

Disaster Recovery Appliance VMware User Guide

Arcserve UDP Cloud Direct

v6.2.2

arcserve[®]

Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the "Documentation") is for your informational purposes only and is subject to change or withdrawal by Arcserve at any time. This Documentation is proprietary information of Arcserve and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Arcserve.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Arcserve copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Arcserve that all copies and partial copies of the Documentation have been returned to Arcserve or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, ARCSERVE PROVIDES THIS DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL ARCSERVE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF ARCSERVE IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Arcserve.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

© 2017 Arcserve, including its affiliates and subsidiaries. All rights reserved. Any third party trademarks or copyrights are the property of their respective owners.

Contact Arcserve Support

The Arcserve Support team offers a rich set of resources for resolving your technical issues and provides easy access to important product information.

[Contact Support](#)

With Arcserve Support:

- You can get in direct touch with the same library of information that is shared internally by our Arcserve Support experts. This site provides you with access to our knowledge-base (KB) documents. From here you easily search for and find the product-related KB articles that contains the field-tested solutions for many top issues and common problems.
- You can use our Live Chat link to instantly launch a real-time conversation between you and the Arcserve Support team. With Live Chat, you can get immediate answers to your concerns and questions, while still maintaining access to the product.
- You can participate in the Arcserve Support Global User Community to ask and answer questions, share tips and tricks, discuss the best practices and participate in conversations with your peers.
- You can open a support ticket. By opening a support ticket online, you can expect a callback from one of our experts in the product area you are inquiring about.
- You can access other helpful resources appropriate for your Arcserve Support product.

Contents

Chapter 1: Working With Disaster Recovery Appliance for VMware	1
Verify Prerequisites	2
Download Disaster Recovery Appliance for VMware	3
Deploy Disaster Recovery Appliance On-premises for VMware	5
Configure the Network Interfaces	9
Complete Disaster Recovery Appliance Configuration in Portal	18

Chapter 1: Working With Disaster Recovery Appliance for VMware

The Arcserve UDP Cloud Direct Disaster Recovery Appliance is a virtual appliance that enables Site-to-Site virtual private network (VPN) connectivity between a customer's On-premises environment and recovered systems in the UDP Cloud Direct environment.

This section contains the following topics:

Verify Prerequisites	2
Download Disaster Recovery Appliance for VMware	3
Deploy Disaster Recovery Appliance On-premises for VMware	5
Configure the Network Interfaces	9
Complete Disaster Recovery Appliance Configuration in Portal	18

Verify Prerequisites

Prerequisites for deploying the UDP Cloud Direct Disaster Recovery Appliance:

- Virtual compute resources (runs on VMware vSphere, Microsoft Hyper-V, and Oracle VirtualBox)
 - ◆ 512 MB RAM
 - ◆ 2 GB HDD
- IP address for the internal network interface.
- Publicly accessible IP address (not behind a firewall or NAT) for external connectivity.

Download Disaster Recovery Appliance for VMware

Follow these steps:

1. Log into the UDP Cloud Direct Portal.

Login

Account Email

Password

Sign In

[Click here for Ping Identity](#)
[Forgot your password?](#)

2. Click the **Disaster Recovery** tab.

arcserve® UDP CLOUD DIRECT

Systems

VMware

Disaster Recovery

3. Click the **Configure & IP Takeover** from the *Connect Site-to-Site* box.

Connect Site-to-Site

Access your active VMs by connecting your local network with our cloud network. Use this if you're in the office (or have access to it through your company VPN) and if have a partial disaster with only some of the systems on your site down.

Configuration & IP Takeover

Note: At least one virtual instance must be activated to see the connectivity options.

4. Download the UDP Cloud Direct Disaster Recovery Appliance for VMware.


Site-to-Site Setup



1.
Deploy Appliance

2. (optional)
Configure IP Takeover


Download

 For VMware

[Instructions](#)

 For VirtualBox

[Instructions](#)

 For Hyper-V

[Instructions](#)

Deploy Disaster Recovery Appliance On-premises for VMware

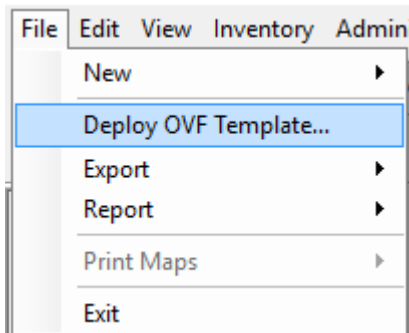
After download, you need to deploy UDP Cloud Direct disaster recovery appliance On-premises for VMware.

Follow these steps:

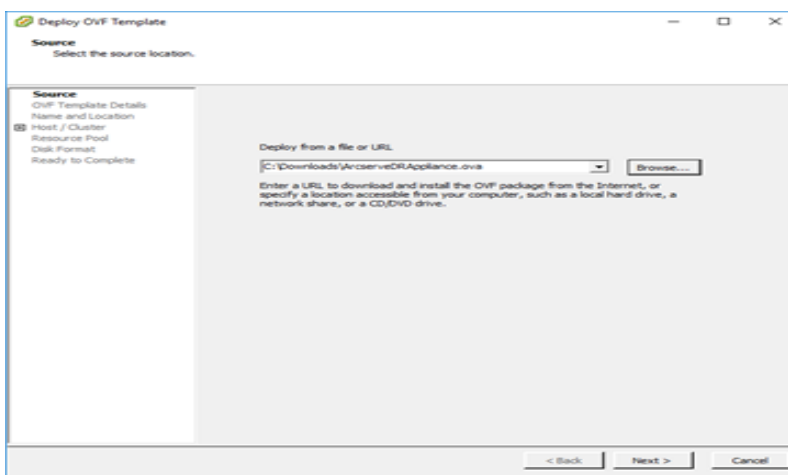
1. Open VMware vSphere Client.



2. Select File -> Deploy OVF Template...



3. Browse to specify the location of the UDP Cloud Direct Disaster Recovery Appliance download, and click **Next**.



4. Continue deploying the virtual appliance by selecting the default settings and clicking **Next** on every screen. When all the settings have been selected, click **Finish** to import the virtual appliance.

5. Once the virtual appliance is imported, click **Edit virtual machine settings** from Basic Tasks.

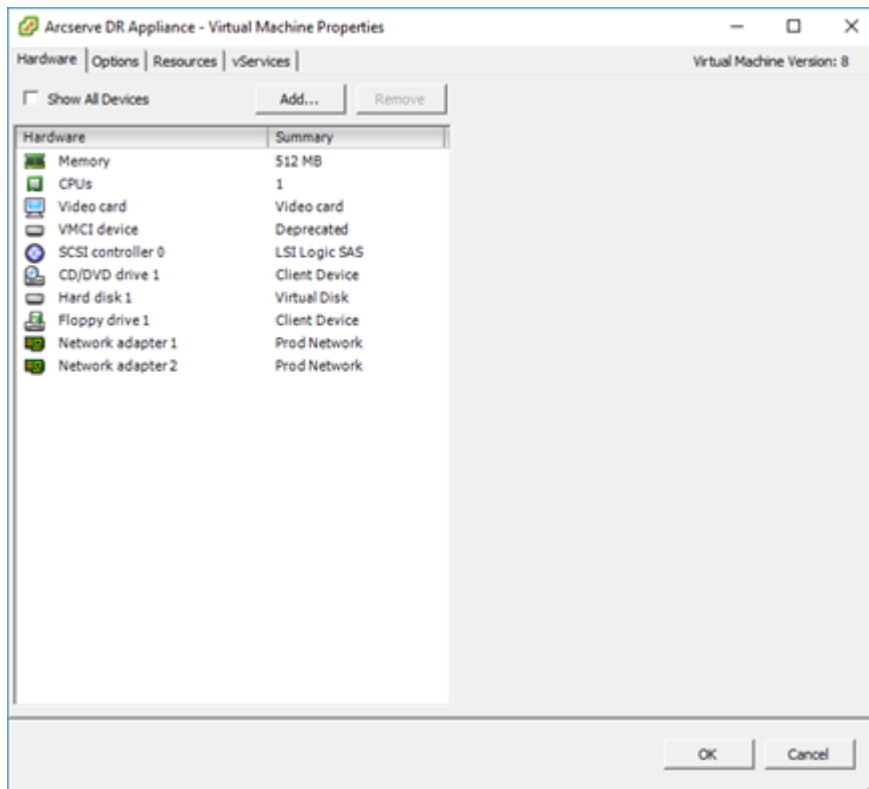
Basic Tasks

 **Power on the virtual machine**

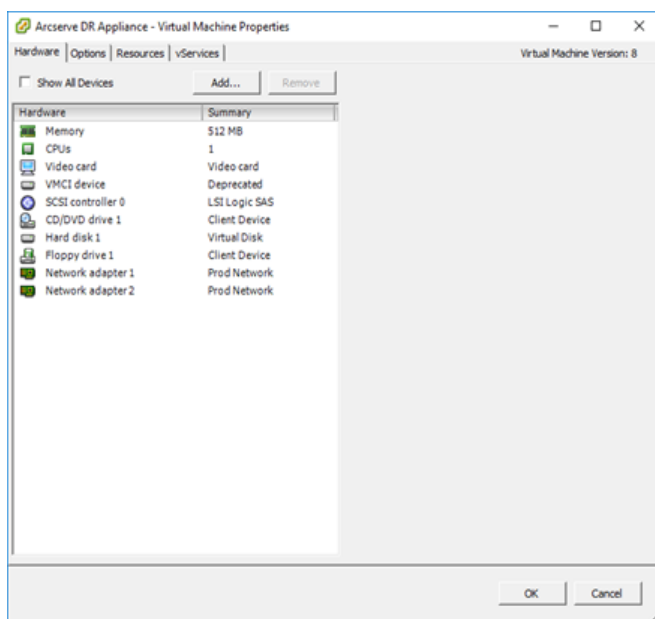
 **Edit virtual machine settings**

6. Configure the two network adapters.

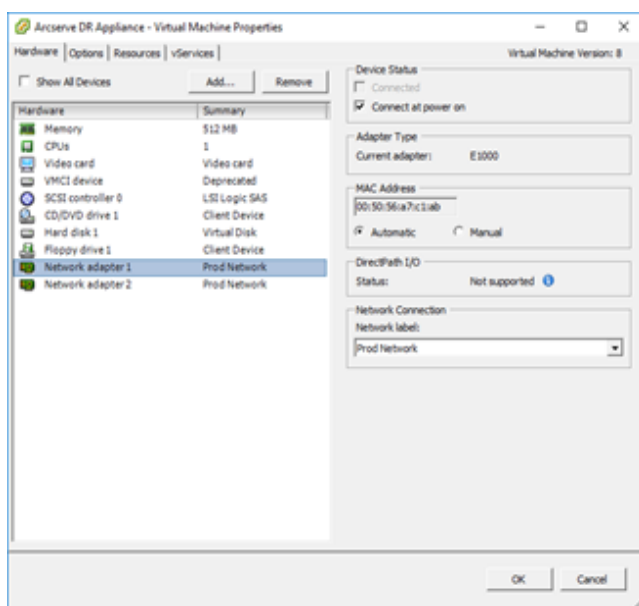
Note: One adapter should be on your internal network, while the other should be publicly accessible (not behind a firewall or NAT).



- Configure Network Adapter 1 to use your internal network.



- Configure Network Adapter 2 to use the external publicly accessible network.



7. Click **OK** to save the changes to the appliance settings.
8. Now, start the imported appliance by clicking **Power on the virtual machine** from Basic Tasks.



9. When the virtual appliance finishes booting, click the **Console** tab.

The Welcome screen appears.



Configure the Network Interfaces

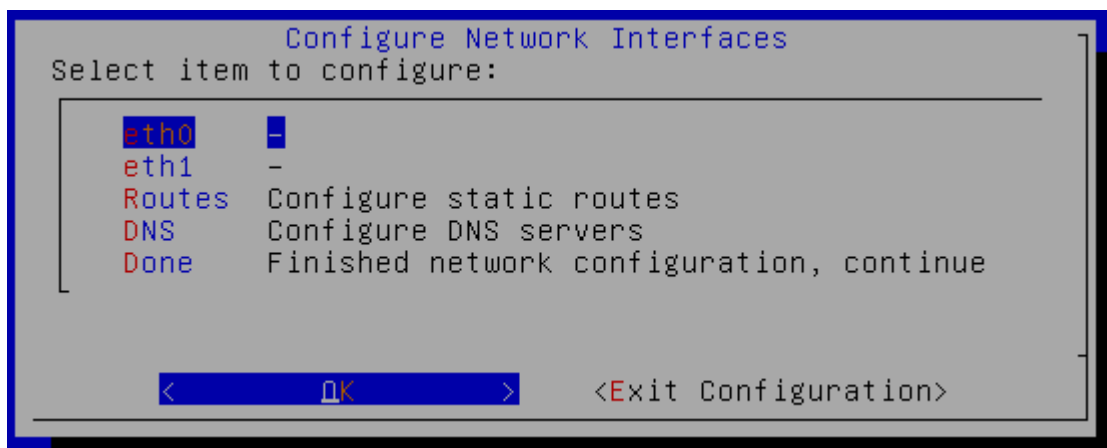
After deployment, you need to configure the network interfaces of the UDP Cloud Direct Disaster Recovery Appliance.

Follow these steps:

1. As the Welcome screen appears after successful deployment of the virtual appliance, press **Enter**.

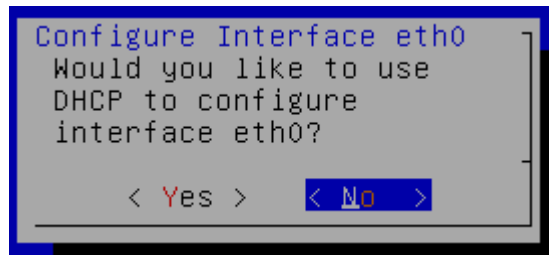


You are led to the menu to configure the network interfaces. Here, you will configure the IP address for each network interfaces and also the static routes and DNS server addresses.

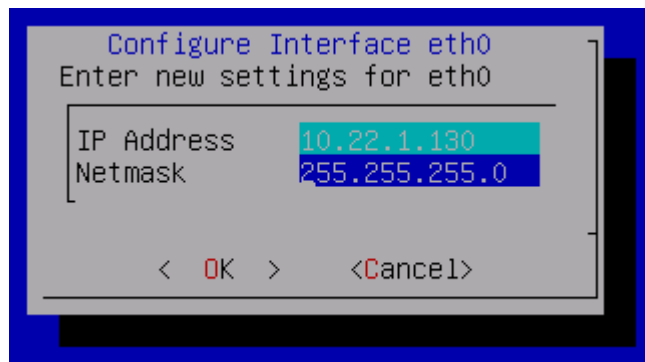
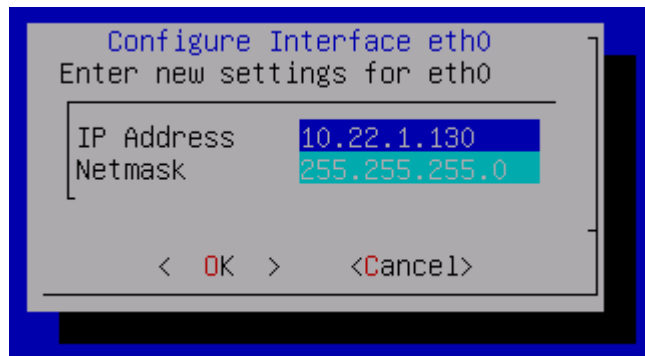


2. Perform the following steps to configure interface eth0:

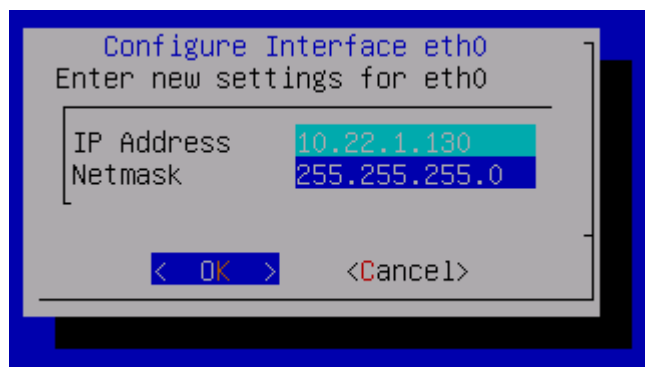
- a. Select **No** when asked if you want to use DHCP with eth0.



- b. To configure the IP address and subnet mask for eth0, use the arrow keys to move between the IP address and Netmask settings.

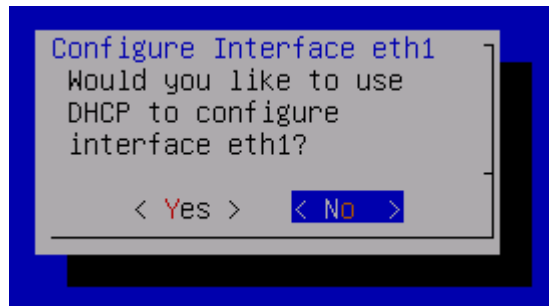


- c. Press the **Tab** key to select **OK**, and then press **Enter** to return to the main menu.

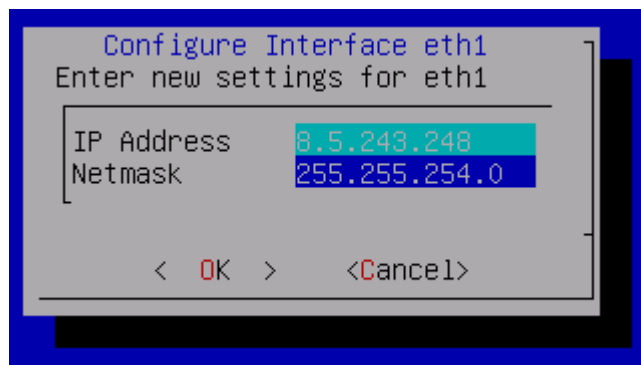
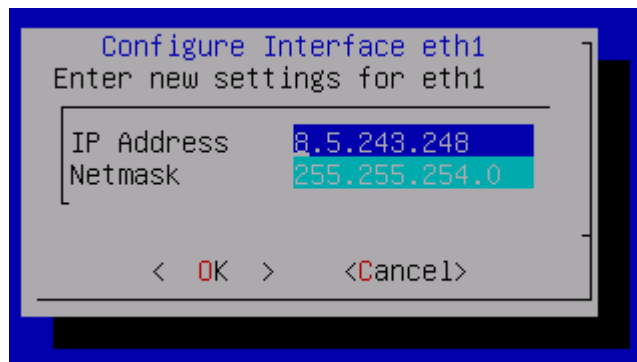


3. Perform the following steps to configure interface eth1:

- a. Select **No** when asked if you want to use DHCP with eth1.

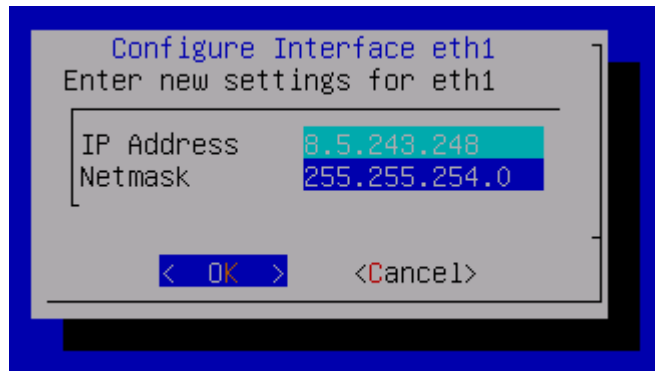


- b. Configure the IP address and subnet mask for eth1. Use the arrow keys to move between the IP address and Netmask settings.

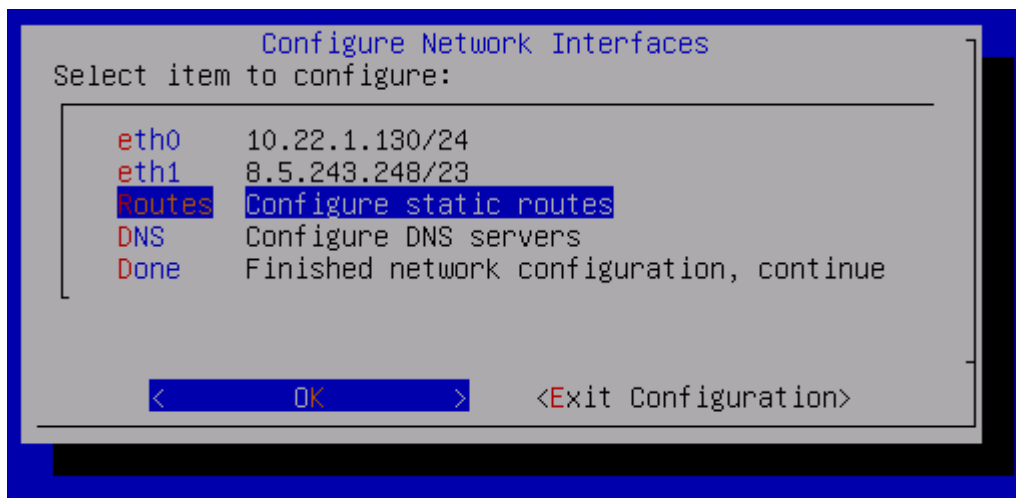


- c. Press the **Tab** key to select **OK**, and press **Enter** to return to the main

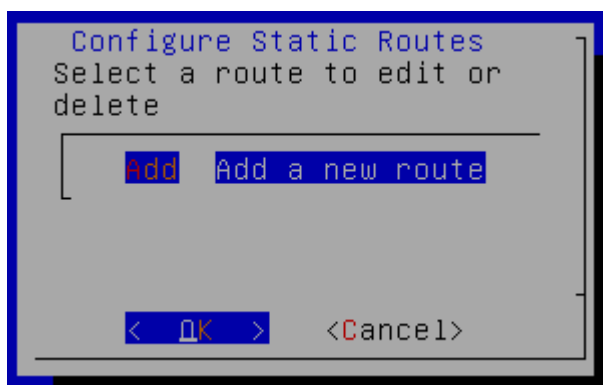
menu.



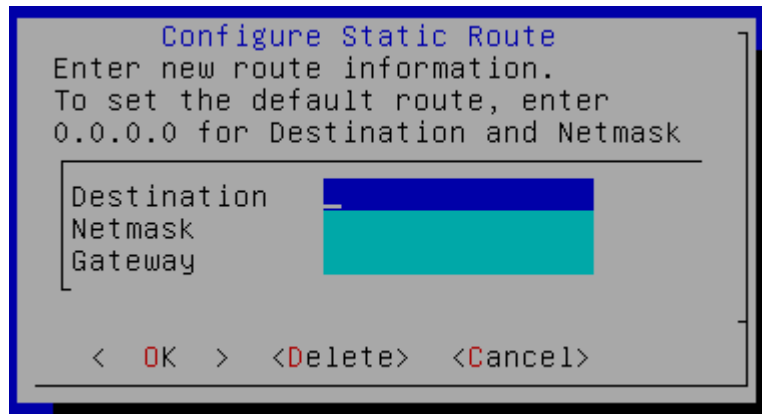
4. Perform the following steps to configure static routes::



We recommend to add default static routes for both the internal and external gateways.



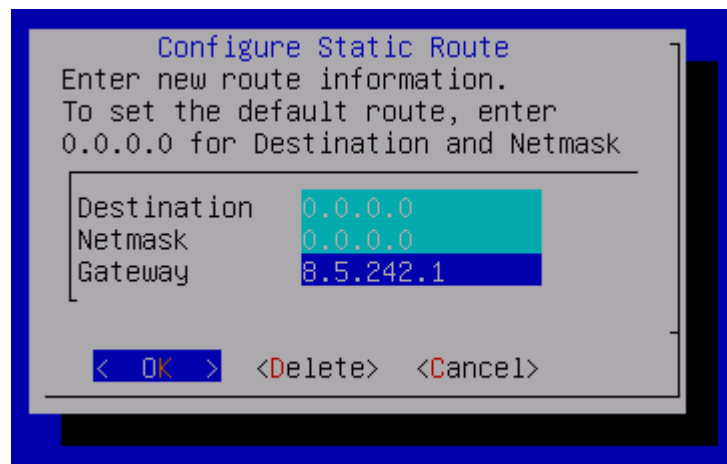
- a. Select **Add** to provide a new static route.



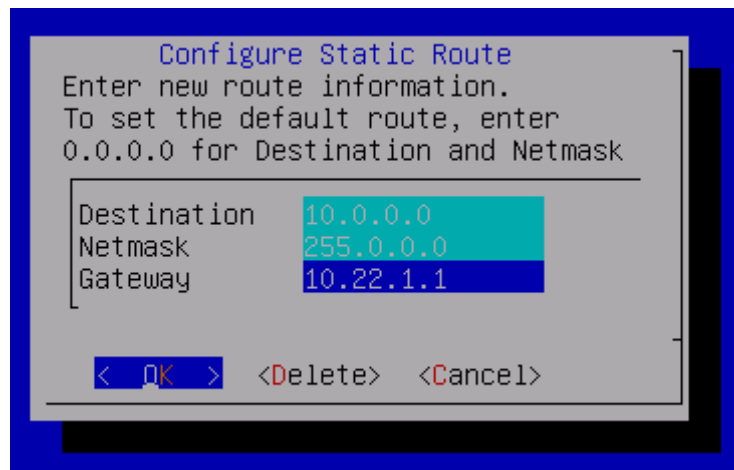
- b. Configure a static route for the external gateway using the following steps:

We recommend to configure a default route, with a value of 0.0.0.0 for the destination and a value of 0.0.0.0 for the netmask.

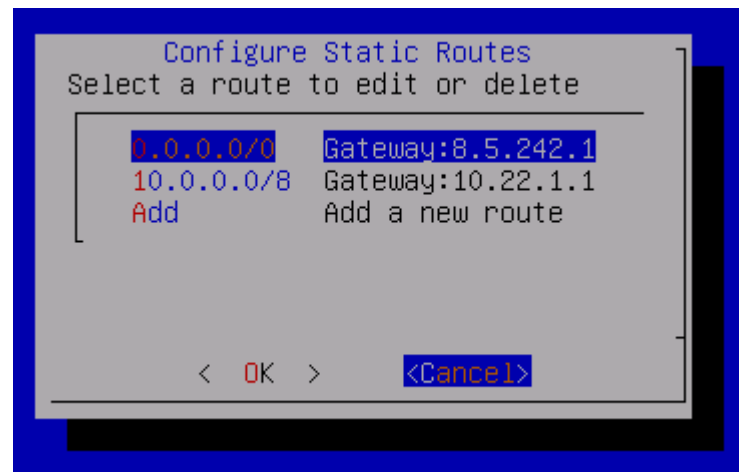
- i. Enter the IP address of your external gateway.



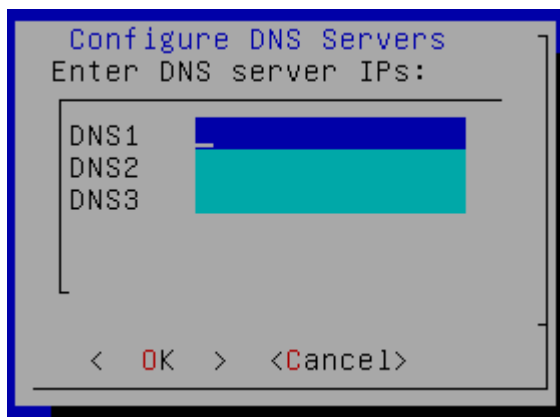
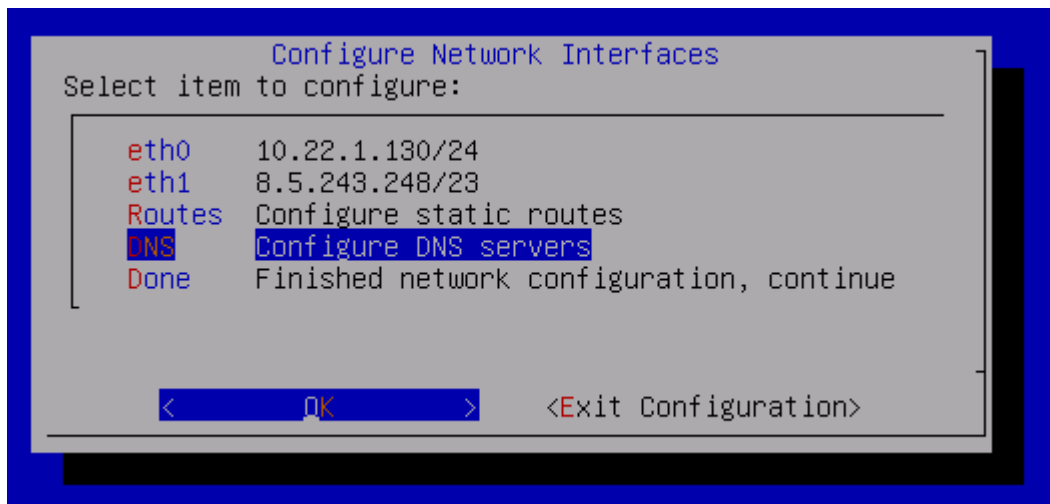
- ii. Press the **Tab** key to select **OK** to return to the menu to configure static routes.
- c. Configure a static route for the internal gateway.



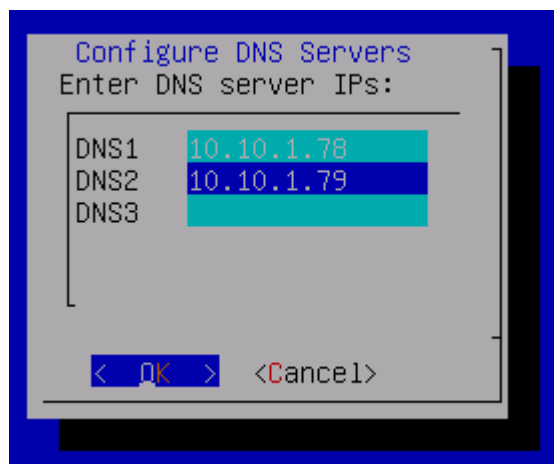
- i. Enter the IP address of your external gateway.
- ii. Press the **Tab** key to select **OK** to return to the menu to configure static routes.



- d. With the static routes configured, press the **Tab** key to select **Cancel** to return to the main menu.
5. Perform the following steps to configure DNS servers:



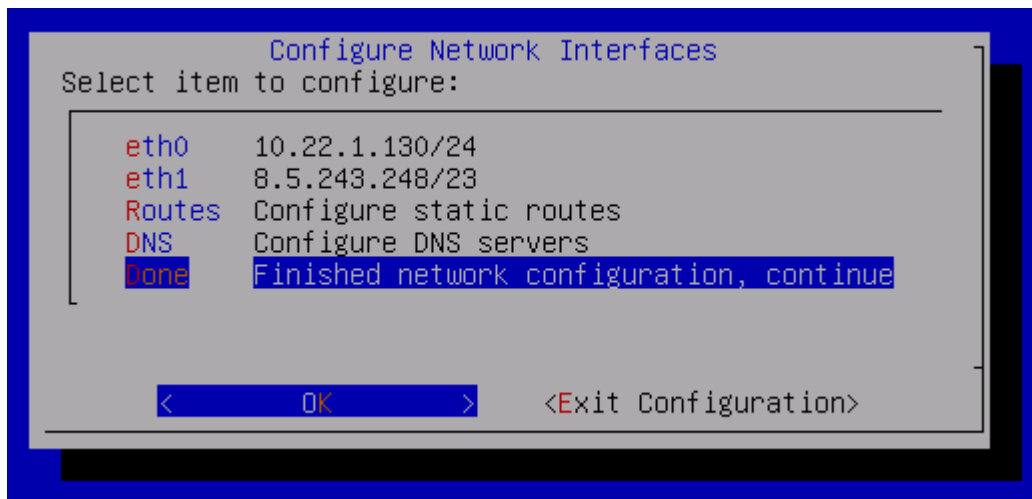
- a. Enter the DNS server IP addresses. Use the arrow keys to move between the DNS server IP address entries.



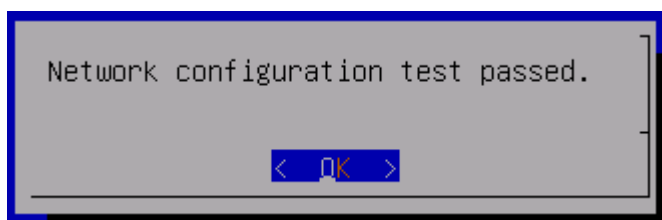
- b. With the DNS server IP addresses entered, press the **Tab** key to select **OK** to return to the main menu.

- When you have finished configuring the network interfaces, select **Done** from the menu.
- Press the **Tab** key to select **OK** and then press **Enter**.

A test is performed to verify whether the network connectivity to the internet is working properly.

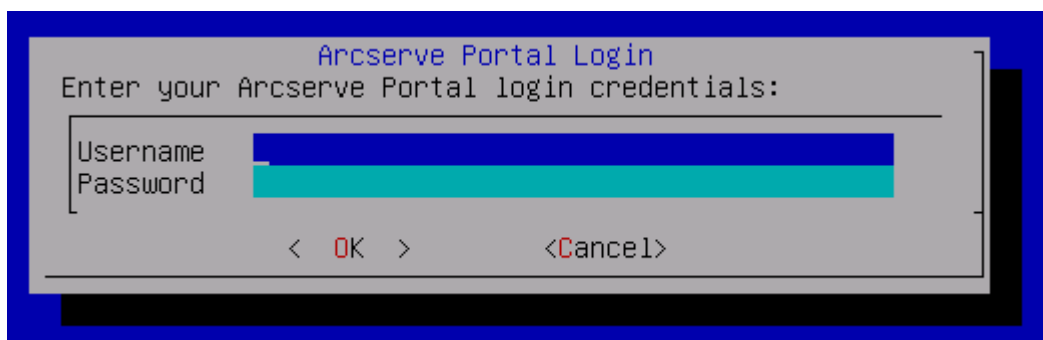


A successful completion of the test displays the following message.



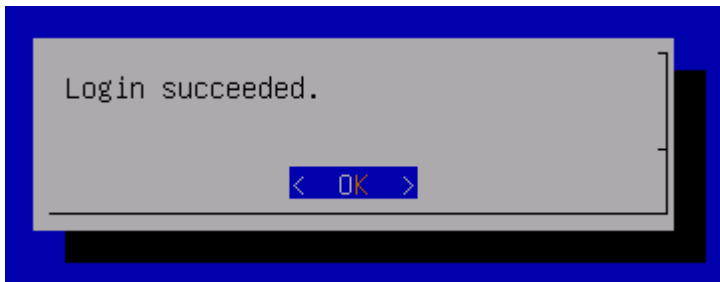
- Select **OK** to acknowledge the success test.

You will be prompted to enter your UDP Cloud Direct Portal login credentials.



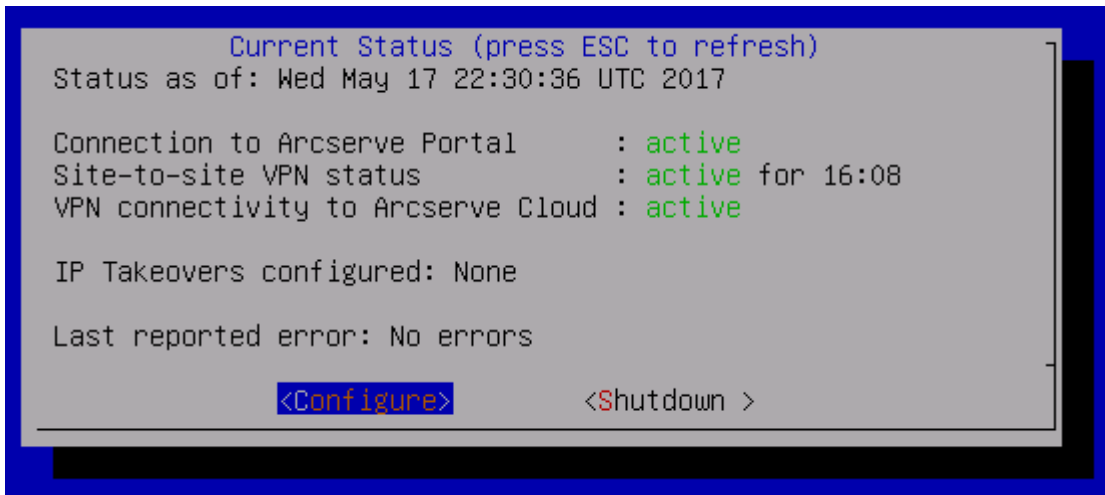
- Enter the credentials and select **OK**.

The successful validation of your UDP Cloud Direct Portal credentials results into the following message:



10. Select **OK** to acknowledge the message.

The connection status of the UDP Cloud Direct Disaster Recovery Appliance is displayed.



Complete Disaster Recovery Appliance Configuration in Portal

Now, you need to complete the configuration in the UDP Cloud Direct Portal.

Follow these steps:

1. Open [link](#) and enter login credentials.

Login

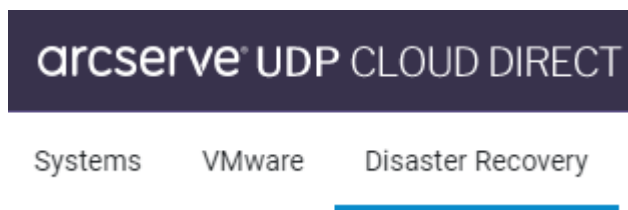
Account Email

Password

Sign In

[Click here for Ping Identity](#)
[Forgot your password?](#)

2. From the UDP Cloud Direct Portal, click the **Disaster Recovery** tab.



3. Click **Configuration & IP Takeover** available within the *Connect Site-to-Site* box.

Connect Site-to-Site

Access your active VMs by connecting your local network with our cloud network. Use this if you're in the office (or have access to it through your company VPN) and if have a partial disaster with only some of the systems on your site down.

[Configuration & IP Takeover](#)

4. Enter the external IP address of the UDP Cloud Direct Disaster Recovery Appliance that you just installed, and the network range of your internal network.

Configure

Appliance Public IP

The public IP address of your VPN gateway

Private IP Range

Your internal network range in CIDR format.
Ex: 192.168.1.0/24

Save Configuration

Delete Configuration

5. Click **Save Configuration**.

Within a few minutes, the UDP Cloud Direct Disaster Recovery Appliance should receive the configuration update from the UDP Cloud Direct Portal and activate your Site-to-Site VPN. The status of the Site-to-Site VPN connection should be reflected in the UDP Cloud Direct Portal with a green vertical bar indicating a successful connection.

Connect Site-to-Site

Access your active VMs by connecting your local network with our cloud network. Use this if you're in the office (or have access to it through your company VPN) and if have a partial disaster with only some of the systems on your site down.

Configuration & IP Takeover

Note: For other machines on your network to be able to access those within your UDP Cloud Direct Infrastructure, you will need to add a static route. This can either be done individually on each server that will connect to the UDP Cloud Direct Infrastructure or on your router.