CloudPassage logo

GhostPorts User Guide

What are GhostPorts?

GhostPorts, a feature of Halo™ Professional, enables strong protection of administrative network access, including two-factor authentication, with the flexibility to allow authorized access from anywhere—easily and securely. This is the most secure way to control access to administrative services on cloud servers. Administrators can lock down all administrative ports, which will dynamically open only for authenticated users, limited to the IP address from which they authenticated. These ports automatically close after a defined period, returning them to an inaccessible state.

The Advantages

GhostPorts help eliminate the worry of attackers continually scanning for administrative ports and attempting to brute-force logins to those services. When GhostPorts is enabled the chosen administrative ports will be invisible to the attacker when they scan your network. This makes it much harder for the attacker to find a way in because they can't even see your open ports.

How it Works

GhostPorts uses USB-based token generators recognizable as USB input-devices. Today, CloudPassage supports the YubiKey® from Yubico, referred to simply as Yubikey throughout this document. Once a specific Halo user has been assigned a YubiKey, the user authenticates to the Halo GhostPorts portal to activate or engage GhostPorts. Firewall policies established for cloud server groups include specific rules for GhostPorts users, which determine the services and ports to be opened for their access.

Halo communicates the source IP address of the GhostPorts user to the servers in the target server group. The GhostPorts user now has the defined access for a specific amount of time and from a specific IP address. Once that time expires, Halo closes the open ports and access is denied.

Each YubiKey value is unique across the Halo Grid, therefore each YubiKey can be assigned to only one user at a time.

Getting Started (for Site Administrators)

Step 1: Acquire a YubiKey for each of your users that you wish to use GhostPorts. These can be ordered directly from Yubico or by filling out the form on cloudpassage.com/ghost.

Step 2: Create user accounts for each of your users. See the CloudPassage Halo User Manual. You must have site administration privileges to add users to the portal.

User Access Privilege Levels

It is important to note that there are two levels of access privileges you may set for GhostPorts users: GhostPorts only or GhostPorts + Halo™ Portal.

GhostPorts Only

GhostPorts Only access allows a user to authenticate to the GhostPorts portal using the Yubikey without having to enter a username or password. In other words, this is single-factor authentication to engage the use of GhostPorts. The user is only allowed access to the GhostPorts engagement portal, not to the Halo Portal.

GhostPorts and Halo™ Portal

This level of access is reserved for users that need both access to the Halo™ Portal and the use of GhostPorts to tightly secure access to cloud servers within your defined server groups.

To set one or both of these access levels, go to "**Settings**" --> "**Site Administration**". From the User tab, select the user you would like to manage. Select the "**Edit**" link located at the far right of the list. The two options are titled "**Enable Halo Portal Access**" and "**Enable GhostPorts Access**". Select the appropriate checkbox(es).

Enabling GhostPorts Access

GhostPorts access is defined by either single factor or two-factor authentication. Single-factor authentication is used when setting "**GhostPorts may be opened with YubiKey alone**". Two-factor authentication is used when setting "**GhostPorts require YubiKey and Halo user password**".

Here are the steps for configuring GhostPorts access:

Step 1: Make sure you have the "**Enable GhostPorts Access**" checkbox enabled.

Step 2: Select the type of GhostPorts authentication desired for this user.

Step 3: Place the YubiKey into a USB port on your computer. Place your cursor into the field marked "**User YubiKey**". Initiate the YubiKey by lightly touching the top circle with the green centered light. The YubiKey key will enter its complete key value into the field.

Step 4: Click on "**Save**". You will notice a portion of the key value disappear. The first twelve characters of the key value will remain displayed in the key field.

Your GhostPorts user is now enabled.

Setting Network Access Policies

With your users now enabled, you may set firewall policies and rules that govern their network access to your cloud servers.

Select the "**Firewall Policies**" menu item under the "**Policies**" tab on the main Halo portal menu (https://portal.cloudpassage.com). Select an existing firewall police or add a new one. Enter a name for your new policy.

In the "**Inbound Rules**" section, set the "**Source**" option to include your GhostPorts user. Completing the Interface, Service, Connection State, Action and Log options, creates the network access rule for the GhostPorts user. Add a new rule for each of your GhostPorts users.

Disabling GhostPorts Access

Disabling GhostPorts access is simply done by unchecking the “Enable GhostPorts Acess” checkbox and clicking on "**Save**" from the same "**Edit (User Admin)**" page.

If you want to unlink a specific YubiKey from a designated administrator in order to allow reuse of that key by another administrator, follow these two steps:

Step 1: Clear the contents of the "**User YubiKey**" field by double-clicking inside the field and pressing the Delete key on your keyboard. Click "**Save**".

Step 2: Uncheck the "**Enable GhostPorts Access**" checkbox. Click "**Save**".

Your YubiKey is ready to be assigned and enabled for someone else.

Using GhostPorts (for GhostPorts users)

The first step you will do to start using GhostPorts is secure your assigned YubiKey from your site administrator.

You will have been assigned one of two GhostPorts access methods: single-factor authentication or two-factor authentication.

Single-Factor Authentication

To connect GhostPorts using single-factor authentication, follow these simple steps:

Step 1: Go to https://portal.cloudpassage.com/ghostports. You will see the following screen:

GhostPorts Token Generator screen

Step 2: Place your YubiKey into your USB port on your computer.

Step 3: Place your cursor in the blank field on the GhostPorts login page.

Step 4: Initiate your YubiKey by lightly touching the top of the key on the green-centered light for about one second. Do not press any other key on your keyboard.

USB Token Generator screen

You will see the field fill with the value generated by your YubiKey. After you are authenticated, the GhostPorts page will display the following:

Two-Factor Authentication

To connect to GhostPorts using two-factor authentication, go to https://portal.cloudpassage.com/login and enter your username and password. Follow these steps:

Step 1: Navigate to the **Settings**-->**GhostPorts** menu.

Follow steps 2 through 4 in the Single-Factor Authentication section above to complete the second step in GhostPorts authentication.

Congratulations! You are now ready to connect to cloud servers that are authorized by Halo for your access. Before attempt access, allow a minute or two for Halo to communicate your GhostPorts status to your cloud servers.