

This guide will get you up to speed quickly on installing CloudPassage Halo. It applies to both the free version as well as the Pro (commercial) version. To understand the differences between the two products, please visit the [CloudPassage Web site](#).

INTRODUCTION

CloudPassage Halo secures your servers by providing:

- Host based firewall management
- Server configuration checking and auditing
- Vulnerability management
- Account management and auditing
- Event logging and alerting

The installation process is quick and easy, although a first time install takes a bit of extra time as we must first create an account.

CREATE A HALO ACCOUNT

To create a Halo account, go to the [CloudPassage registration page](#) and fill out the online form. This form will ask for basic information like the account name you wish to use, your email address, and company name. Once you have verified that you are not a bot, you will be brought to the main logon screen. A onetime password will be sent to your specified email account. Use this password to login for the first time.

As soon as you login, you will be prompted to change your password. This is shown in Figure 1. Type in a strong password and click the Submit button.

Figure 1: You are required to change your password at first login

Servers	Policies	Settings	Support	
----------------	-----------------	-----------------	----------------	--

Password Change Required

Your registration will be completed after you change your temporary password.

Password Construction Rules

Passwords must be at least **eight** characters long and must contain both **numbers and letters**.

Password

Retype Password

Once you change your password, you will be prompted to select a configuration policy for your system. This screen is shown in Figure 2. Which policy you select will be dependent on which operating system you are using, as well as which software you plan on using. Pick the policy that is most appropriate for your configuration.

Figure 2: The policy selection screen

Servers	Policies	Settings	Support	
----------------	-----------------	-----------------	----------------	--

Choose A Configuration Policy

It looks like this is the first time your company has logged on to CloudPassage. Welcome!

The CloudPassage Halo platform uses server configuration policies to help manage the security of your cloud servers. One or more policies can be applied to server groups for flexibility. One example is creating a server group called Web Servers and assigning two policies to it: CentOS Linux and Apache 2.

The policy templates below will give you a jump-start. These templates are always accessible under the Policies menu. For now, please select one and we'll clone it to establish your first policy.

▲ Name	Description	
CentOS Linux - Apache 2.x	This is a configuration policy for an Apache HTTP server running on CentOS Linux systems. It addresses configuration of the http server itself, not the entire Linux operating system. CloudPassage policies may require customization and addition of rules to meet all policy requirements. This and other policy templates can be cloned and customized to fit specific distributions or environments (e.g. varying file paths or process names).	Select
CentOS Linux - Core OS	This configuration security policy has been configured for a default CentOS 5.5 distribution. Rules can be added, removed and modified as needed to fit specific CentOS environments. Last update: November 6, 2010	Select
CentOS Linux - MySQL 5.x	This is a configuration policy for a MySQL database server running on CentOS Linux systems. It addresses configuration of the MySQL server itself, not the entire Linux operating system. CloudPassage policies may require customization and addition of rules to meet all policy requirements. This and other policy templates can be cloned and	Select

INSTALLING THE DAEMON

Once you select a policy, you are guided on how to install the Halo Daemon on your server. There are two possibilities when performing your first install. The first is to simply run the Halo installation script. This is shown in Figure 3. By clicking on the hotlink you can download a script to your system which will take care of the entire installation process.

Figure 3: The Halo install script is the easiest method of installation

Installing Halo Daemons

The instructions below explain the daemon installation process.

The CloudPassage Halo daemon supports 32 and 64 bit versions of Debian, Ubuntu, CentOS, Redhat and Fedora Linux distributions with a 2.6.x kernel (or newer).

Important: The instructions below contain the API key for Chris's install process account. Keep it confidential.

- [CloudPassage daemon for Debian and Ubuntu \(download script\)](#)
- [CloudPassage daemon for CentOS, Fedora, RHEL, and Linux AMI \(download script\)](#)

For those who prefer a more hands on approach to installing Halo, the installation steps are listed as well. Simply copy the commands listed in each yellow box and past them into the command line of your server via an SSH session.

Figure 4: Steps are included to manually install Halo

CloudPassage on Debian and Ubuntu

Before installing the CloudPassage Halo daemon you should make sure you've logged into your server using a user account that has been granted sudo privileges or by using the root user account to run the following commands. If you need to know more about using sudo on a Debian or Ubuntu box, Ubuntu has provided documentation from their community that explains it [here](#).

Installing CloudPassage daemon

1. Add the CloudPassage apt repository:

```
echo 'deb http://packages.cloudpassage.com/7ca8d0c998ea0edbd9852df1131c0457/debian debian main' |  
sudo tee /etc/apt/sources.list.d/cloudpassage.list > /dev/null
```

2. Install curl:

```
sudo apt-get -y install curl
```

3. Import CloudPassage public key:

```
curl http://packages.cloudpassage.com/cloudpassage.packages.key | sudo apt-key add -
```

4. Update apt repositories:

```
sudo apt-get update
```

5. Install CloudPassage daemon:

```
sudo apt-get install cphalo
```

When the installation is complete Halo is ready to go! Upon initial installation Halo will automatically check the server's configuration settings as well as see if there are any known vulnerabilities in the software you are running. You can review the results by click on "Servers" in the main menu, and then clicking on the name of the server. An example is shown in Figure 5.

Figure 5: Status screen which shows the current security state of your server

[Home](#) / [Ip 10 120 62 97](#)

Server name: ip-10-120-62-97
Server status: Active
Connecting from: 75.101.237.53 (USA)
Current group: cbrenton-testing

Booted on: 2011-10-17 20:11:01
[View additional server details](#)
[Halo daemon log](#)

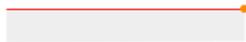
Installed Halo Daemon version: 2.3.1 (Up to date)

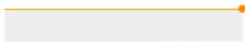
 **Configuration Scan** Last ran: 11 minutes ago (Completed w/errors) Current Policies
[AAA-Base Security Policy](#)



 **2 critical issues**

 **1 other issue**





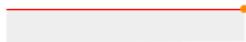
[More detail](#)

 **Software Scan** Last ran: 11 minutes ago (Completed)



 **5 critical packages**

 **20 non-critical packages**





[More detail](#)

 **Security Events** No events logged in the last 24 hours



No critical events

No other events





[More detail](#)

 **Firewall Management** Last checked: 4 minutes ago (Active) Current Policy
[cbrenton-firewall-testing](#)

WHAT TO DO NEXT

Once Halo is installed you can create a firewall policy, audit user account information or customize the configuration check for your particular needs.

For more information on how to use Halo, please see the Halo [Quickstart Guide](#) or [User Manual](#). If you plan on using authenticated port access, you may also wish to review the [GhostPorts User Guide](#).