Multi-Factor Network Authentication

Setup Guide

Multi-Factor Network Authentication (also called GhostPorts) is a powerful security feature available with the Halo™ Workload Firewall Management security module. Multi-Factor Network Authentication enables strong protection of network access to your workloads or servers, with the flexibility to allow easy, secure access from anywhere.

Contents:

About GhostPorts Multi-Factor Network Authentication
   The Advantages
   How It Works

Administering Multi-Factor Network Authentication
   Set Up a GhostPorts User
   Create a Firewall Rule to Enable Server Access
   Disable a User's GhostPorts Access
   Change GhostPorts Session Length

Authenticating With GhostPorts
   Verify Your Phone Number (for SMS Authentication)
   Authenticate to GhostPorts
   Manually Close GhostPorts

About GhostPorts Multi-Factor Network Authentication

Multi-Factor Network Authentication is the most secure way to control access to services on cloud servers. For example, administrators can by default 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

Multi-Factor Network Authentication helps to eliminate the worry of attackers continually scanning your servers for open ports and attempting brute-force logins to those services. When Multi-Factor Network Authentication is enabled, the protected ports will be invisible to attackers when they scan your network. This makes it much harder for attackers to find a way in because they can't even see your open ports.
When a server administrator authenticates to the Multi-Factor Network Authentication gateway, the administrative ports on that administrator's server are open only for a limited amount of time, and only from the administrator's current IP address. Potentially malicious users attempting to access the server at the same time are denied.

By using Multi-Factor Network Authentication to provide secure access to your cloud servers, you are able to:

- Hide your sensitive applications from the world
- Enable secure access by remote employees no matter how mobile they are
- Combine the strength of multi-factor authentication with the convenience of software or hardware tokens
- Avoid the need for additional client software or infrastructure
- Work seamlessly across multiple elastic public, hybrid, and private cloud environments
- Fulfill compliance requirements for multiple security standards (PCI, HIPAA, FISMA, and others)
- Be up and running in less than 10 minutes

How it Works

Multi-Factor Network Authentication implements its strong multi-factor authentication by requiring both Halo login credentials and a second factor, involving a one-time password either transmitted by SMS text message or generated by a hardware device.

- For transmission by SMS, Halo generates a one-time password and sends it to the authenticating user's mobile phone in a text message.
- For a hardware device, CloudPassage supports the YubiKey® from Yubico. A YubiKey is a one-time-password generator packaged as a USB input device. YubiKey values are unique across all of Halo, so each YubiKey can be assigned to only one user at a time.

In the Halo portal, the Multi-Factor Network Authentication gateway is called GhostPorts. Once a Halo site administrator has enabled GhostPorts access for a user, authentication is a simple process. The GhostPorts user logs into the Halo portal and authenticates to GhostPorts, using either YubiKey or SMS code. In response, Halo temporarily opens the required ports on the required servers for access from that user's machine. The user then connects to the server outside of Halo for example through SSH or RDP.
To enable this targeted access, you set up firewall policies for server groups that include rules for GhostPorts users. The rules determine the specific services and ports to be opened for each GhostPorts user's access.

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

Administering Multi-Factor Network Authentication

Administering Multi-Factor Network Authentication for your cloud servers means creating and managing users with the appropriate privileges, and establishing appropriate firewall rules for the server groups that those users need to access. In summary, it is a two-step process:

1. **Set up one or more GhostPorts users**
   a. First, obtain the user's mobile phone number or purchase a YubiKey for the user.
   b. On the Site Administration page, create or edit a user: specify the authentication type, specify the user type, enable GhostPorts access, and activate the user.
      For details, see Set Up a GhostPorts User, next.

2. **Create a firewall rule to enable server access through GhostPorts**
   a. Create or edit a firewall policy for the server group that the GhostPorts user needs access to.
   b. In that policy, create a rule that grants that user (or all GhostPorts users) access to specific services and ports.
      For details, see Create a Firewall Rule to Enable Server Access, below.

*Note*: When you disable GhostPorts access for a user who has been using a YubiKey for authentication, you can then reassign that YubiKey to another GhostPorts user. See Disable a User's GhostPorts Access.
To set up yourself or another person as a GhostPorts user, you must be a Halo NetSec or Halo Professional user with site-administrator privileges.

Before creating the user, do this:

- If the person is to use SMS authentication, obtain that user's valid mobile phone number. Text messaging must be enabled for that mobile account.
- If the person is to use hardware authentication, acquire a YubiKey. You can order the keys directly from Yubico.

Then log into the Halo portal to create the user:

1. In the main menu, choose Site Administration and then select the Users tab.
2. Either click Add New User or select an existing user and click Edit for that user.
3. Specify and set up the user’s authentication method, as described below in Set Up Multi-Factor Authentication.

For more details on administering users, in the Halo Operations Guide see Managing Halo Users.

**Set Up Multi-Factor Authentication**

Authentication to GhostPorts requires a one-time password either transmitted to the user by SMS or generated by the user with a hardware device (YubiKey). Follow these steps to configure the authentication type:

1. Select the multi-factor authentication method desired for this user: **SMS code and password** or **YubiKey and password**, or both. For each one you select, the page expands to show new fields.

2. Set up the authentication method:

   **If you selected SMS code and password** —
   a. In the available field, enter the telephone number at which the user will receive the SMS authentication codes. It must be a valid mobile phone account with text messaging enabled.
   b. Click Save. The user receives an email invitation to use Multi-Factor Network Authentication (GhostPorts).

   **If you selected YubiKey and password** —
   a. Place the YubiKey into a USB port on your computer, with the metal contacts and circle facing upward ( ). Place your cursor into the User YubiKey field. 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.
   b. Click 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. The user receives an email invitation to use GhostPorts.

3. Click Save.

The user is now enabled for multi-factor authentication. The next step is to enable access to GhostPorts.

**Enable GhostPorts Access**
There are two classes of access privilege that you may set when creating or editing a user: portal access or GhostPorts access. Select either or both checkboxes on the Add New User / Edit User page, as appropriate.

- **Enable Halo Portal Access.** This class of access is for users that need to use the security-monitoring features of the Halo portal. If you select this checkbox, you then must decide whether the user is a standard Halo user or a site administrator. For information, in the *Halo Operations Guide* see Managing Halo Users.

- **Enable GhostPorts Access.** This class of access is for users that need secure access to servers. You must select at least this checkbox to give the user GhostPorts access. Then click *Add* or *Save*.

The user can now access GhostPorts to use Multi-Factor Network Authentication. The final task is to give the user access to specific services on specific servers, by adding rules to firewall policies.

### Create an Inbound Firewall Rule to Enable Server Access

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

In the Halo portal, select **Firewall Policies** under the **Policies** menu. Select an existing firewall policy or add a new one.

In the **Inbound Rules** section, create a rule and set the values of the **Interface** (Linux only), **Source**, **Service**, **Connection State** (Linux only), and **Action** options, as the example in the following table shows:

<table>
<thead>
<tr>
<th>Interface</th>
<th>Source</th>
<th>Service</th>
<th>Conn. State</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Windows: n.a.</em></td>
<td><em>GhostPorts username</em> (select from list under GhostPorts Users), or All GhostPorts users*</td>
<td><em>Windows: rdp (TCP/3389)</em></td>
<td><em>Windows: n.a.</em></td>
<td>ACCEPT</td>
</tr>
<tr>
<td><em>Linux: Hardware interface used to access this server</em></td>
<td><em>GhostPorts username</em> (select from list under GhostPorts Users), or All GhostPorts users*</td>
<td><em>Linux: ssh (TCP/22)</em></td>
<td><em>Linux: ANY</em></td>
<td></td>
</tr>
</tbody>
</table>

*Selecting this gives access under this firewall rule to all GhostPorts users.*
Make sure that the firewall policy is assigned to the server group that includes the servers your GhostPorts user needs access to.

You will need to add a new rule to the appropriate firewall policy for each of your GhostPorts users, or you can add a single rule to cover all GhostPorts users if they all need exactly the same access.

See *Workload Firewall Management Setup Guide* for detailed information on creating and modifying Halo firewalls.

### Disable a User's GhostPorts Access

You can disable GhostPorts access for any user by simply clearing the **Enable GhostPorts Access** checkbox and clicking **Save** on the Edit User page.

If the user's authentication type was YubiKey, that YubiKey is now unlinked from the user and is ready to be assigned to and enabled for someone else.

### Change GhostPorts Session Length

By default, Multi-Factor Network Authentication sessions expire after 4 hours unless the user manually closes GhostPorts before that time (see **Manually Close GhostPorts**). If you want to change that maximum session length, go to the **Advanced Settings** tab on the Site Administration page.

From the drop-down list under **GhostPorts**, select a time length from 1 hour to 24 hours. That expiration time will apply to all of your organization's Multi-Factor Network Authentication sessions.
If you are a GhostPorts-only user or a Halo user with GhostPorts access, you will have been assigned one of two multi-factor authentication methods: YubiKey plus Halo password, or SMS code plus Halo password. The process that you follow to authenticate is simple:

1. Prepare for authentication
   - For SMS authentication, log into the Halo portal to verify your authentication phone number. For detailed instructions, see Verify Your Phone Number (for SMS Authentication).
   - For YubiKey authentication, obtain your activated YubiKey device from your administrator.

2. Authenticate and access your servers
   - Using any computer anywhere, log into the Halo portal and authenticate to GhostPorts. For detailed instructions, see Authenticate to GhostPorts.
   - During a time window, access your servers directly from that same computer.
   - Optionally close GhostPorts when you are finished. For detailed instructions, see Manually Close GhostPorts.

Verify Your Phone Number (for SMS Authentication)

If you will be authenticating to GhostPorts with an SMS code, you first need to verify to Halo that the authentication phone number assigned to you is the correct one. The verification process includes demonstrating that the phone can receive a code from Halo.

**Step 1:** Go to https://portal.cloudpassage.com/login and enter your Halo username and password.

**Step 2:** Go to the Phone Verification page:
   - If you are a GhostPorts user but not a Halo user, you are brought directly to the page.
   - If you are both a Halo user and GhostPorts user, after you log in, Halo sends an SMS message containing a 6-digit authentication code to your phone, then displays the Phone Verification page.

**Step 3:** In the Phone Verification form, inspect the partially masked phone number, of the form XXX-XXX-XX67, to verify that the last two digits displayed match the number of the phone that you are authorized to use to authenticate to Halo.

**Step 4:** If the phone number matches:
Click **Send Verification Code**. Halo sends a 6-digit verification code to the phone number associated with your Halo account.

- When you receive the message on your phone, copy the six-digit verification code into the **Verification Code** field on the GhostPorts page, then click **Submit**.

---

**Multi-Factor Authentication with SMS**

**Phone Verification**

An SMS containing a 6-digit verification code has been sent to your phone. The code is valid for 5 minutes after it is sent. Enter the code in the box below and click **Submit** to complete the verification of your phone number.

<table>
<thead>
<tr>
<th>Verification Code</th>
<th>Submit</th>
<th>04:58</th>
</tr>
</thead>
</table>

---

**Note:** You have 5 minutes from the time you click **Send Verification Code** until the code expires. If you do not complete this step within that time, you can click **Send Verification Code** again to have another code sent to you.

If Halo receives the code successfully, it displays the following on the GhostPorts page:

Your authentication phone number is verified, and you now can log into GhostPorts to access your servers.

---

**Authenticate to GhostPorts**

**Note:** If you have logged into the Halo portal using multi-factor authentication or through single sign-on, and if you click the **GhostPorts** button within one minute of logging into Halo, you are immediately authenticated to GhostPorts and you don't have to follow the procedure described in this section. But if you wait for over a minute before clicking **GhostPorts**, or if you have logged into Halo using your Halo password, you will need to authenticate to GhostPorts as described here.

To authenticate to GhostPorts, follow these steps:

1. Log into the Halo portal.

2. Go to the Open GhostPorts page:
   - If you are a GhostPorts-only user, you are brought directly to the GhostPorts is Closed page.
   - If you are both a Halo user and a GhostPorts user, click the closed **GhostPorts** button ( ) in the Halo portal menu bar. The GhostPorts is Closed page appears — for SMS authentication, for YubiKey, or for both, depending on which authentication types you are enabled for.

3. Click either **Send SMS** or **Use YubiKey**.
**Authenticate with SMS:**

- If you clicked **Send SMS**, an SMS message containing an authentication code has been sent to your phone. When it arrives, enter it into the **Authentication Code** field.
  
  **Note:** The code is sent by SMS, and normal text-messaging charges for your account may apply.

- Click **Submit** to send the SMS authentication code to GhostPorts.
  
  **Note:** You have 5 minutes from the time you receive the code to enter it into the field and click **Submit**. If you do not send the code before it expires, you can click **Re-send Authentication Code** to receive another code.

**Authenticate with a YubiKey:**

- If you clicked **Use YubiKey**, place your YubiKey into the USB port on your computer, with the metal contacts and circle facing upward 🔄.

- Click within the **Enter YubiKey** field to make it active.

- 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. You will see the field fill with the value generated by your YubiKey.

- Click **Submit** to send the YubiKey authentication code to GhostPorts.

After you have authenticated successfully, the GhostPorts is Open page displays a success banner:
Also, in the portal page header, the GhostPorts button now indicates that GhostPorts is open.

**Congratulations!** You are now ready to connect to cloud servers that are authorized by Halo for your access. Before attempting access, allow a few moments for Halo to communicate your multi-factor authentication status to your cloud servers.

### Manually Close GhostPorts

If you are accessing a server through Multi-Factor Network Authentication, that access will automatically terminate and the port you are using will be closed after the session expiration time is reached (by default, four hours after you opened GhostPorts). Note that logging out of the portal does not close your open GhostPorts.

If you want to maintain the highest security on your servers, you can optionally close GhostPorts before the time limit, as soon as you no longer need access. When you have finished using your servers, click the open **GhostPorts** button in the Halo portal page header. The GhostPorts is Open page appears:

![GhostPorts are Open](image)

Click **Close GhostPorts** to immediately terminate permission to log into the server from your IP address.

*Note:* If another GhostPorts user is also accessing the same ports on the same server group from the same IP address, the ports won't be closed until that user either manually closes them or is timed out.

After you have successfully closed the ports, the GhostPorts is Closed page displays a success banner:

![GhostPorts are Closed](image)

---

Copyright ©2016 CloudPassage Inc. All rights reserved. CloudPassage® and Halo® are registered trademarks of CloudPassage, Inc.