package is found, the following popup is displayed:



Click on the "View Update" button to go to the release history screen.

Release History

There is an update available for Hiptest.

[Install Update](#)

Status	Version	Date Released	Date Installed	
New	0.9.57.3 (182)	Jul 11, 2016 5:38 PM	Never	Release Notes Install
Current	0.9.57.0 (166)	Jun 2, 2016 4:20 PM	Jul 12, 2016 2:27 PM	Release Notes

From there, you see the available releases, one per airgap package file in the Update Path. You can review the release notes and install any newer release.

Click on "Install Update" button to perform the upgrade. It will extract the new images, install them and restart Hiptest. Note that during upgrade, the service is down until it finishes.

Now on the dashboard, you should see the service is up and running.

Hiptest is up to date

[Check Now](#)

Current version: 0.9.57.3

[View release history](#)

Congratulations, you have just upgraded Hiptest!

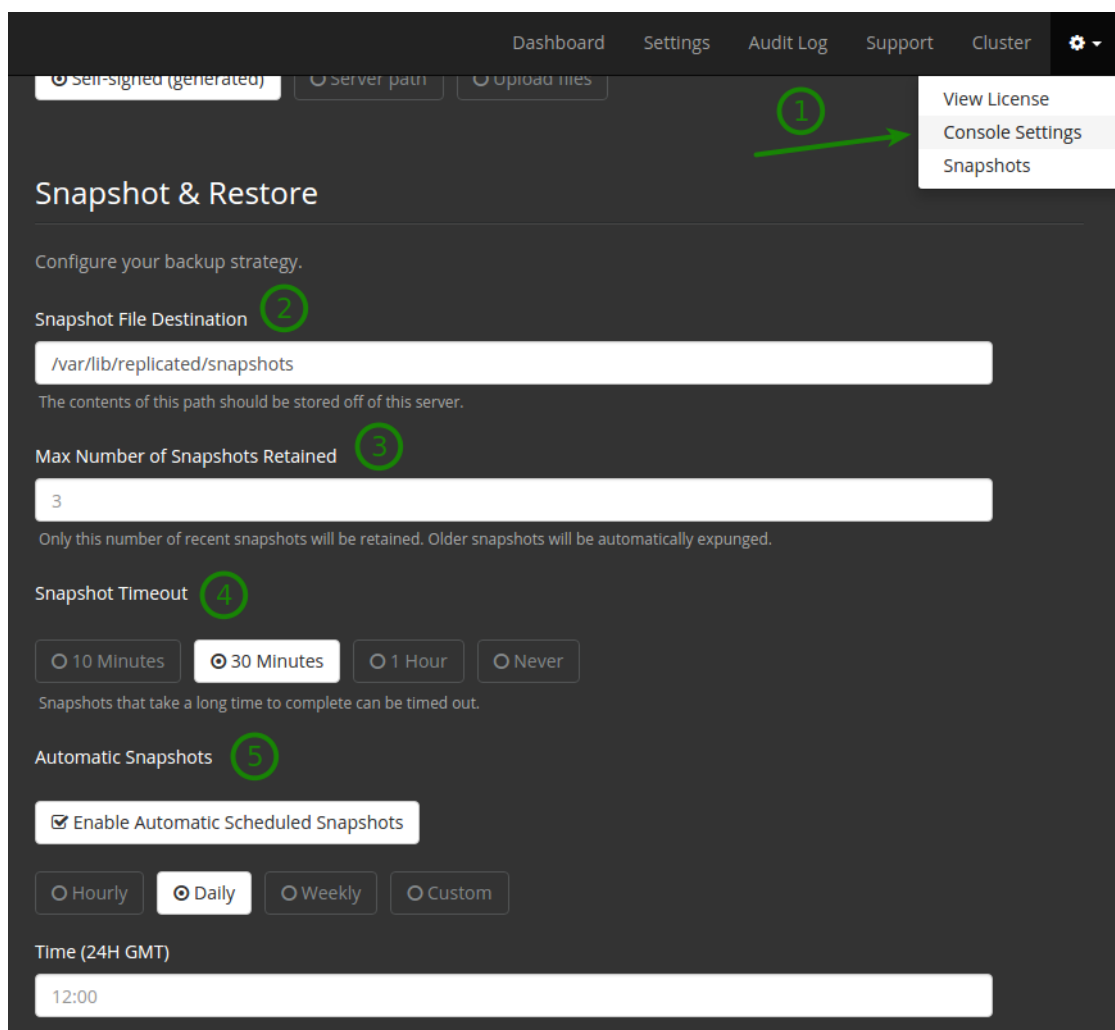
Backup & Restore

Backup

The administration console has the ability to take snapshots of your Hiptest on-premises installation. This feature is available since Hiptest on-premises version 0.9.59.0. **The snapshot feature is for server migration or disaster recovery purposes.**

Automatic snapshots

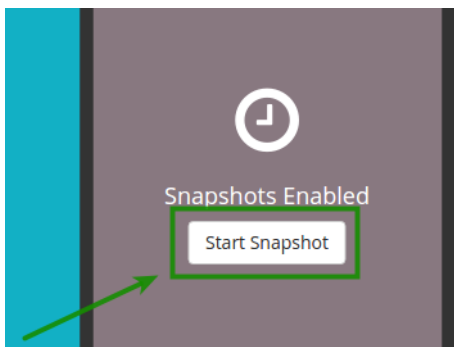
You can configure automatic snapshots from the console settings:



1. Access the Snapshot & Restore settings from the cog menu.
2. The default location for saving a snapshot on a replicated enabled host is: `/var/lib/replicated/snapshots`, the last snapshots will be located in that directory. *Note: We highly recommend you copy this folder to a additional location on a different physical host/SAN to ensure redundancy.*
3. Select how many snapshots to keep. 3 snapshots are kept by default.
4. Snapshot timeout should be configured to 30 minutes.
5. Configure the frequency of automatic snapshots.

Starting a snapshot

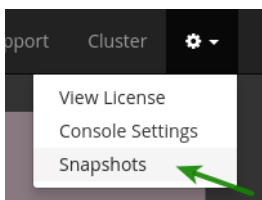
At any moment you can take a snapshot of Hiptest. To do so, click on the "Start Snapshot" button from the dashboard.



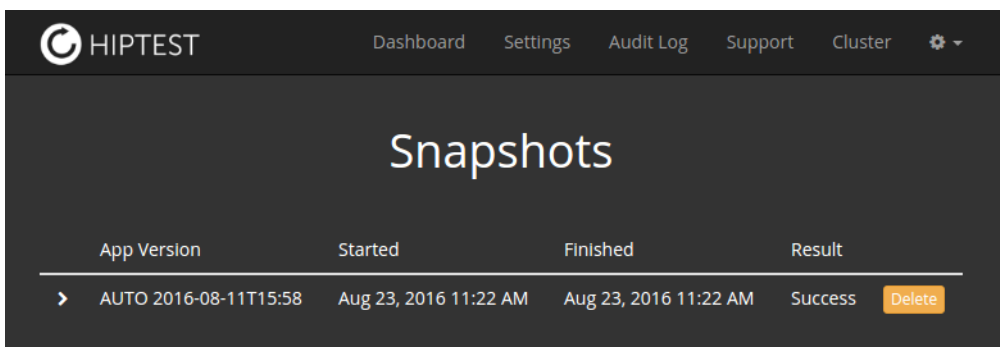
The process takes a couple of minutes to complete.

List snapshots

You can list your snapshots from the cog menu:

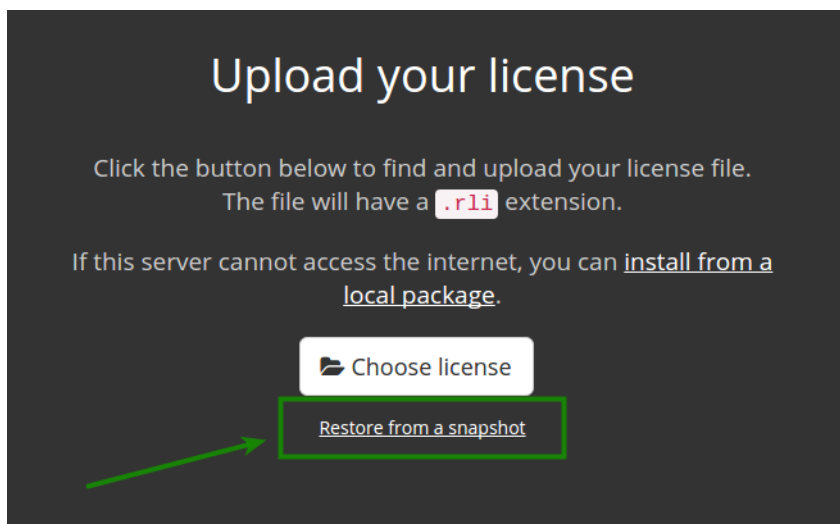


From there, you can see all snapshots along with their applicative version and the creation date.

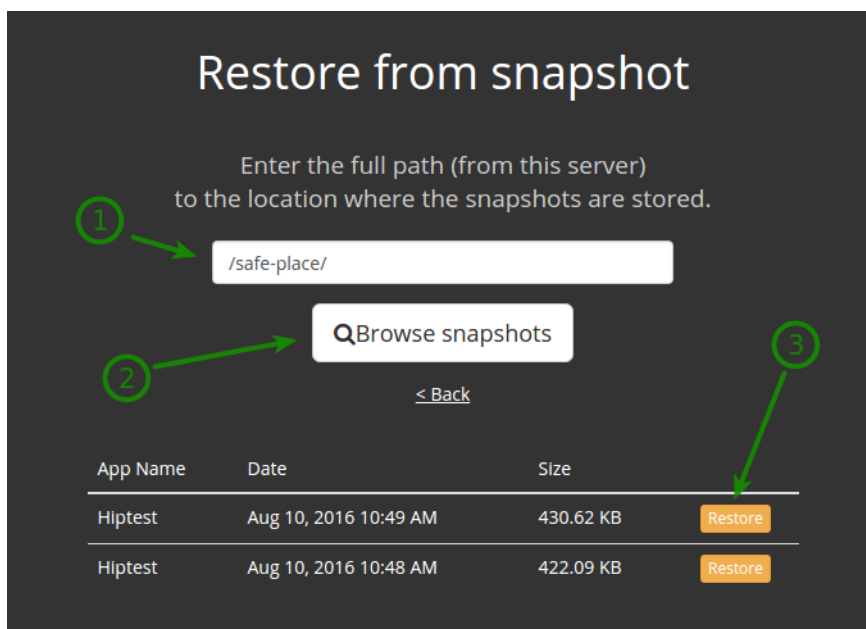


Restore

To restore you need to create a fresh install of replicated which you can find instructions for at first chapter. Before running the web console at <https://:8800>, place a copy of the full snapshot directory on the host. Proceed through the https setup screen and on the upload your license page click the 'restore from a snapshot' link.

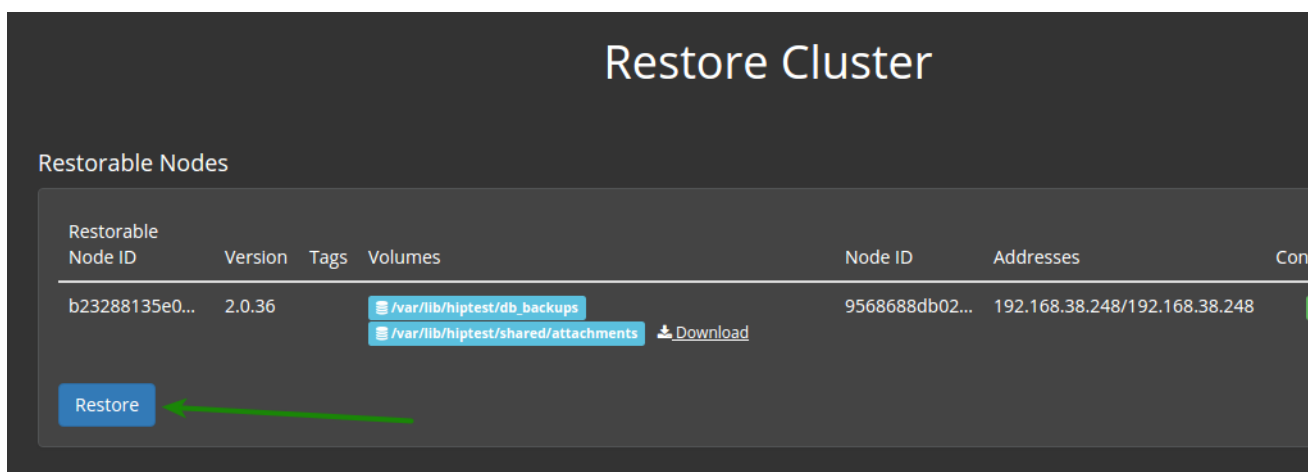


You will be redirected to this screen:



1. Enter the path on the host where you have copied the snapshots folder,
2. Click "Browse snapshots",
3. Locate the latest version you would like to backup from and click the "Restore" button.

You will be given options to download the restored volumes. Click "Restore" button to continue.



Once volumes have been restored, you will be redirected to the cluster screen:

Cluster

Daemon Address

Secret Token

Nodes

Node ID	Version	Tags	Addresses	Connected	Initialized	Filter Contain...
9568688db02...	2.0.36		192.168.38.248/192.168.38.248	✓	✓	✓

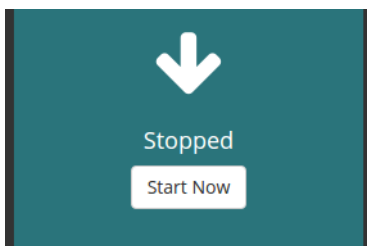
Add Node

Containers

State	Container ID	Node ID	App Component Name	App Container Name	Image	Started At
-------	--------------	---------	--------------------	--------------------	-------	------------

The restore is not completed yet. Data is in the volumes, now it need to be transferred to the database. There are two commands to run manually from the host. Hiptest needs to be started.

Start Hiptest from the dashboard:



Then open a terminal on the host and enter the following commands:

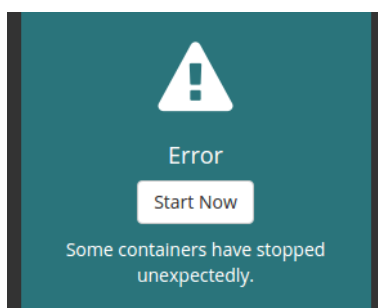
```
source /etc/replicated.alias
hiptest restore-postgres-db
hiptest restore-elasticsearch-db
```

Here is a sample of the output you will get:


```
tom ~ # source /etc/replicated.alias
tom ~ # hiptest restore-postgres-db
create temporary hiptest_restored database.
import backup into hiptest_restored database.
stopping db connections to hiptest database.
renaming hiptest database as hiptest_previous database.
renaming hiptest_restored database as hiptest database.
removing now unnecessary hiptest_previous database.
db restore completed successfully.

tom ~ # hiptest restore-elasticsearch-db
Migrating elasticsearch indexes
Resetting SuggestionsIndex
  Imported SuggestionsIndex::Tag for 0.1s, documents total: 0
Resetting FiltersIndex
  Imported FiltersIndex::Scenario for 0.21s, documents total: 8
Resetting EditorSuggestionsIndex
  Imported EditorSuggestionsIndex::Actionword for 0.1s, documents total: 17
  Imported EditorSuggestionsIndex::StepLocation for 0.08s, documents total: 23
Resetting ProjectsIndex
  Imported ProjectsIndex::Project for 0.08s, documents total: 4
Resetting TestRunIndex
  Imported TestRunIndex::ScenarioSnapshot for 0.08s, documents total: 11
  Imported TestRunIndex::FolderSnapshot for 0.03s, documents total: 7
  Imported TestRunIndex::TestRun for 0.02s, documents total: 3
Resetting TestPlanIndex
  Imported TestPlanIndex::Folder for 0.08s, documents total: 6
  Imported TestPlanIndex::Scenario for 0.02s, documents total: 8
  Imported TestPlanIndex::Actionword for 0.04s, documents total: 17
```

During the database restore, active database connections have been interrupted. That's why the dashboard indicates that some containers have stopped unexpectedly.



Click "Start Now" to restart Hiptest.

The restore is now complete.

Migrating from Hiptest Cloud

It is possible to migrate all your data from Hiptest Cloud to a on-premises installation. Importing data from Cloud overwrites all existing Hiptest data of an on-premises installation, so it is really meant to be used on first installation. If you are interested, contact support@hiptest.net so we can send you an archive containing your cloud data.

The archive data we send you contains a partial database dump and your attachments. Extract it at the root of your server and then delete it:

```
cd /
sudo tar xzf /tmp/cloud_data.tar.gz
shred /tmp/cloud_data.tar.gz
```

Then you will need to perform the same steps as if you were restoring from a backup. Open a terminal on the host and enter the following commands:

```
source /etc/replicated.alias
hiptest restore-postgres-db
hiptest restore-elasticsearch-db
```

Here is a sample of the output you will get:

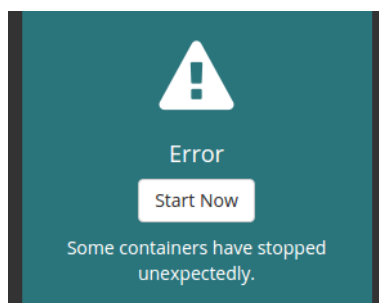
```

tom / # source /etc/replicated.alias
tom / # hiptest restore-postgres-db
create temporary hiptest_restored database.
import backup into hiptest_restored database.
loading migration data to public schema.
stopping db connections to hiptest database.
renaming hiptest database as hiptest_previous database.
renaming hiptest_restored database as hiptest database.
removing now unnecessary hiptest_previous database.
db restore completed successfully.

tom / # hiptest restore-elasticsearch-db
Migrating elasticsearch indexes
Resetting SuggestionsIndex
  Imported SuggestionsIndex::Tag for 1.35s, documents total: 4199
Resetting FiltersIndex
  Imported FiltersIndex::Scenario for 0.83s, documents total: 1654
Resetting EditorSuggestionsIndex
  Imported EditorSuggestionsIndex::Actionword for 0.33s, documents total: 1098
  Imported EditorSuggestionsIndex::StepLocation for 1.79s, documents total: 1835
Resetting ProjectsIndex
  Imported ProjectsIndex::Project for 0.07s, documents total: 103
Resetting TestRunIndex
  Imported TestRunIndex::ScenarioSnapshot for 4.31s, documents total: 12125
  Imported TestRunIndex::FolderSnapshot for 0.71s, documents total: 2258
  Imported TestRunIndex::TestRun for 0.07s, documents total: 310
Resetting TestPlanIndex
  Imported TestPlanIndex::Folder for 0.34s, documents total: 491
  Imported TestPlanIndex::Scenario for 0.86s, documents total: 1654
  Imported TestPlanIndex::Actionword for 0.5s, documents total: 1098

```

During the database restore, active database connections have been interrupted. That's why the dashboard indicates that some containers have stopped unexpectedly.



Click "Start Now" to restart Hiptest.

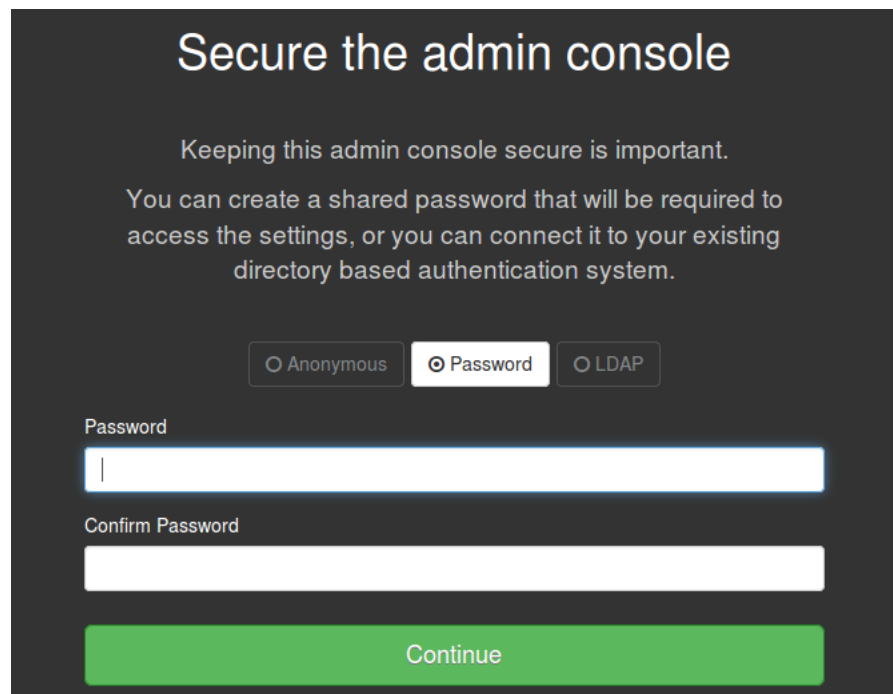
The migration is now complete. You can log in to Hiptest using the same credentials you had on the Cloud version.

In the administration console settings, you should set the username of the person in charge of Hiptest on-premises in your organization. This user's email will be displayed on the Hiptest landing page so that new users know which person to reach if they want an account.

Troubleshooting

I lost the password of the Hiptest on-premises administration console

The console password has been set at Hiptest on-premises installation. This is the screen where the password is set:



If you have lost this password, it can be reset: login to the server where Hiptest on-premises is installed and enter the following commands:

```
source /etc/replicated.alias
replicated auth reset
```

As some commands are run through `sudo`, it will ask for a password. You must enter your linux account password here.

You should then get the following message:

```
Authentication is now disabled. Please visit https://<ip_address>:8800/create-password to set up a new password.
```

Head to the given URL to reset your Hiptest on-premises administration console password.

It hangs when creating a new snapshot.

Symptoms: you are creating a new snapshot from the dashboard. The spinner is spinning for a long time and the status text is displaying "Backing up container volumes".

This is a known issue that is fixed since Replicated version 2.0.1649. You should upgrade to latest Replicated version.

I restored from a snapshot but I lost my data.

You probably forgot to restore the Hiptest data after restoring your server from the snapshot. You need to run the following commands on the host:

```
source /etc/replicated.alias
hiptest restore-postgres-db
hiptest restore-elasticsearch-db
```

Refer to the **Restore** section of this guide for further information.

One user lost his/her password

If a user has lost his password, he can ask for a reset password link from the Hiptest sign in page. If the SMTP settings are correctly filled, the user will receive the reset password link to his inbox.

If the user can't receive emails, it is still possible to get the reset password link from the command line with the `get-reset-password-link` command. For this, open a terminal and type the following commands:

```
source /etc/replicated.alias
hiptest get-reset-password-link <user-email>
```

This command will regenerate the reset password token and display the link to the reset password page. Here is an example usage:

```
tom ~ # source /etc/replicated.alias
tom ~ # hiptest get-reset-password-link christophe.bliard@hiptest.net
Reset password token regenerated for user 'christophe.bliard@hiptest.net'.
The URL to reset the password of the user is:

    https://192.168.38.248/users/password/edit?reset_password_token=5Dttp6ZSy3V8ZLL8nrnt

This link is valid for 21600 seconds
and will expire on Wed, 14 Sep 2016 19:49:40 +0000.
```

From there, you can copy/paste this link and send it to the user that wants to reset his/her password.

I want to set the password of one user

You can set the password of a user with the `set-password` command. For this, open a terminal and type the following commands:

```
source /etc/replicated.alias
hiptest set-password <user-email> <password>
```

Here is an example usage:

```
tom ~ # source /etc/replicated.alias
tom ~ # hiptest set-password christophe.bliard@hiptest.net Hell0 World
Password for user 'christophe.bliard@hiptest.net' successfully changed to 'Hell0 World'.
```

Release notes

[1.1.1.0] - 2017-01-04

Fixed

- Hiptest
 - Fix import projects page display issue.
- On-premises platform
 - Better detection of Hiptest fully started.

[1.1.0.0] - 2016-12-27

Added

- Hiptest
 - Add support for [JIRA mandatory fields](#) on issues creation. Checkboxes, lists, datetime picker, text area fields are now supported.
 - Multiple scenarios can be added to a test run directly from the test run page.
 - [Can add pie charts based on tags usage](#). Available from the Metrics tab.
 - Can unassign oneself from a project.
 - [Notification system](#): be notified when access or role in a project has changed.
 - Notifications are also displayed when test runs are updated.
 - The datatable can be maximized to full-screen, for easier edition.
 - Can duplicated a datatable row.
- On-premises platform
 - Release notes are now visible from Support tab in administration console.
 - Some logs are formatted as JSON.

Updated

- Hiptest
 - Performance improvements.
 - Improve compatibility of JUnit XML result file with cucumber-js and cucumber-java.
 - Archived test runs no longer get exported when downloading backups.
 - A Collapsed folder now show total number of scenarios, including those from subfolders.
- Hiptest-publisher
 - Use version 0.18.1.
 - Generate output compatible with Cucumber-js 0.10.0.

Fixed

- Hiptest
 - Can now upload files up to 100 Mo. Limit was 1 Mo before.
 - Pusher JS library is no longer downloaded from Internet. It is now provided by the app to workaround external downloading policy which were blocking it.
 - When importing RobotFramework result file, the update message is now read from status tag.
- On-premises platform
 - When (re)starting, wait until the whole application has finished booting up.

[1.0.0.0] - 2016-10-19

Added

- Hiptest
 - Jira integration now support both Jira Server and Jira Cloud.
 - Add revision history. Last user modification and time is displayed for every items.
 - Add Reader role. A user assigned with this role will be unable to create or modify anything in the project.
 - Jira issue creation from Hiptest is now available with Jira server.
 - Scenarios and folders can now be reordered with drag'n'drop.
 - Project backup is now done asynchronously.
 - Various performance improvements.
 - CSV files can be used as attachments.
 - NUnit result files can now be imported in external test runs.
 - Can easily move to next/previous scenarios with dedicated buttons.
 - In a test run, can assign all tests of a folder to a user.
- On-premises platform
 - Now possible to migrate data from Cloud app to on-premises app.

Fixed

- Hiptest
 - Creation text boxes no longer remain opened after a focus out in folder page.

Removed

- Hiptest
 - Slack integration is not available for on-premises version.

[0.9.62.0] - 2016-10-05

Added

- On-premises platform
 - Support SMTP without authentication.

[0.9.61.0] - 2016-09-16

Added

- Hiptest
 - Invitation links do not expire anymore (They used to expire after 3 months)

[0.9.60.1] - 2016-09-14

Fixed

- Hiptest
 - Badges are available again

[0.9.60.0] - 2016-09-14

Added

- Hiptest
 - Ability to display reset password link for a user
 - Ability to change password for a user

[0.9.59.0] - 2016-08-24

Added

- Hiptest publisher
 - Use version 0.15.9.
 - Add support for Protractor
- On-premises platform
 - Backup/Restore is now possible through snapshotting.

Fixed

- Hiptest publisher
 - Fix trailing double-quote stripping in free text for Gherkin export

[0.9.58.0] - 2016-07-22

Added

- Hiptest
 - Display cumulated stats of all test runs visible in the project dashboard.
 - In test run, Can assign all tests of a folder to a user.
 - Integrate with Jenkins server.
 - Add symbol notations. Symbols are copied as-is when exported to automation, allowing to set custom variables or pieces of code. [See documentation](#) for more details.
 - Can add free text to an actionword call, allowing to pass JSON data or other multiline text as parameter.
 - Can import docstrings from gherkin features.
 - Display all parameters in tests view.
 - Action words can have a description.

- Tests can have status "Work in Progress".
- Can add all scenarios of a folder to a test run.
- Hiptest publisher
 - Use version 0.15.7.
 - When test run id cannot be found for the project, a list of available test runs is displayed.
 - Can choose a test run by its name with `--test-run-name`.
 - Can define filename of exported files with `--filename-pattern`.
 - Can prevent export of test UIDs in gherkin feature files with `--no-uids`.

Fixed

- Hiptest
 - Can edit a scenario description that was set to blank text.
 - Realtime notifications work correctly on every browsers.
 - Can download test scripts from Hiptest automation tab.
- Hiptest JIRA plugin
 - Folders and tests from archived test runs are not visible anymore.
- Hiptest publisher
 - Fixes in Python, C# and Javascript exports.
 - Fixes `actionwords_signature.yaml` file generation which could be different depending on command line parameters.

Removed

- On-premises platform
 - The real-time communication server use same ports as Hiptest, to prevent issues with SSL self-signed certificate.

[0.9.57.4] - 2016-07-13

Added

- On-premises platform
 - The real-time communication server ports are now configurable. Useful if it conflicts with existing services.

[0.9.57.3] - 2016-07-11

Fixed

- On-premises platform
 - Fix an issue preventing Hiptest to start on servers having IPv6 disabled.

[0.9.57.2] - 2016-06-24

Fixed

- On-premises platform
 - Fix start order of components. Previously it could lead to not receiving finished background jobs notifications (for example, at test run creation, the user could need to refresh the browser to see test run creation completion).

[0.9.57.0] - 2016-06-02

Added

- Hiptest
 - Badges for integration in any web-based tool
 - Scenario filtering based on tags for test run creation page
 - Quick folder access in test run creation page
 - Support "But" Gherkin keyword
- Hiptest-publisher service
 - Support rendering of folder definition as setup
 - Support Docstrings for Gherkin based languages
 - Enable tags in Robot Framework export
 - Support "But" Gherkin keyword
- On-premises administration console
 - Ability to edit application secret key for troubleshooting
 - Show CPU & Memory usage for Hiptest

Changed

- Hiptest-publisher service

- Enhance Behave, Behat and CucumberJS feature files import: now fully supports datasets
- Performance enhancements

Fixed

- Hiptest-publisher service
 - Syntax fixing in Python and Gherkin export

[0.9.56.0] - 2016-05-06

Added

- Reviewed scenarios selector when creating new test run

Changed

- Enhanced Jenkins integration

[0.9.55.0] - 2016-04-22

Added

- Enable default user creation

Changed

- Better management of invitations

[0.9.53.0] - 2016-04-01

Added

- Enjoy Hiptest on-premises