Veeam PN 2.1

Version 2.1

User Guide

November, 2019

NOTE:

Read the End User Software License Agreement before using the accompanying software programs. Using any part of the software indicates that you accept the terms of the End User Software License Agreement.

Contents

Contacting Veeam Software

At Veeam Software we value the feedback from our customers. It is important not only to help you quickly with your technical issues, but it is our mission to listen to your input and build products that incorporate your suggestions.

Customer Support

Should you have a technical concern, suggestion or question, visit the Veeam Customer Support Portal at www.veeam.com/support.html to open a case, search our knowledge base, reference documentation, manage your license or obtain the latest product release.

Company Contacts

For the most up to date information about company contacts and offices location, visit www.veeam.com/contacts.html.

Online Support

If you have any questions about Veeam products, you can use the following resources:

- Full documentation set: www.veeam.com/documentation-guides-datasheets.html
- Community forum at forums.veeam.com

About This Guide

This user guide provides information about Veeam PN 2.1.

Intended Audience

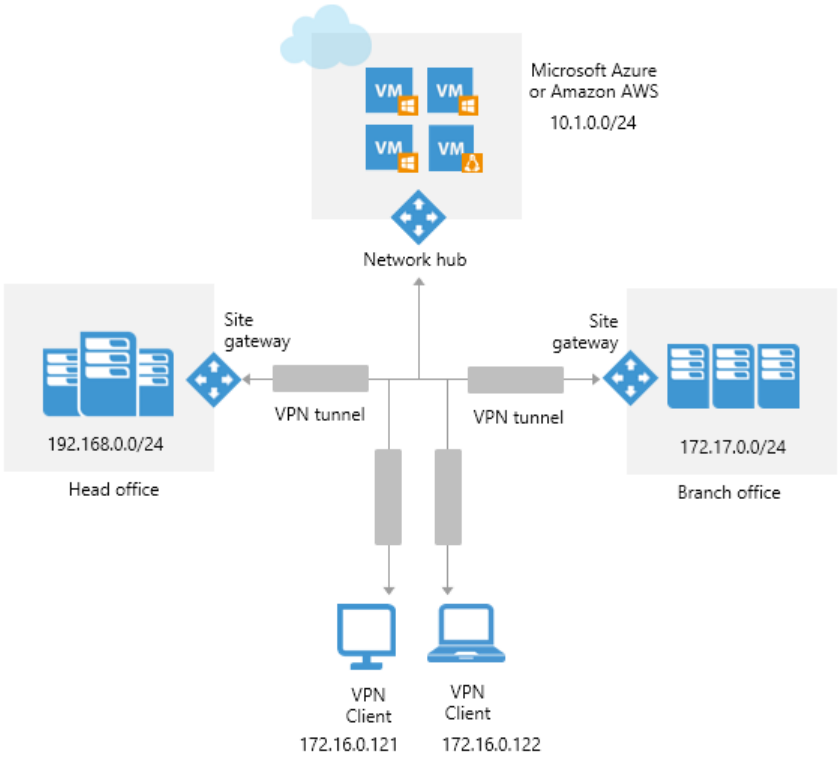
The user guide is intended for anyone who wants to use Veeam PN to implement site-to-site and point-to-site VPN scenarios for Microsoft Azure, Amazon AWS and on-premises networks.

About Veeam PN

Veeam Powered Network (Veeam PN) is a free Veeam solution that supplements the Veeam functionality of restore to cloud repositories (Azure, Amazon EC2) and allows you to create a VPN connection between remote sites over the public network. You can use Veeam PN to implement the following scenarios:

- Microsoft Azure
  - Set up a site-to-site VPN between company offices and a Microsoft Azure network to which VMs restored in Microsoft Azure are connected.
  - Set up a point-to-site VPN between remote computers and a Microsoft Azure network to which VMs restored in Microsoft Azure are connected.
  - Allow remote users to get access to a company network through a Microsoft Azure network.
- Amazon AWS
  - Set up a site-to-site VPN between company offices and an Amazon AWS network to which VMs restored in Amazon EC2 are connected.
  - Set up a point-to-site VPN between remote computers and an Amazon AWS network to which VMs restored in Amazon EC2 are connected.
  - Allow remote users to get access to a company network through an Amazon AWS network.

Veeam PN lets you set up VPN connections between Microsoft Azure or Amazon AWS networks and on-premises networks. The solution is based on the WireGuard®* and OpenVPN technology and features a web-based interface that simplifies VPN configuration and administration.



* WireGuard is a registered trademark of Jason A. Donenfeld.

Usage Scenarios

Veeam PN allows you to configure two types of VPN connections:

- Site-to-site VPN
- Point-to-site VPN

Site-to-site VPN

A site-to-site VPN allows you to establish a secure connection between remote networks over a public network. You can implement the site-to-site VPN scenario if you need to join on-premises networks and private cloud networks in Microsoft Azure or Amazon AWS. For example, if some of your VMs are restored to Microsoft Azure or Amazon EC2, you can join the cloud network to which these VMs are connected with company on-premises networks.

Veeam PN also lets you set up a VPN exclusively for on-premises networks. This scenario lets you extend the company network and make resources in one remote site available to machines and users in another remote site. For example, you can join several company networks into a single private network or allow machines and users from company branch offices to connect to the company datacenter.

Technology

Site-to-site VPN functionality of Veeam PN is based on WireGuard technology. WireGuard does not support TCP, but Veeam PN eliminates this limitation by tunneling UDP encrypted traffic in TCP tunnel. WireGuard has significant performance advantage compared to OpenVPN:

- It is implemented inside the Linux kernel, so no userspace-kernel cycles wasted.
- WIreGuard scales up to all available CPU's (not stuck only on one CPU as in case of OpenVPN).

To learn more about WireGuard functionality, see the WireGuard's White Paper.

Topology

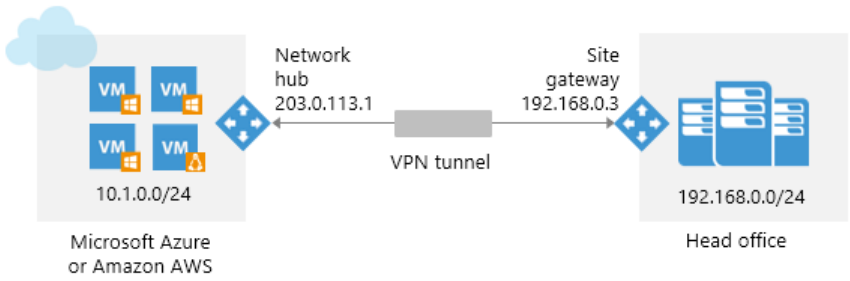
In the VPN, all traffic between remote networks is routed over a secure communication channel — VPN tunnel. To establish a VPN tunnel, Veeam PN uses its appliances: network hub and site gateways.

The Veeam PN VPN is organized around the **network hub**. The network hub is the core of the VPN infrastructure. The hub is responsible for all background work: traffic routing, encryption, user management, authentication and so on.

The network hub is accessible from all remote networks added to the VPN. Veeam PN supports two deployment scenarios for the network hub: you can deploy the network hub in Microsoft Azure or in an on-premises network.

The network hub acts as one point of the VPN tunnel. To create the other point of the VPN tunnel, you must deploy a **site gateway** in a remote network that you plan to add to the VPN. The site gateway is a virtual appliance that establishes a secure connection with the network hub.

In the site-to-site scenario, all traffic in the VPN is handled by the network hub and site gateways. You do not need to additionally configure VPN settings on standalone machines in remote sites.



The VPN organized with Veeam PN has the star network topology. All traffic in the VPN is always routed through the network hub. For example, you add three remote networks to the VPN: 2 on-premises networks and

a cloud network in Microsoft Azure. With such configuration, you must deploy the network hub in Microsoft Azure, and a site gateway in each on-premises network. All traffic will be routed through the network hub in Microsoft Azure, even if machines from one on-premises network need to communicate with machines in the other on-premises network.

DNS forwarding

Since version 2.0, Veeam PN supports DNS forwarding and client configuration:

- Fully automatic detection of DNS settings
- Endpoint clients automatically receive DNS settings to resolve all FQDNs in all connected sites

In the network hub console, you can disable DNS forwarding, and see the list of DNS servers and DNS suffixes for configured sites. For details, see Enabling and Disabling DNS.

> **NOTE:**
>
> To bring DNS forwarding feature on site configuration an administrator should change configuration of local DNS server, so all requests to domain suffixes of other sites should be forwarded to local Veeam PN site appliance or change DNS server IP address settings individually on each client machine.

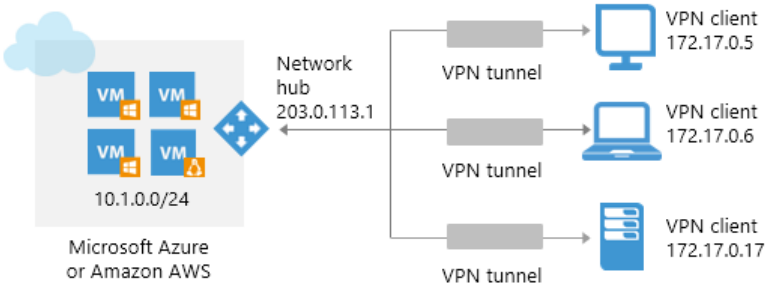
Point-to-site VPN

Overview

A point-to-site VPN allows you to establish a secure connection from a standalone computer to a remote network. You can implement the point-to-site scenario, for example, if you want to allow remote users to communicate with machines restored to Microsoft Azure and Amazon EC2. You may also implement this scenario if you want to provide remote users with access to resources in an on-premises company network.

As well as in the site-to-site scenario, in the point-to-site scenario the VPN is organized around the **network hub**. The network hub is placed in a network to which remote users must gain access. You can deploy the network hub in Microsoft Azure, Amazon AWS or in an on-premises network, depending on the usage scenario.

To let a remote user access the VPN organized with Veeam PN, you must set up **OpenVPN** on the user computer and configure it in a proper way. The user side does not require a site gateway or a public-facing IP address or DNS name. Whenever a remote user needs to communicate with a machine in the VPN, it establishes a connection to the network hub. The network hub then routes traffic to necessary resources in the VPN.



DNS forwarding

Since version 2.0, Veeam PN supports DNS forwarding and client configuration:

- Fully automatic detection of DNS settings
- Endpoint clients automatically receive DNS settings to resolve all FQDNs in all connected sites

> **NOTE:**
>
> To bring DNS forwarding feature on site configuration an administrator should change configuration of local DNS server, so all requests to domain suffixes of other sites should be forwarded to local Veeam PN site appliance or change DNS server IP address settings individually on each client machine.

System Requirements

Network Hub in Microsoft Azure

A1 VM size (1 core, 1.75 GiB RAM, 70 GB of disk space) is minimum. For more information about VM sizes in Microsoft Azure, see https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-windows-sizes.

Network Hub in Amazon AWS

t2.micro instance (1 vCPU, 1GiB RAM). For more information about EC2 instance types, see https://aws.amazon.com/ec2/instance-types/.

Network Hub in On-Premises Network

- Platform: VMware vSphere ESXi host/cluster 5.0 or later (hardware version 8 and later).
- Host RAM: 1 GB.
- Appliance disk size: 3.9 GB (thin-provisioned disk) or 16 GB (thick-provisioned disk).

Site Gateways

Appliance disk size: 3.9 GB (thin-provisioned disk) or 16 GB (thick-provisioned disk).

Standalone Computers

See system requirements to OpenVPN clients: https://openvpn.net/index.php/open-source/documentation/install.html.

Web Browsers

To access Veeam PN portals, you can use any of the following web browsers: Microsoft Internet Explorer 11 or later, Microsoft Edge updated for KB4486996 (OS Build 16299.967) or later, Mozilla Firefox 56 or later, Google Chrome 62 or later.

Networking Schemes

Networks that you add to the VPN with Veeam PN must have different IP schemes. Otherwise you will need to configure routing settings manually.

Used Ports

Make sure that you open the required ports, listed below.

From	To	Protocol	Port	Notes
Site gateways	Network hub	TCP/UDP	1194	Default port on which the network hub listens for site gateway connections. You can change the port in the network hub settings. For details, see Configuring VPN Settings.
Standalone computers	Network hub	TCP/UDP	6179	Default port on which the network hub listens for standalone computers connections. You can change the port in the network hub settings. For details, see Configuring VPN Settings.
Browser	Network hub or site gateway	HTTPS	443	Port used to communicate with the network hub or site gateway portal.
Client machine	Network hub or site gateway	SSH	22	[Optional] Default SSH port used as a control channel from the client machine to the network hub or site gateway appliance.
	DNS server	UDP	53	Port used for communication with the DNS server.

Deployment and Configuration

To set up the VPN infrastructure with Veeam PN and enable secure communication between remote sites and users, you must perform the following steps:

Site-to-Site Scenario

1. **Deploy and configure the network hub**.

   You must deploy the network hub in Microsoft Azure, Amazon AWS or in an on-premises site. The network hub is the core of the VPN infrastructure. The network hub manages incoming and outgoing traffic and provides clients with access to resources in the VPN. For more information, see Deploying Network Hub.

2. **Register Veeam PN clients.**

   You must register clients in the network hub portal. In the site-to-site scenario, clients are on-premises networks that you add to the VPN. For more information, see Registering Clients.

3. **Deploy and configure site gateways.**

   You must deploy a site gateway in every remote network that you add to the VPN (except the network in which the network hub is deployed). The site gateway is a virtual appliance that establishes a VPN tunnel with the network hub, which lets the VPN traffic to travel securely between remote sites. For more information, see Deploying Site Gateways.

4. **Add static routes for outgoing traffic on default gateways.**

   In every remote network that you add to the VPN, you must add a new route on the default gateway. The route must destine traffic outgoing from the network to the site gateway. For more information, see Adding Static Routes on Default Gateways.

Point-to-Site Scenario

1. **Deploy and configure the network hub**.

   You must deploy the network hub in Microsoft Azure, Amazon AWS or in an on-premises site. The network hub is the core of the VPN infrastructure. The network hub manages incoming and outgoing traffic and provides clients with access to resources in the VPN. For more information, see Deploying Network Hub.

2. **Register Veeam PN clients.**

   You must register clients in the network hub portal. In the point-to-site scenario, clients are standalone computers that must have access to the VPN. For more information, see Registering Clients.

3. **Configure standalone computers**.

   You must configure VPN settings on all standalone computers that must have access to the VPN. For more information, see Configuring Standalone Computers.

Deploying Network Hub

The first step of the VPN infrastructure configuration is to deploy the network hub. The network hub is the core component in the VPN infrastructure that provides VPN connections and services to remote sites and users. All traffic in the VPN is routed through the network hub.

Veeam PN supports two scenarios of the network hub deployment:

- **Microsoft Azure deployment**

  This scenario is recommended if you run some applications and services in Microsoft Azure and need to join an on-premises network with the Microsoft Azure network (site-to-site scenario), or provide users in remote networks with access to applications and services in Microsoft Azure (point-to-site scenario). In such situation, you must place the network hub in a Microsoft Azure network. After that, you must deploy site gateways in on-premises networks (site-to-site scenario) or configure OpenVPN on remote user computers (point-to-site scenario).

  Setup of the VPN infrastructure with the network hub residing in Microsoft Azure is easier. You do not have to manually configure routing on remote sites — routes between remote sites are automatically added to the user-defined routing table in the Microsoft Azure network. However, since the VPN traffic is routed through the Microsoft Azure, such deployment scenario may involve additional expenses.

- **Amazon AWS deployment**

  This scenario is recommended if you run some applications and services in Amazon AWS and need to join an on-premises network with the Amazon AWS network (site-to-site scenario), or provide users in remote networks with access to applications and services in Amazon AWS (point-to-site scenario). In such situation, you must place the network hub in an Amazon AWS network. After that, you must deploy site gateways in on-premises networks (site-to-site scenario) or configure OpenVPN on remote user computers (point-to-site scenario).

  Setup of the VPN infrastructure with the network hub residing in Amazon AWS is easier. You do not have to manually configure routing on remote sites — routes between remote sites are automatically added to the user-defined routing table on the Amazon AWS network. However, since the VPN traffic is routed through Amazon AWS, such deployment scenario may involve additional expenses.

- **On-premises deployment**

  This scenario is recommended if you want to join several remote on-premises networks (site-to-site scenario) or provide remote users with access to resources in an on-premises network (point-to-site scenario). In such situation, you must place the network hub in an on-premises network. After that, you can deploy site gateways in other on-premises networks that you want to add to the VPN (site-to-site scenario) or configure OpenVPN on remote user computers (point-to-site scenario).

  Setup of the VPN infrastructure with the network hub residing in an on-premises network is more complicated than that for Microsoft Azure. You will need to manually configure routing between local sites. For more information, see Adding Static Routes on Default Gateways.

Deploying Network Hub in Microsoft Azure

If you want to place the network hub in Microsoft Azure, you must deploy the network hub from the Microsoft Azure Resource Manager template named *Veeam PN*. The template lets you deploy a 64-bit Linux virtual appliance on which Veeam PN components are set up. You can then configure the appliance as the network hub.

To deploy and set up the network hub, you must perform the following steps:

Step 1. Deploy Network Hub Appliance in Azure

Step 2. Configure Network Hub Settings

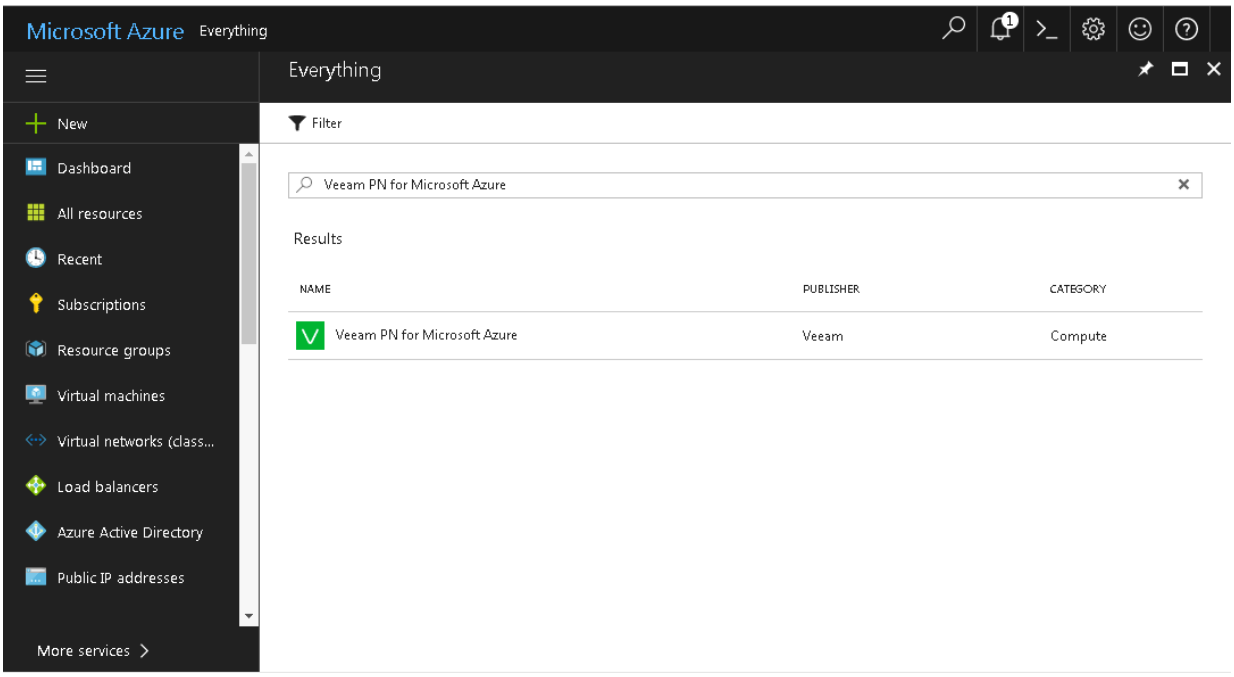
Step 3. Configure Clients

> **NOTE:**
>
> You can deploy the network hub using the Azure Resource Manager model only. You cannot use the Classic deployment model.

Step 1. Deploy Network Hub Appliance in Azure

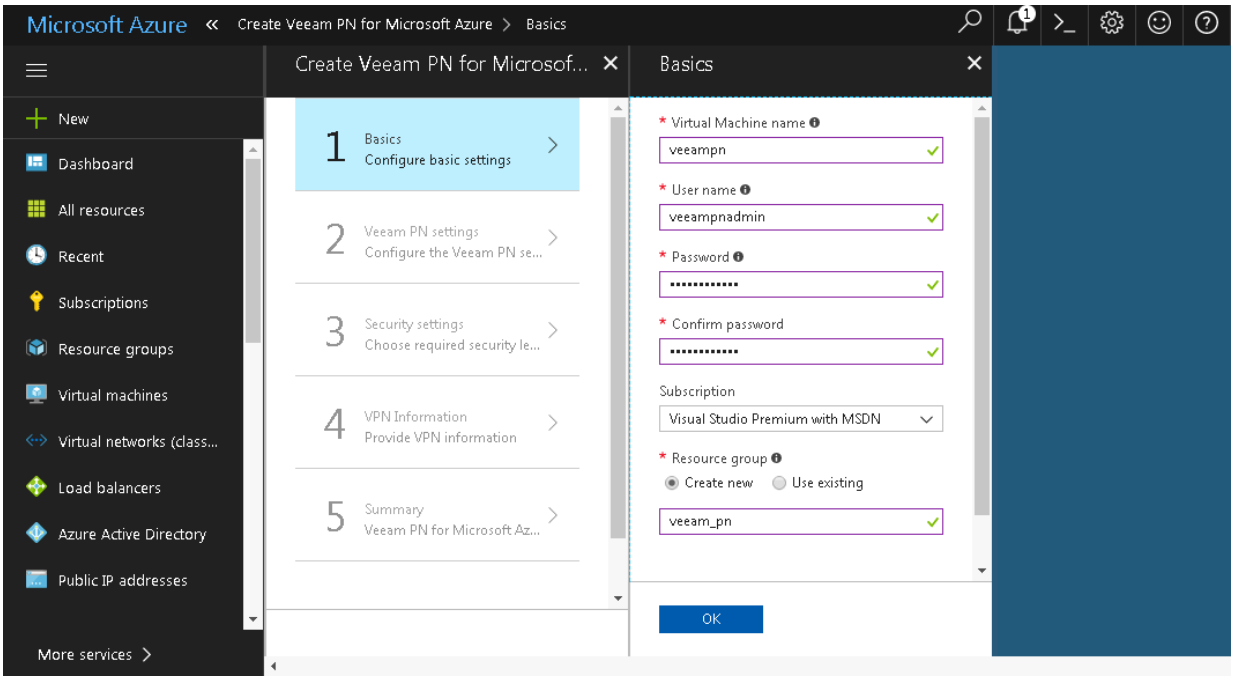
To deploy a network hub appliance from the Microsoft Azure template:

1. Sign in to the Microsoft Azure portal at https://portal.azure.com.
2. In the menu on the left, click **New**.
3. In the marketplace, search for the *'Veeam PN for Microsoft Azure'* template.
4. Select the template and click **Create**.



5. On the **Basics** blade, specify basic VM settings: VM name, user credentials for the network hub administrator account, subscription, resource group and location.

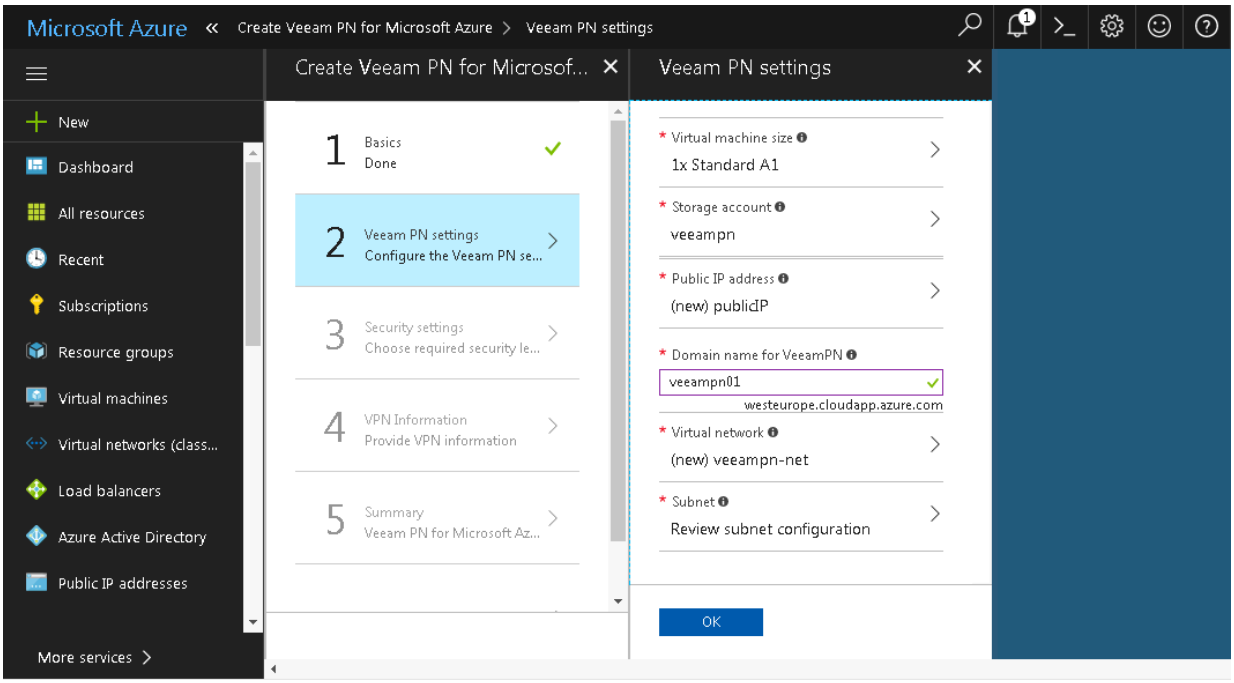
6. Click **OK**.



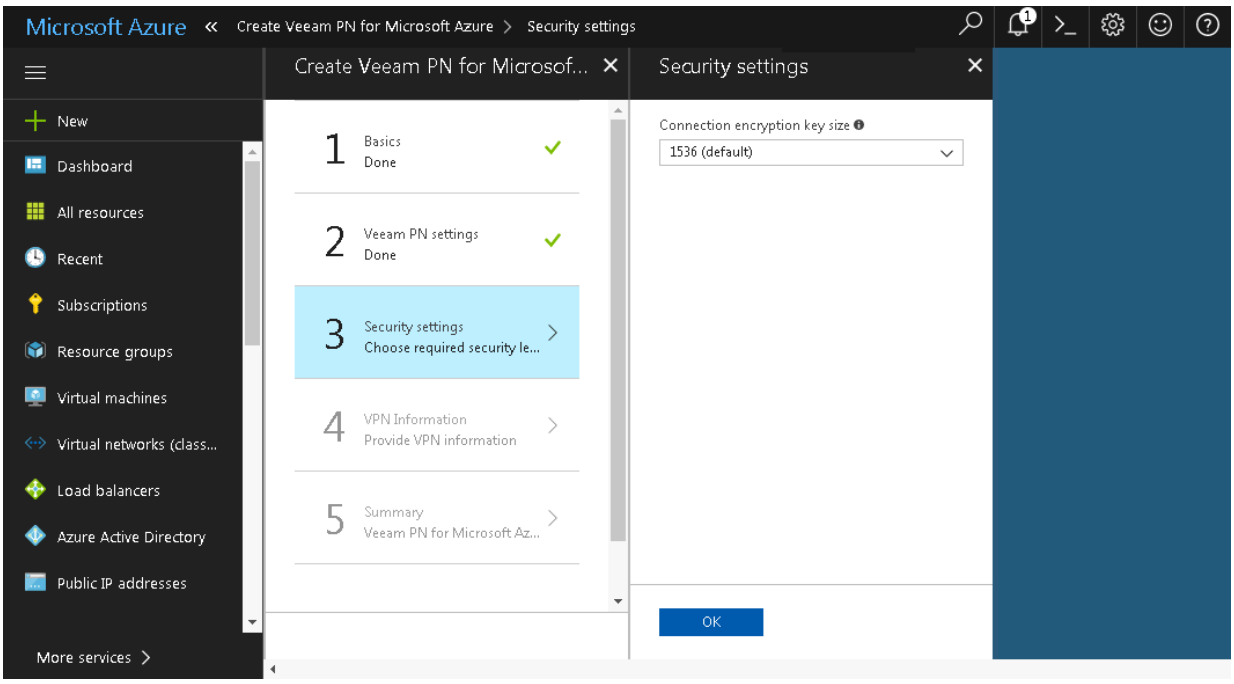
7. On the **Veeam PN Settings** blade, specify settings for the network hub:

   - In the **Virtual machine size** section, select the VM size. Make sure that the VM configuration meets minimal requirements to the network hub. For details, see System Requirements.
   - In the **Storage account** section, select a storage account whose resources you want to use to store disks of the network hub appliance.
   - In the **Public IP address** section, enter a public IP address for the network hub appliance. The network hub appliance will be accessible by this IP address.
   - In the **Domain name for VeeamPN** section, enter a domain name for the network hub appliance. The network hub appliance will be accessible by this domain name.
   - In the **Virtual network** section, specify to which Microsoft Azure network the network hub appliance must be connected.
   - In the **Subnet** section, specify a subnet to which the network hub appliance must be connected.

8. Click **OK**.



9. Veeam PN uses a self-signed SSL certificate to enable secure data communication in the VPN. On the **Security settings** blade, specify the certificate key length.



10. On the **VPN Information** blade, specify VPN settings for the network hub:

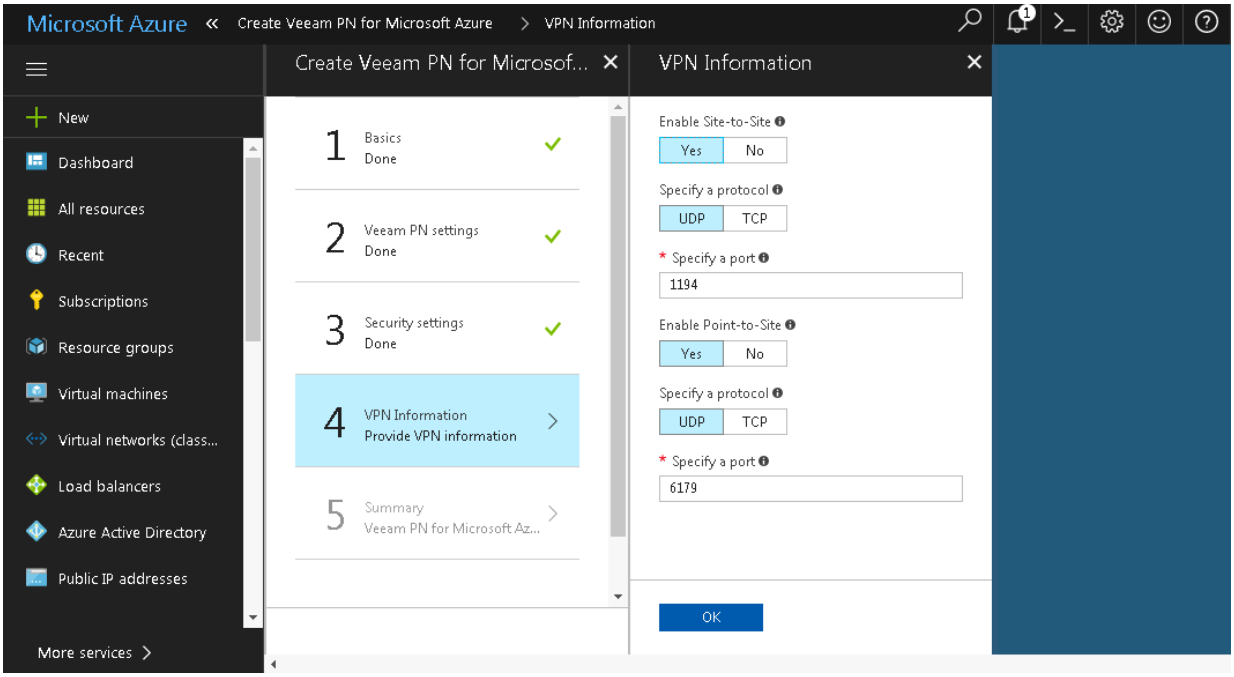
    - To implement the site-to-site scenario, in the **Enable Site-to-Site** field, click **Yes**. In the **Specify a protocol** field, specify a protocol that you want to use for communication between VPN components: UDP or TCP. In the **Specify a port** field, specify a port on which the network hub must listen for site gateway connections. By default, port 1194 is used.

    - To implement the point-to-site scenario, in the **Enable Point-to-Site** field, click **Yes**. In the **Specify a protocol** field, specify a protocol that you want to use for communication between VPN components: UDP or TCP. In the **Specify a port** field, specify a port on which the network hub must listen for standalone computer connections. By default, port 6179 is used.

11. Click **OK**.

NOTE:

It is recommended that you use the UDP protocol. While TCP guarantees delivery of data packets, UDP ensures faster data transmission since it does not require any data flow control.



12. On the **Summary** blade, review details of the network hub and click **OK**.

13. On the **Buy** blade, review the terms of use and privacy policy information and click **Purchase**.

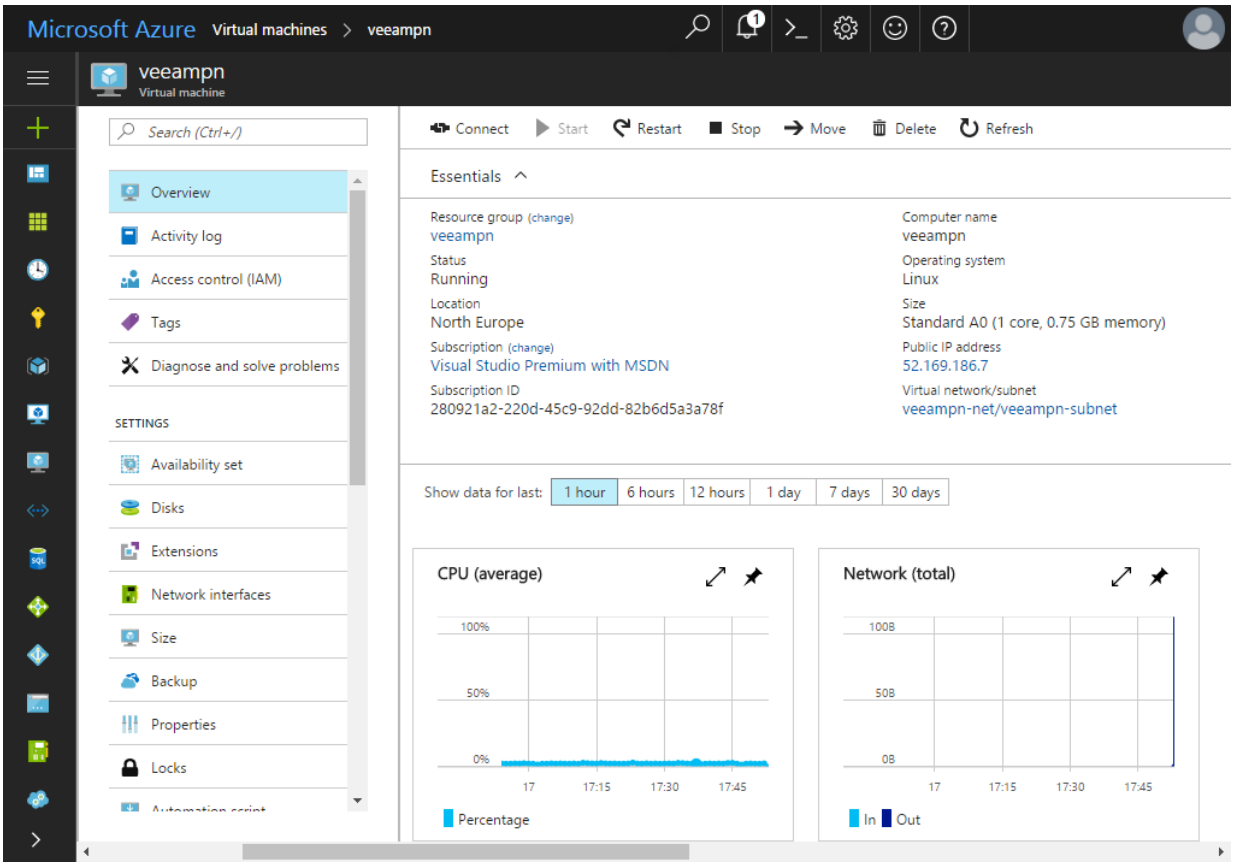
    Veeam PN will deploy the network hub from the Microsoft Azure template. The deployment process typically takes several minutes. Wait for this process to complete and proceed to the network hub configuration.

Step 2. Configure Network Hub Settings

After you deploy the network hub from the Microsoft Azure template, you must configure initial settings for the network hub.

To configure initial network hub settings:

1. In the Microsoft Azure portal, open properties of the newly deployed appliance and get an IP address of the appliance.

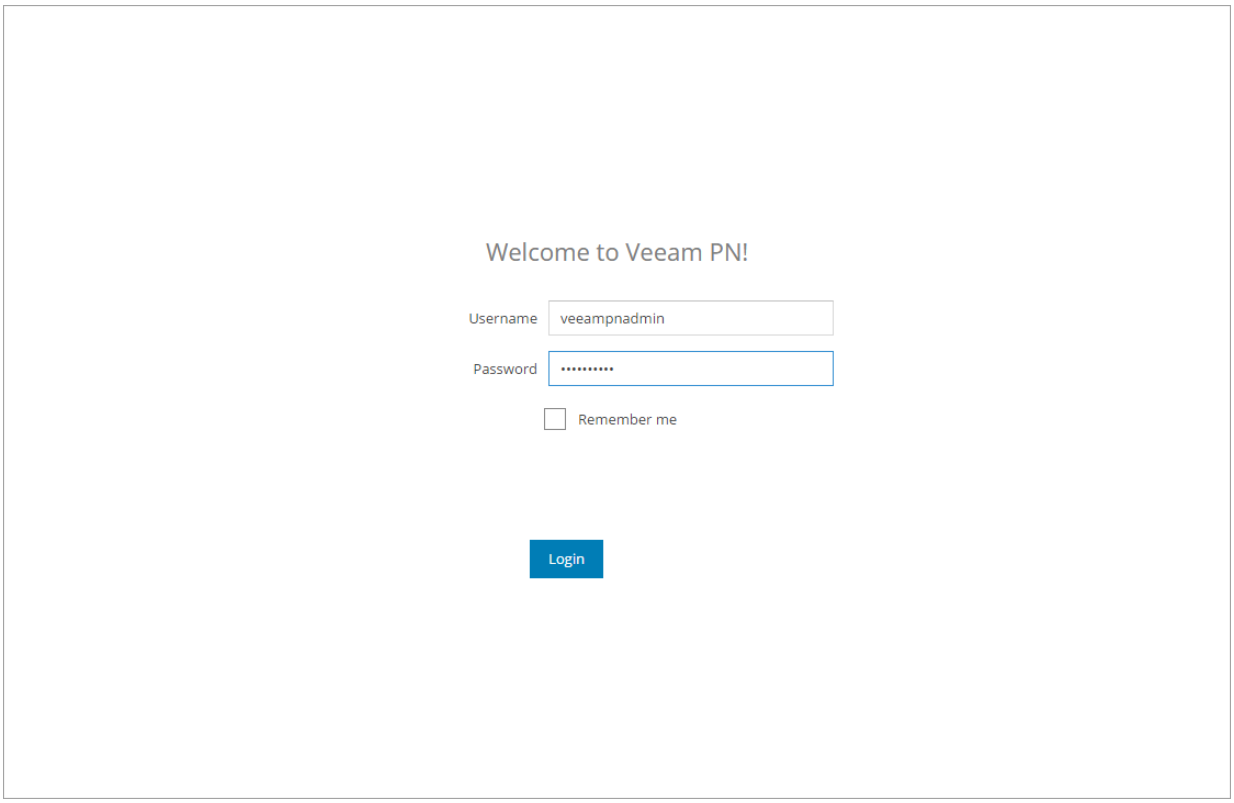


2. In a web browser, access the network hub portal by the following address: `https://<networkhubIP>`, where `<networkhubIP>` is the IP address of the network hub deployed in Microsoft Azure.

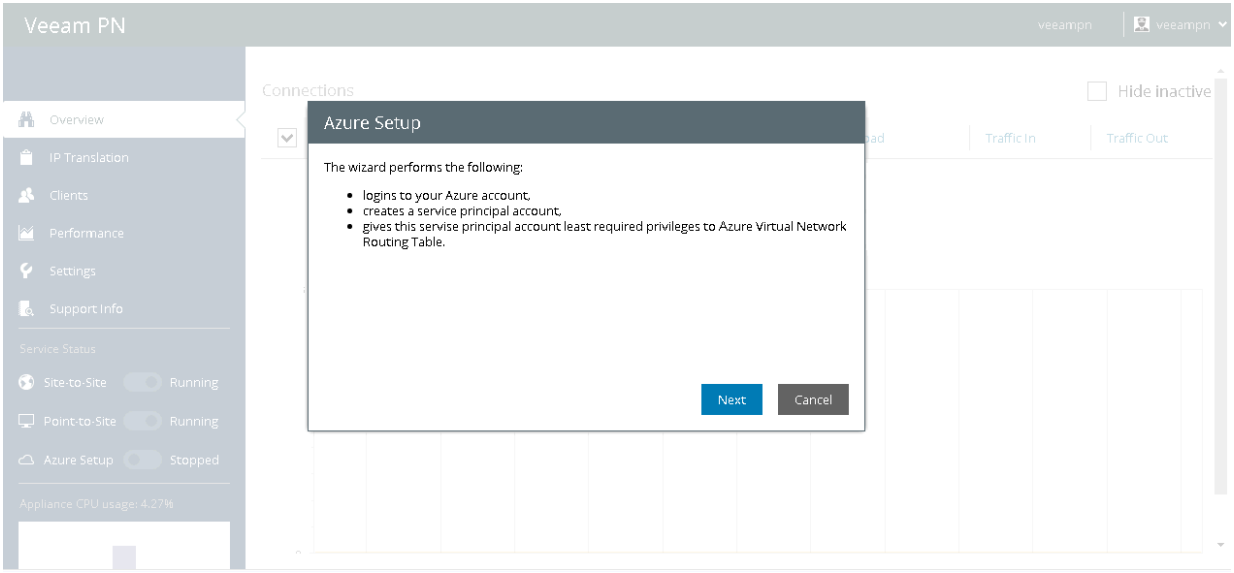
   When you access the network hub portal in the web browser, the browser will display a warning notifying that the connection is untrusted. Ignore the warning and agree to proceed to the portal.

3. At the **Welcome** screen of the portal, log in to the network hub portal under the network hub administrator account. You specified credentials for the network hub administrator account on the **Basic** blade when you deployed the network hub appliance from the Microsoft Azure template.

4. Click **Login**.



5. On the welcome screen of the **Azure Setup** wizard, click **Next**.



6. Veeam PN requires that you authenticate in Microsoft Azure Active Directory. The **Azure Setup** wizard will display the https://aka.ms/devicelogin link and an authentication code. Copy the code to the Clipboard, open the https://aka.ms/devicelogin link in a web browser and enter the code in the code field.

7. Click **Next**.

8. Veeam PN will proceed with configuring the network hub settings and assign the Network Contributor role on the routing table in the Microsoft Azure network to the network hub administrator account. Wait for the process to complete and click **Finish**.

> **TIP:**
>
> To pass through the **Azure Setup** wizard once again, in the Veeam PN portal open the **Settings** view, click the **Azure** tab and click **Apply** at the bottom of the page.

Step 3. Configure Clients

After you configure the network hub, do the following:

1. Log in to the network hub portal using the following address: `https://<networkhub>/`.
2. Configure settings for clients — on-premises networks (site-to-site scenario) and standalone computers (point-to-site scenario). For more information, see Configuring Clients.

If necessary, you can change the network hub settings: configure alerts, enable SSH access to the network hub appliance and so on. For more information, see Configuring Network Hub Settings.

Deploying Network Hub in Amazon AWS

If you want to place the network hub in Amazon AWS, you must deploy the network hub in AWS Marketplace.

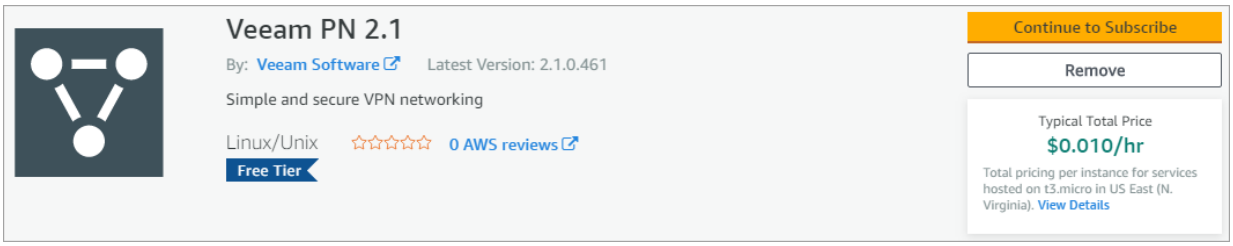
When you launch deploy of Veeam PN in AWS Marketplace, AWS CloudFormation deploys a 64-bit Linux virtual appliance on which Veeam PN components are set up.

To deploy and set up the network hub, perform the following steps:

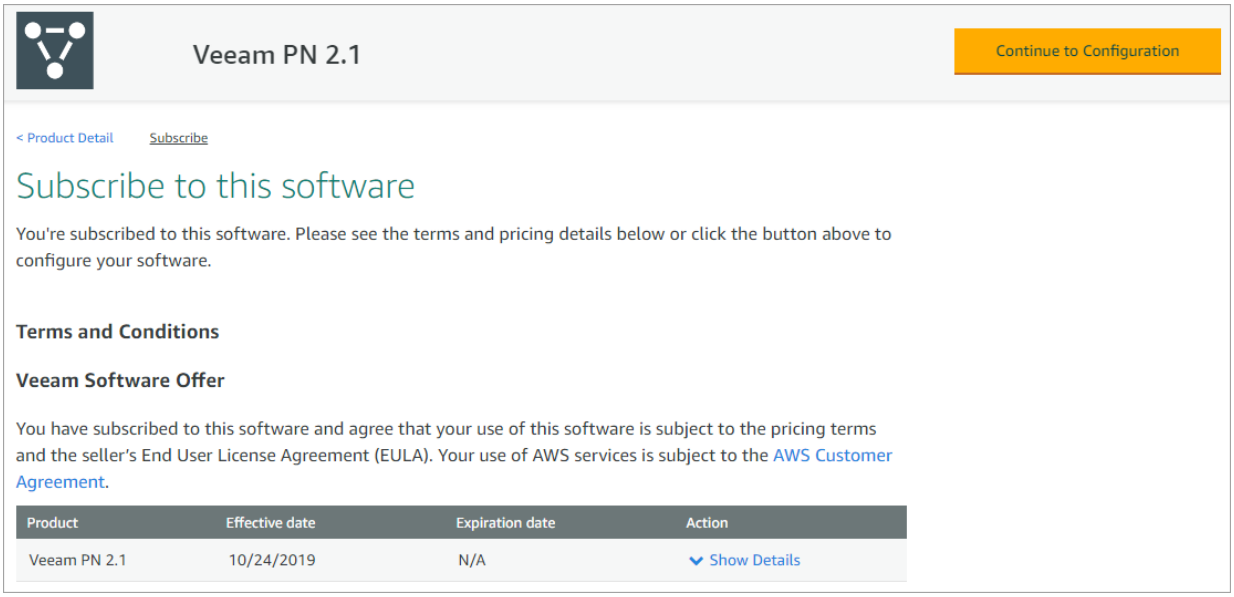
Step 1. Deploy Network Hub Appliance in Amazon AWS

To deploy a network hub appliance in Amazon AWS, do the following:

1. Open the Veeam PN 2.1 product page on the Amazon AWS marketplace: https://aws.amazon.com/marketplace/pp/B07ZDL12SM.
2. At the Veeam PN product page, click **Continue to Subscribe**.



3. At the subscription page, click **Show Details** and click **End User License Agreement** to read the Veeam End User License Agreement.
4. Read the AWS Customer Agreement and click **Continue to Configuration**.

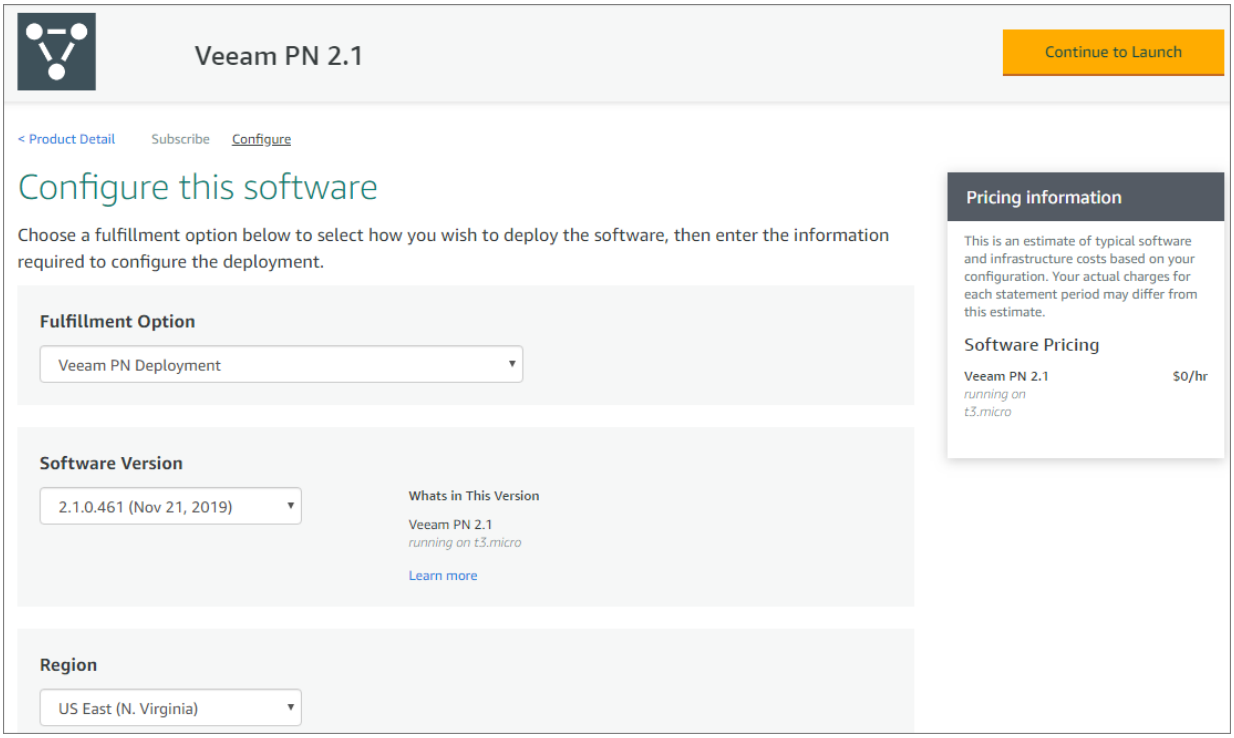


5. At the configuration page, select the deployment options:

   a. In the **Fulfillment Option** drop-down list, leave the default selection **Veeam PN Deployment**.

   b. In the **Software Version** drop-down list, select the latest version of Veeam PN.

   c. In the **Region** drop-down list, select an Amazon EC2 region where you want to place the stack resources. For details, see the Regions and Availability Zones section of the Amazon Elastic Compute Cloud User Guide.

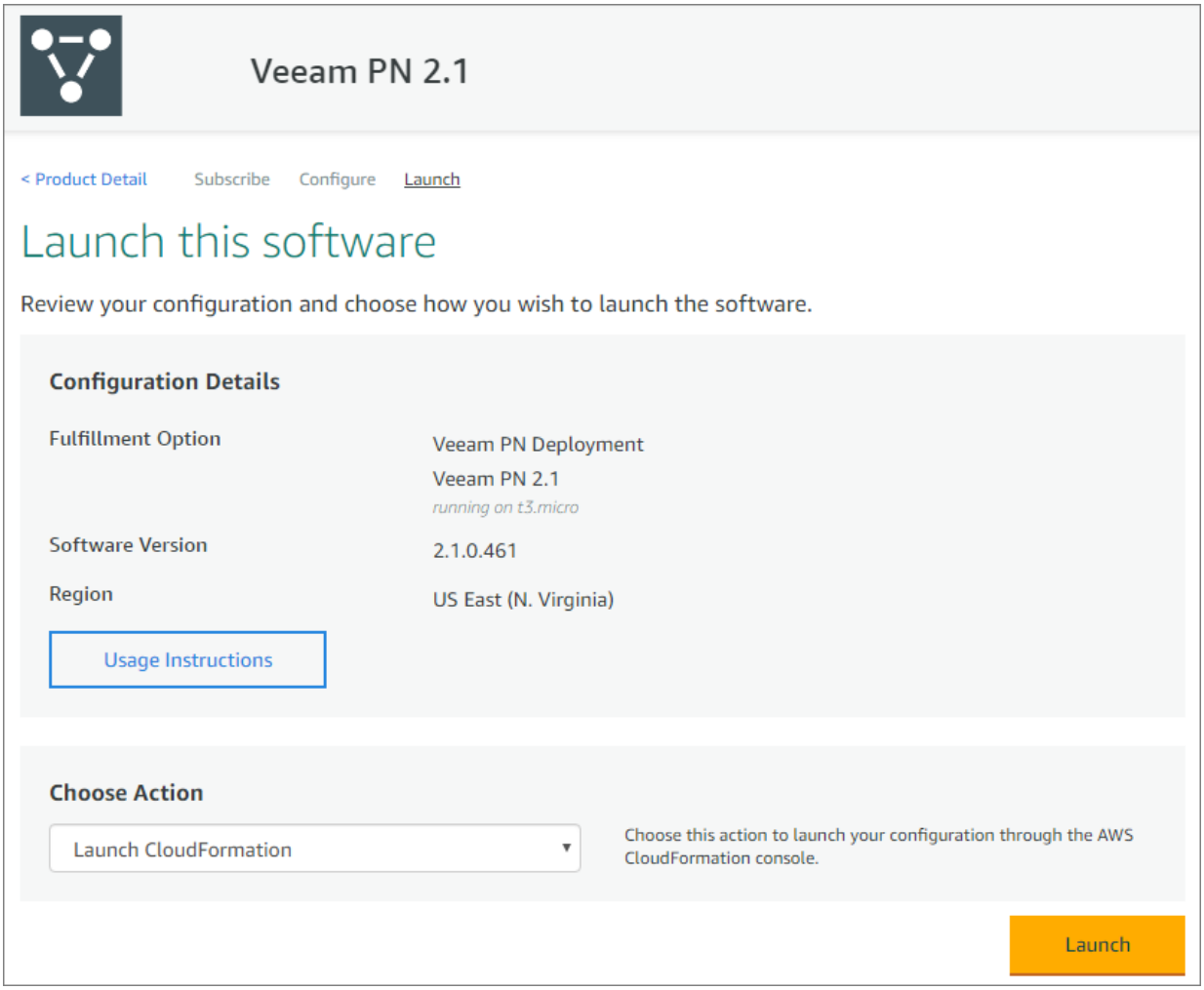


6. At the launching page, review the configuration:

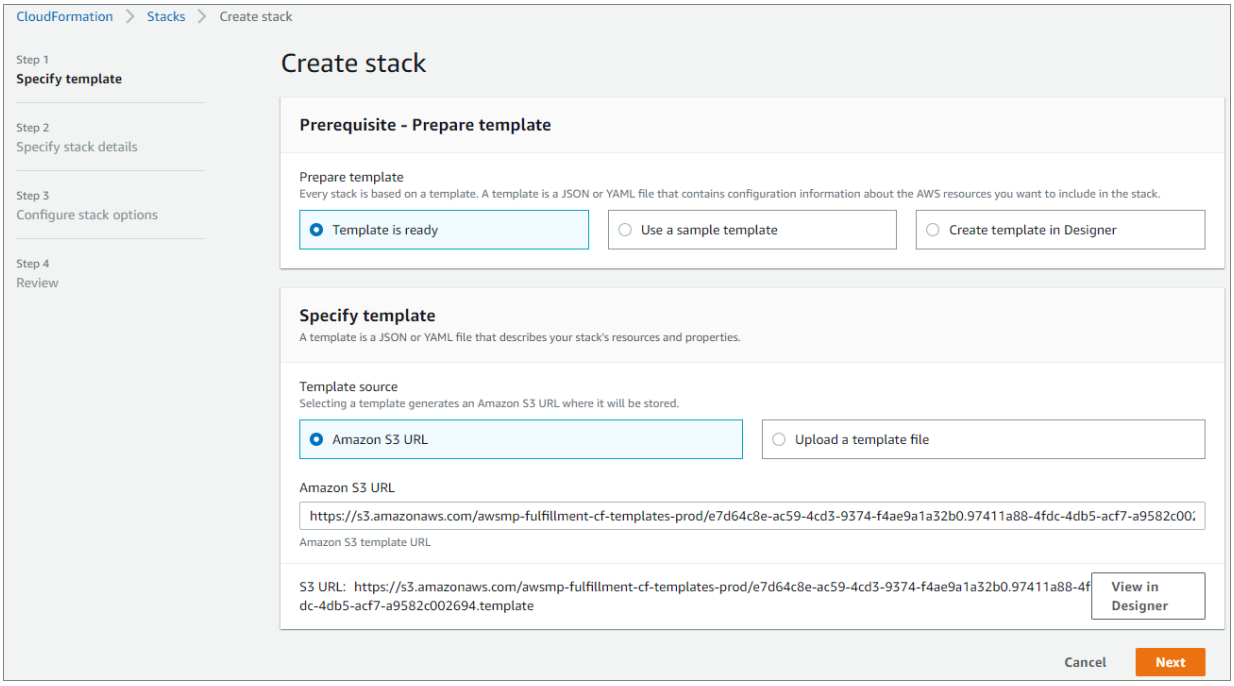
   a. Click **Usage Instructions** to see the list of resources which will be created by CloudFormation. Usage Instructions also include the list of parameters which you will need to specify before creating the resources.

   b. At the **Choose Action** field, leave the default selection: **Launch CloudFormation**.

   c. Click **Launch** to start the **Create Stack** wizard.



7. At the **Specify template** step of the wizard, you can specify the stack template settings. If you launch deployment of Veeam PN from AWS marketplace, the stack template settings are already configured. Thus, you can leave the default settings as shown below and click **Next**.



8. At the **Specify stack details** step, do the following:

   a. At the **Stack name** field, specify a name for the stack.

   b. Recommended instance type is *t3.micro*. You can leave the default selection.

   c. From the **Key Pair** list, select an existing EC2 key pair. For details on how to create EC2 key pairs, see the Amazon EC2 Key Pairs section of the Amazon Elastic Compute Cloud User Guide.

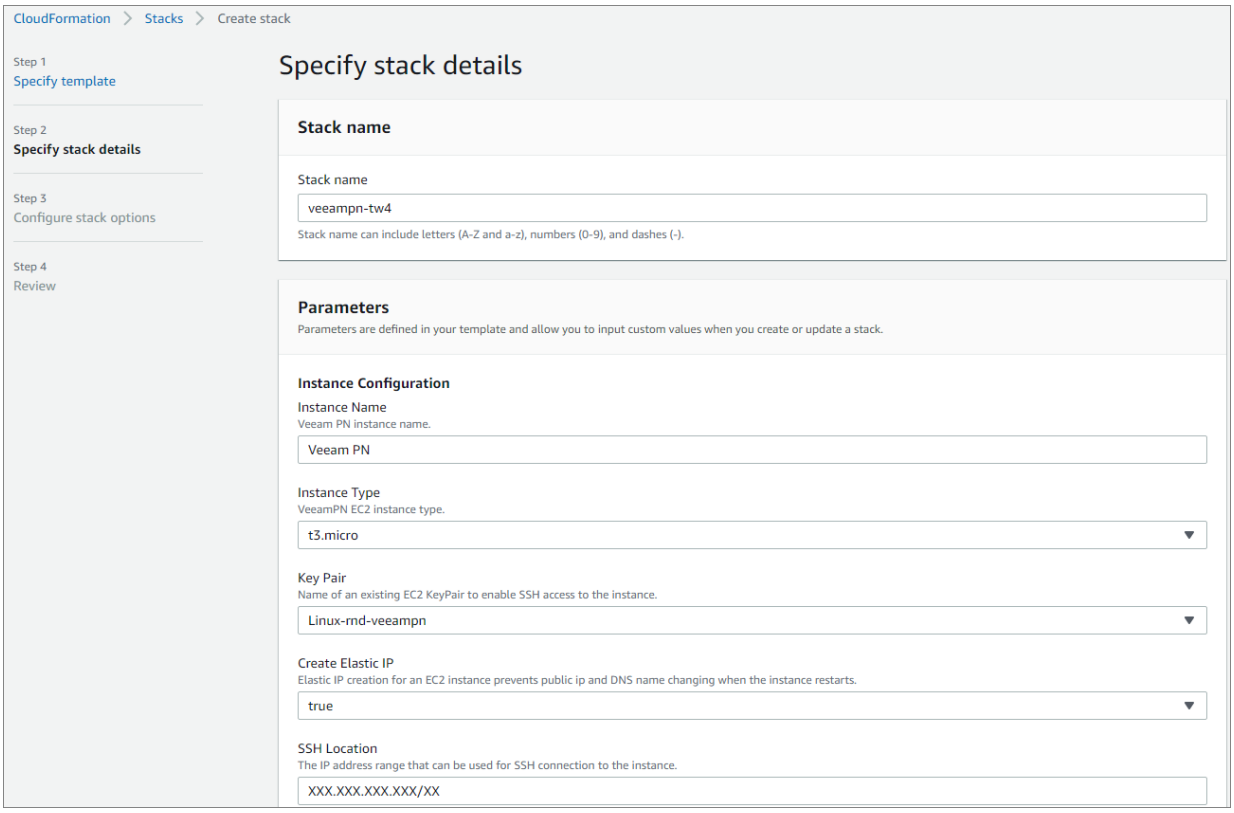
   d. At the **Create Elastic IP** setting, leave the default value to prevent changing of public IP and DNS name.

   e. At the **SSH Location** field, specify a range of IP addresses that you will use to connect via SSH to your EC2 instances.

      If you don't know the IP addresses which will be used to connect via SSH, you can enter *0.0.0.0/0* and add the addresses later in the setting of the EC2 security groups. For instructions on how to add security group rules, see the Security Groups section of the Amazon Virtual Private Cloud User Guide.

IMPORTANT!

In the **SSH Location** field, you can add only one IP range. If you want to add additional IP ranges after deploying the network hub, you can go to the EC2 security group settings and edit inbound rules for SSH connections. You can add multiple rules for all required IP addresses.

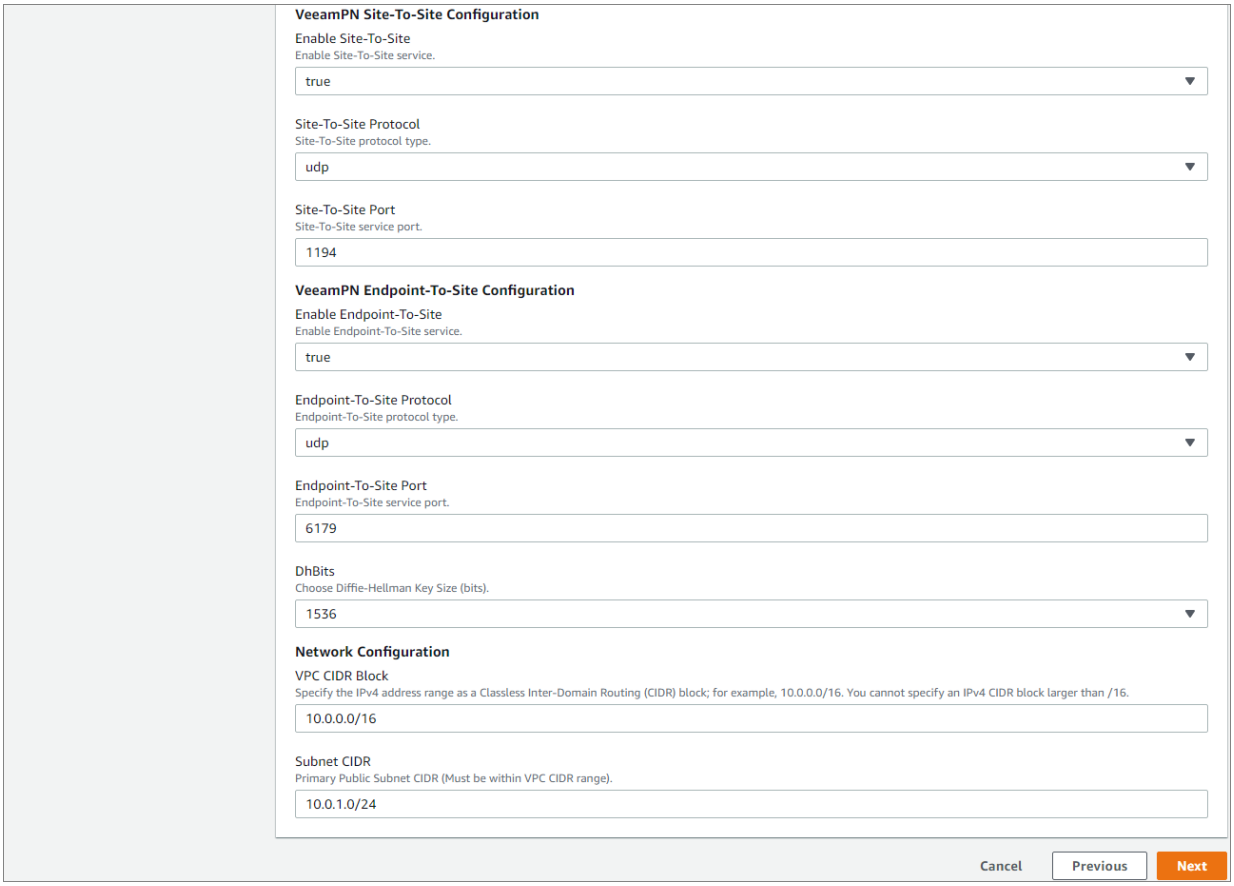


f. At the **VeeamPN Site-To-Site Configuration** and **VeeamPN Endpoint-To-Site Configuration** sections, you can leave the default settings for the ports, protocols and Deffie-Hellman Key Size which will be used when creating a VPN tunnel between sites and endpoints.

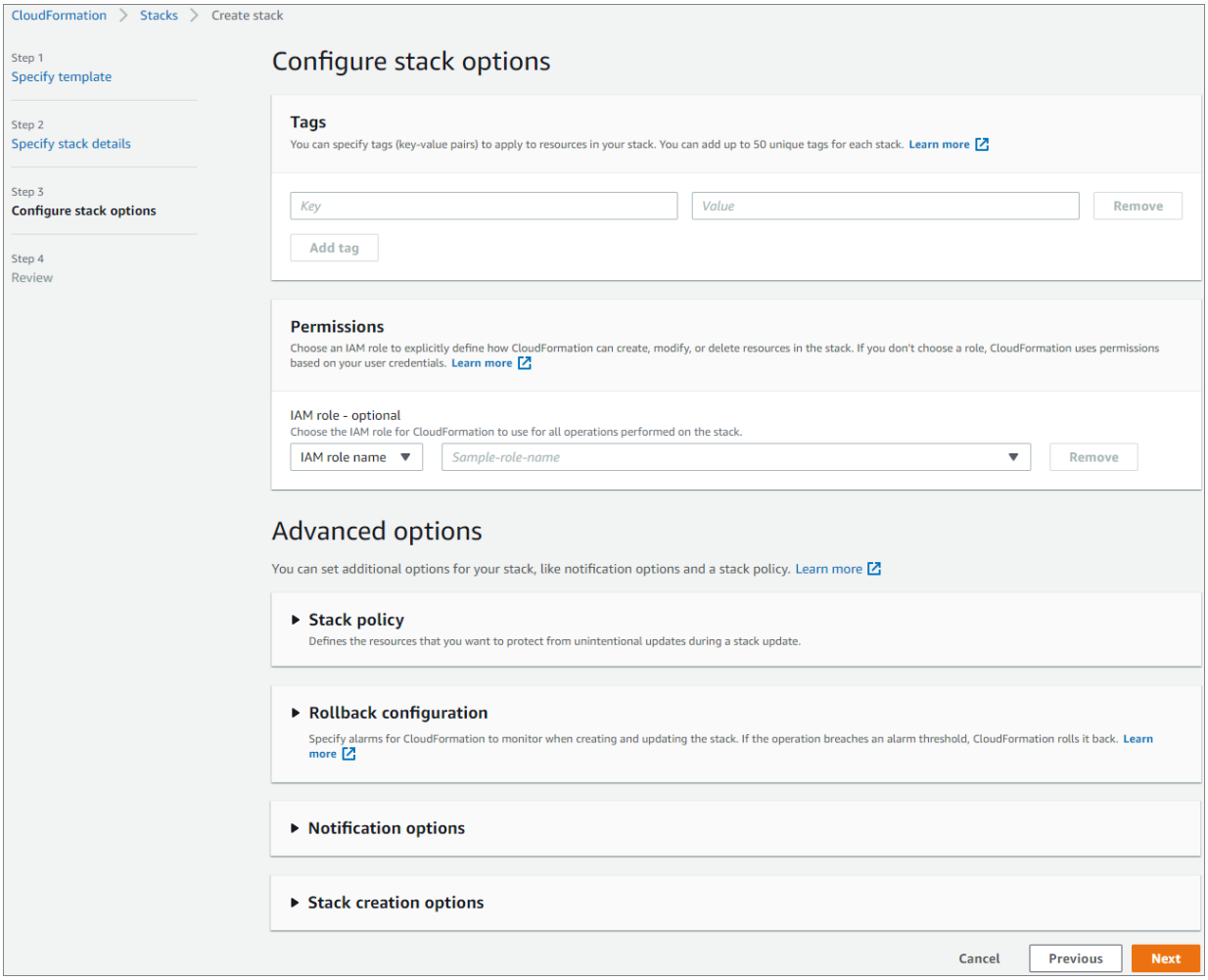
g. When you launch the stack deployment, AWS CloudFormation will create a virtual private cloud (VPC). VPC is a virtual network dedicated to your AWS account. You can leave the default settings or specify the required IP range as a CIDR block.

   For details on CIDR blocks of VPC, see the VPCs and Subnets section of the Amazon Virtual Private Cloud User Guide.

h. Click **Next**.

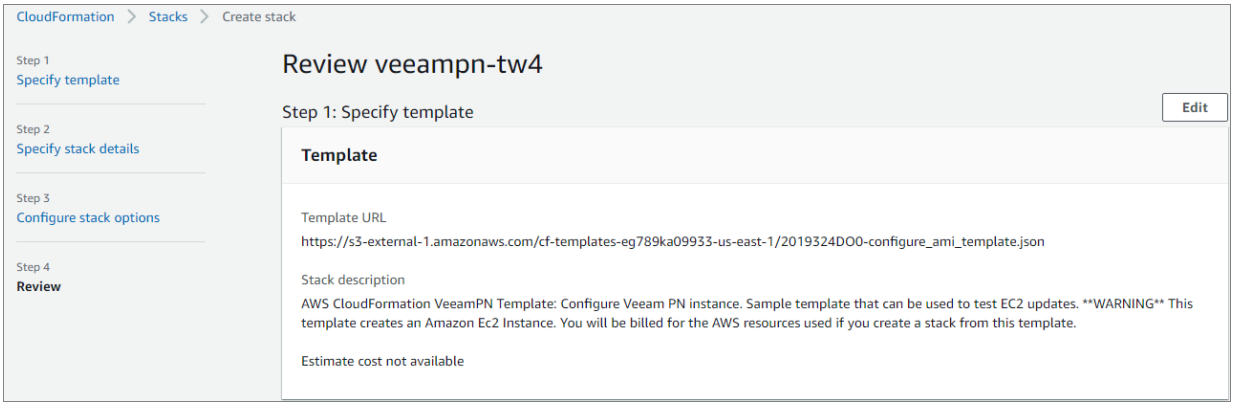


9. At the **Configure stack options** step of the wizard, specify required tags, IAM role permissions and other additional settings for the stack. For more information about stack options, see the Setting AWS CloudFormation Stack Options section of the AWS CloudFormation User Guide.



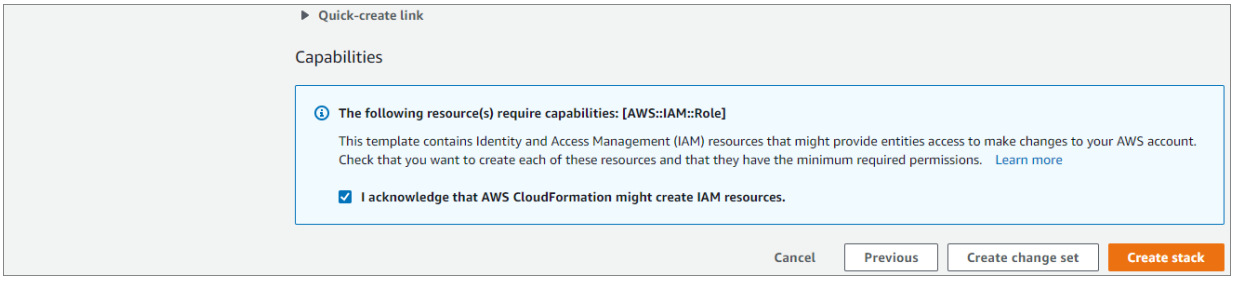
10. At the **Review** step of the wizard, you will see the configuration summary of the stack that will be created for Veeam PN.

    a. Review the Veeam PN stack settings.



    b. Check the **I acknowledge that AWS CloudFormation might create IAM resources** check box.

    c. Click **Create stack**.

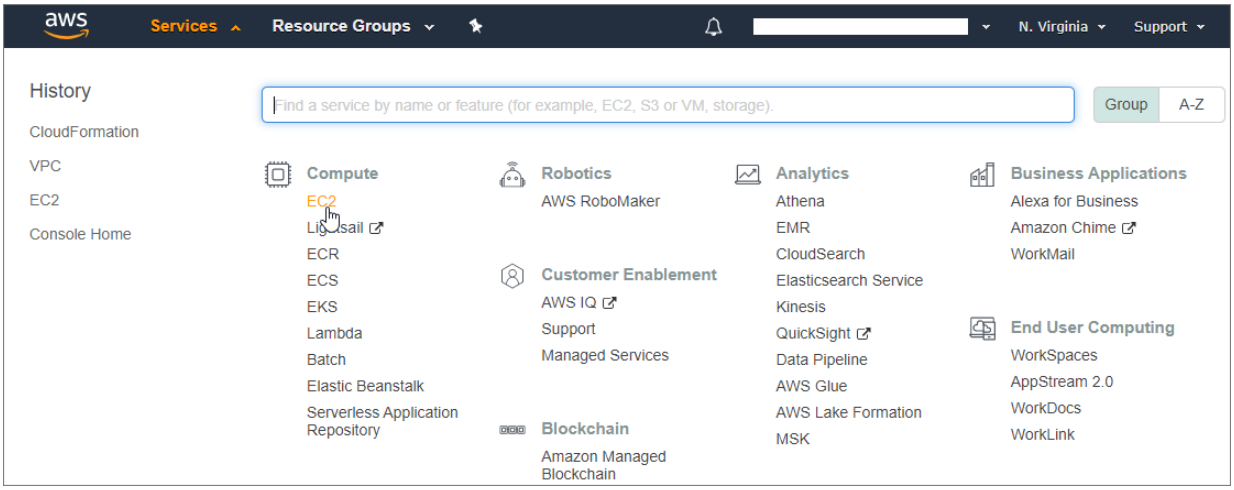


Step 2. Log in to Veeam PN Console

After you create an AWS CloudFormation stack for Veeam PN, you can log in to the Veeam PN web console and configure network hub settings.

To log in to the Veeam PN web console, do the following:

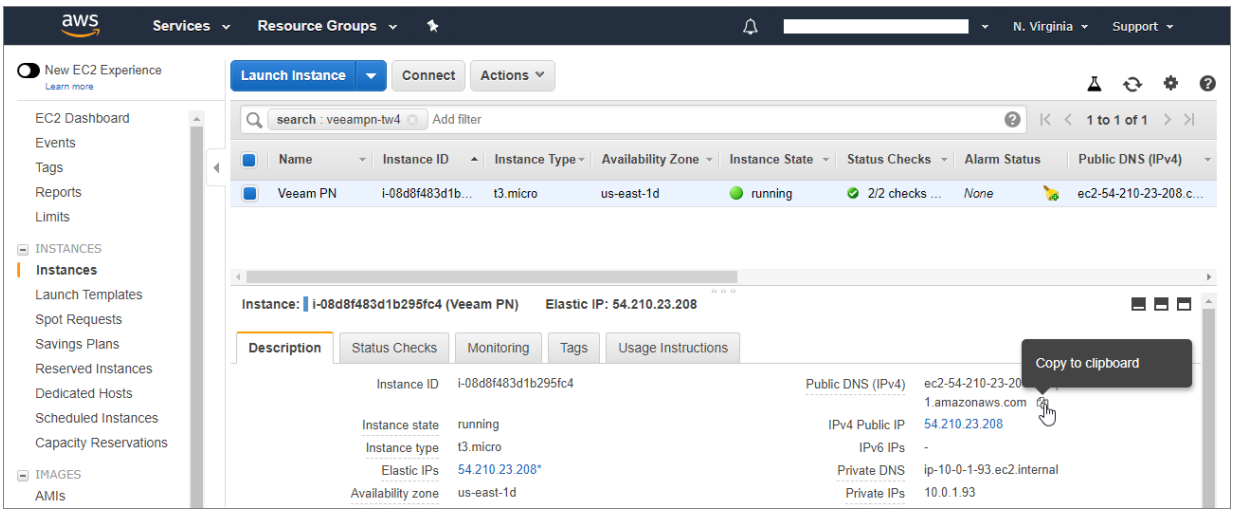
1. In the AWS console, click **Services** and select **EC2**.



2. From the list on the left of AWS console, select **Instances**.

3. From the list of instances, select the instance you have created on Step 3. Configure Network Hub Settings.

4. At the **Description** tab of the instance settings, copy the public DNS name of the instance.

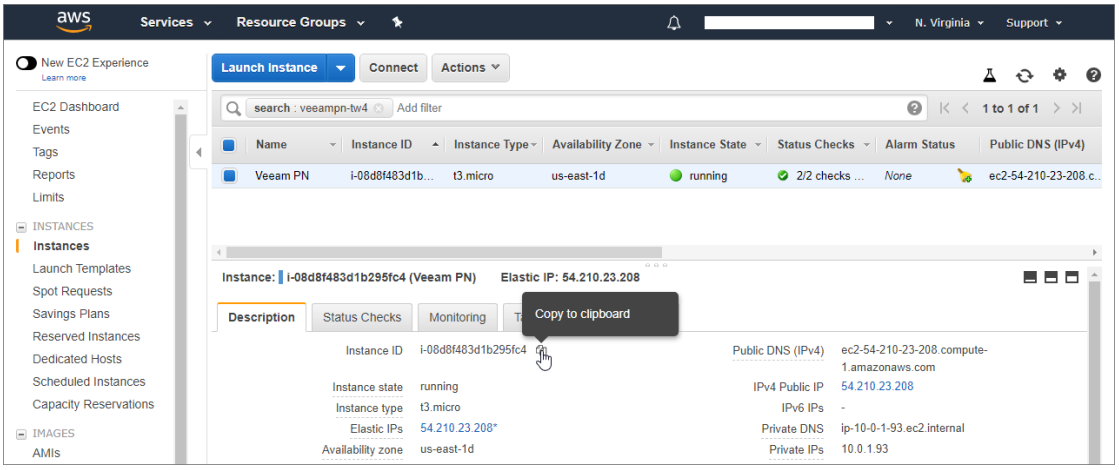


5. In a web browser, access the network hub portal by the following address: `https://publicDNS`, where `<publicDNS>` is the public DNS address of the stack deployed in Amazon AWS.

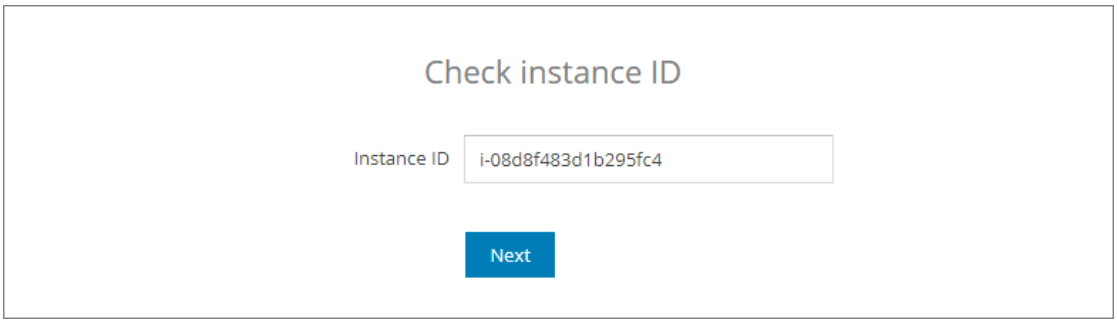
   When you access the network hub portal, the browser will display a warning notifying that the connection is untrusted. Ignore the warning and agree to proceed to the portal.

6. At the welcome screen of the network hub portal, you will be asked to provide an instance ID. Do the following:

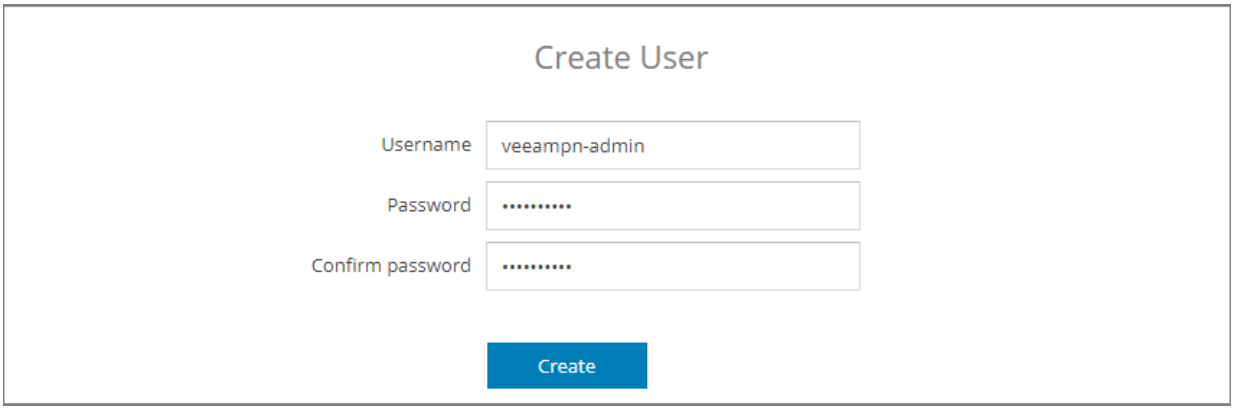
   a. Go back to AWS console and copy the instance ID of the created stack.



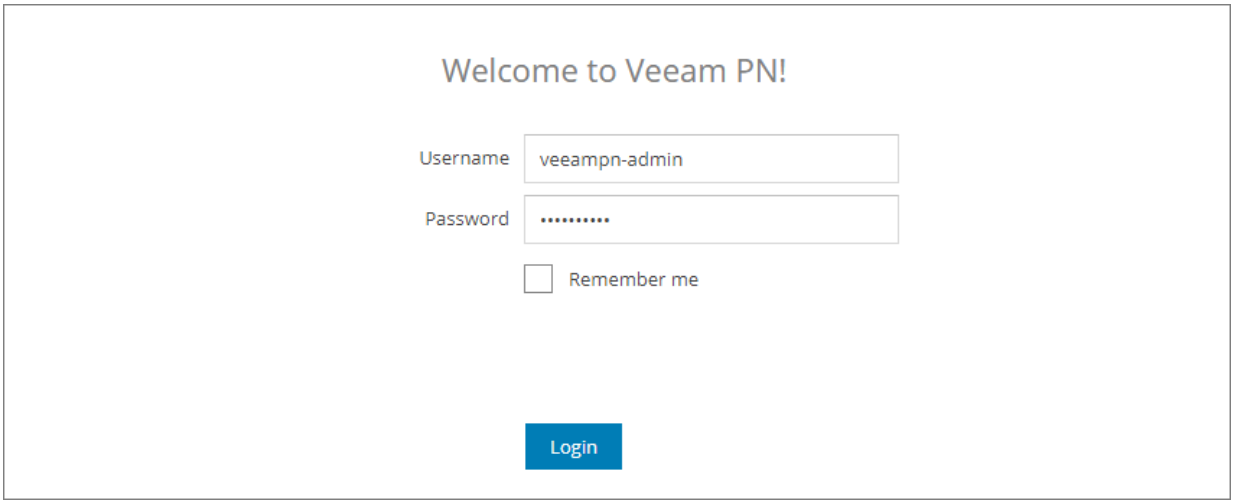
b. At the welcome screen of the network hub, paste the instance ID and click **Next**.



7. When you open the network hub for the first time, you need to crate a user account.
   a. Specify a name and a password for the network hub user account.
   b. Click **Create**.



8. Enter the username and password for the account created at the previous step and click **Login**.



Step 3. Configure Clients

After you log in to the network hub console, you can configure settings for clients — on-premises networks (site-to-site scenario) and standalone computers (point-to-site scenario). For more information, see Configuring Clients.

If necessary, you can change the network hub settings: configure alerts, enable SSH access to the network hub appliance and so on. For more information, see Configuring Network Hub Settings.

Deploying Network Hub in On-Premises Network

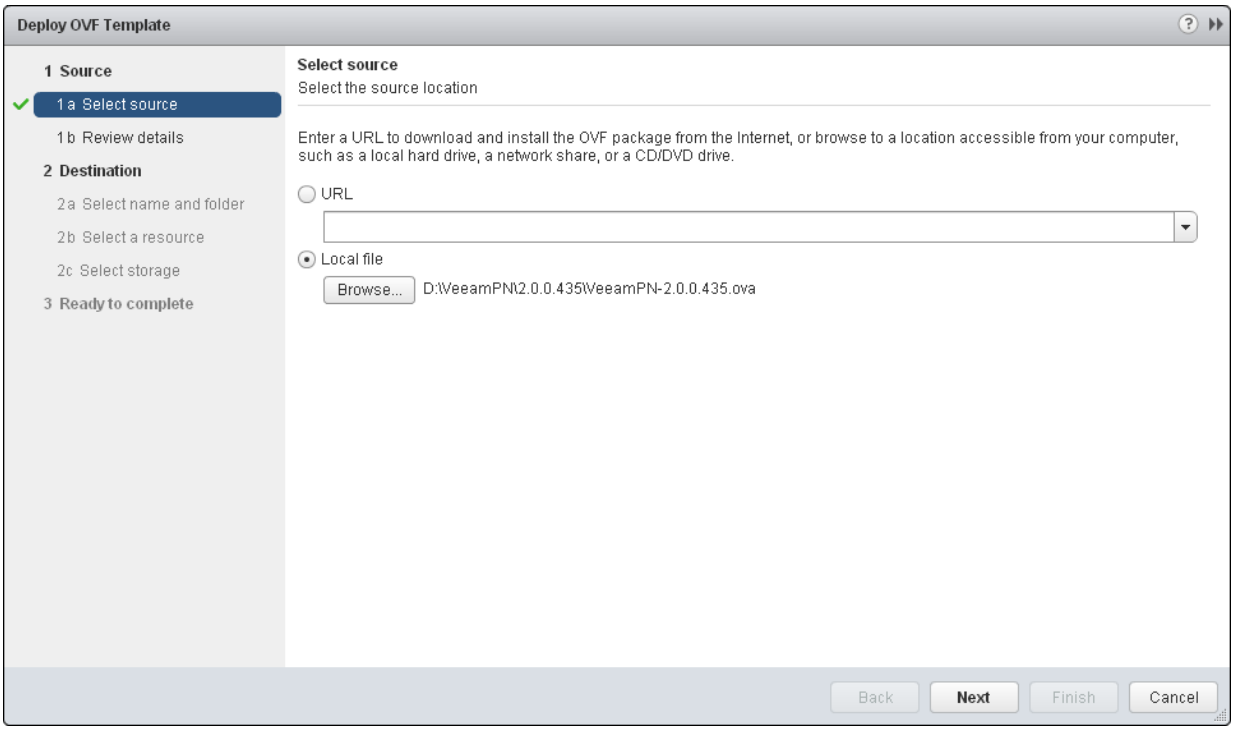
If you want to place the network hub in an on-premises network, you must deploy a Veeam PN appliance in the VMware vSphere environment. The Veeam PN appliance is distributed as an OVA package. The package contains a pre-configured 64-bit Linux virtual appliance on which Veeam PN components are set up.

To deploy and set up the network hub, you must perform the following steps:

Step 1. Deploy Hub Appliance

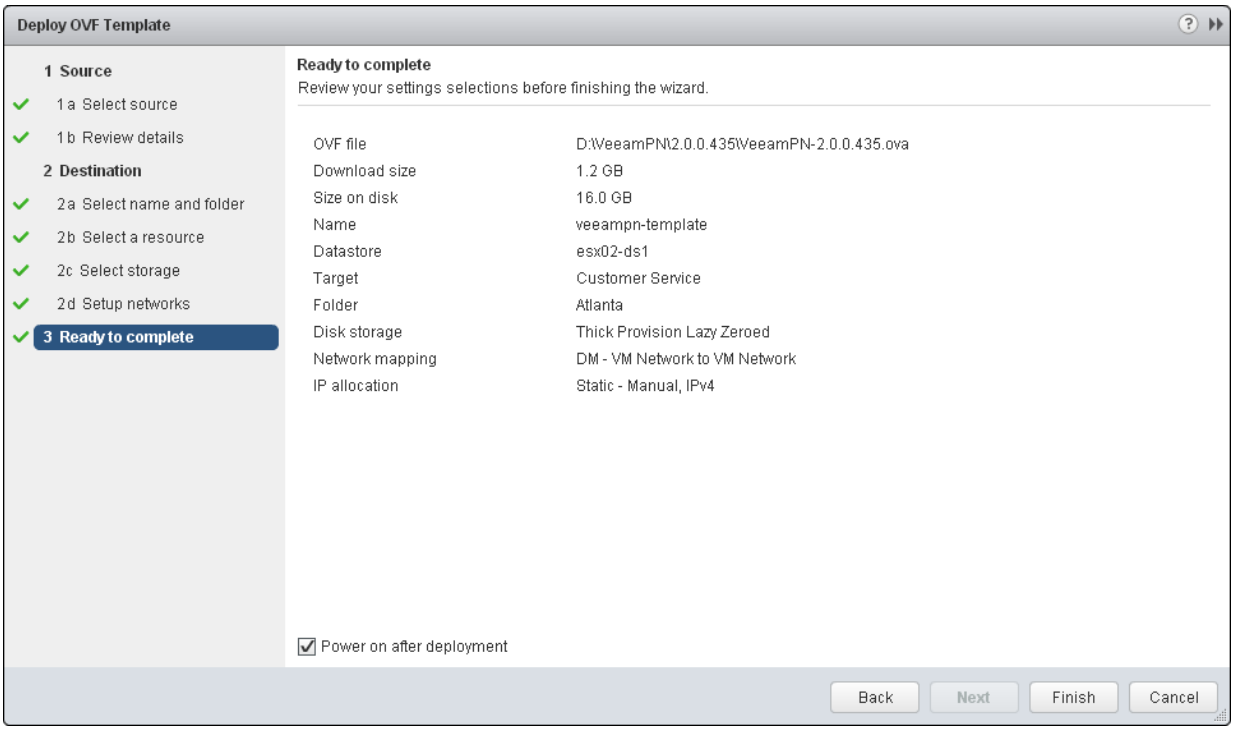
To deploy the network hub from the OVA package:

1. Download the Veeam PN OVA package from: https://www.veeam.com/downloads.html and save it in a network shared folder.
2. In VMware vSphere Web Client, open the hosts and clusters inventory list and select a host on which you want to register the appliance.
3. From the menu at the top of the working area, select **Actions** > **Deploy OVF Template**.
4. At the **Select source** step of the wizard, select **Local file**, click **Browse** and browse to the Veeam PN OVA package.



5. Follow the next steps of the wizard and specify appliance deployment settings: datastore on which the appliance disk must be placed, disk format, network to which the appliance must be connected and so on.

6. At the last step of the wizard, select the **Power on after deployment** check box and click **Finish**.



VMware vSphere will deploy the Veeam PN appliance on the selected host. The deployment process typically takes several minutes. Wait for this process to complete and proceed to the network hub configuration.

Step 2. Configure Network Hub

Right after deployment, the Veeam PN virtual appliance is impersonalized. To set up the network hub, you must customize the appliance — configure the network hub settings on it.

To configure initial settings for the network hub:

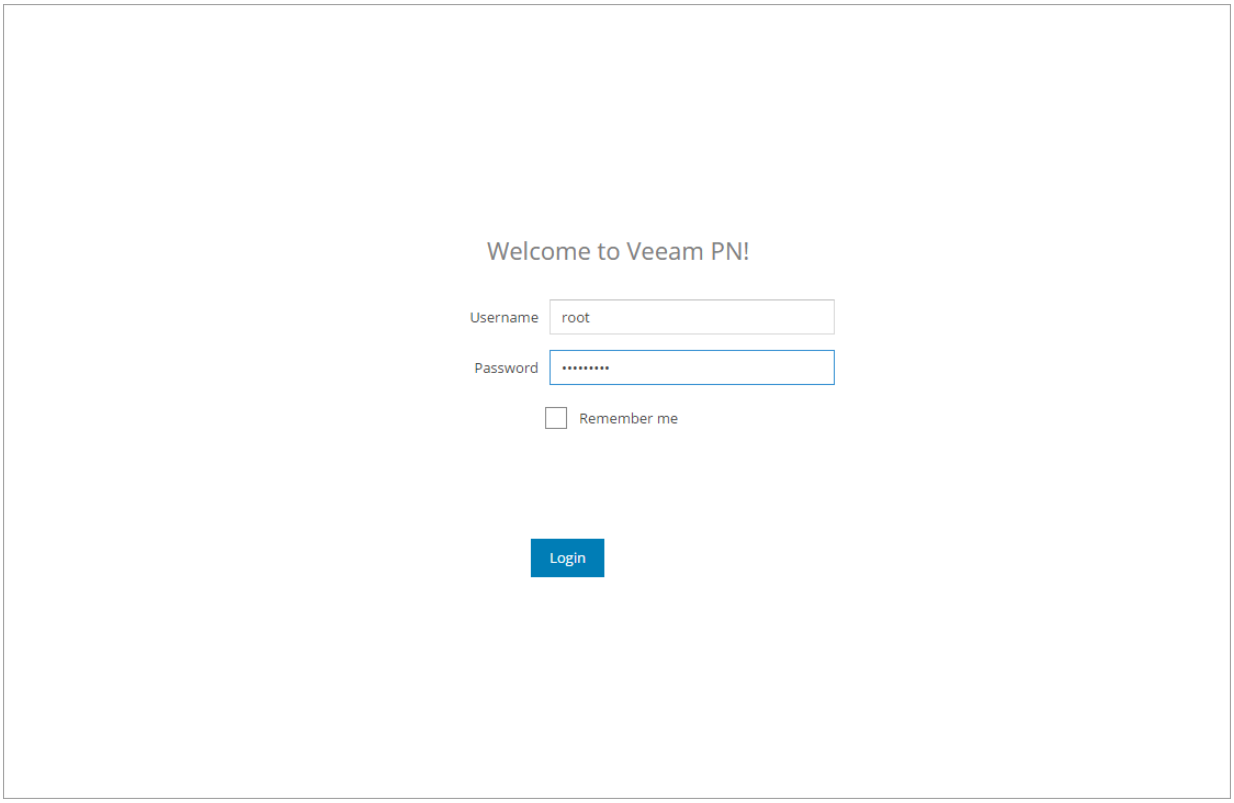
1. In VMware vSphere Web Client, navigate to the **Summary** tab and get an IP address of the appliance.
2. In a web browser, access the network hub portal by the following address: `https://<applianceIP>`, where `<applianceIP>` is the IP address of the deployed appliance.

   When you access the network hub portal in the web browser, the browser will display a warning notifying that the connection is untrusted. Ignore the warning and agree to proceed to the portal.

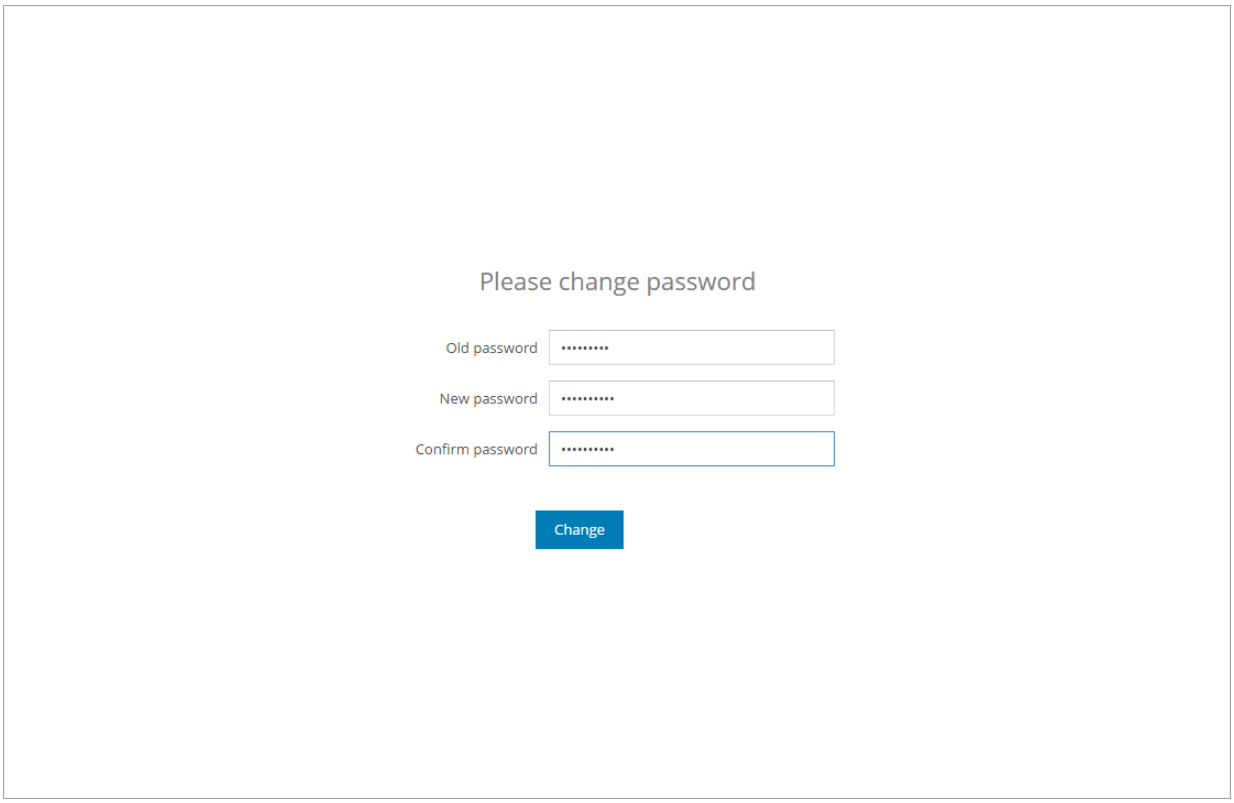
3. At the **Welcome to Veeam PN** screen of the portal, log in to the network hub portal under the in-built Administrator account. The Administrator account has the following credentials:

   - Username: *root*
   - Password: *VeeamPN*

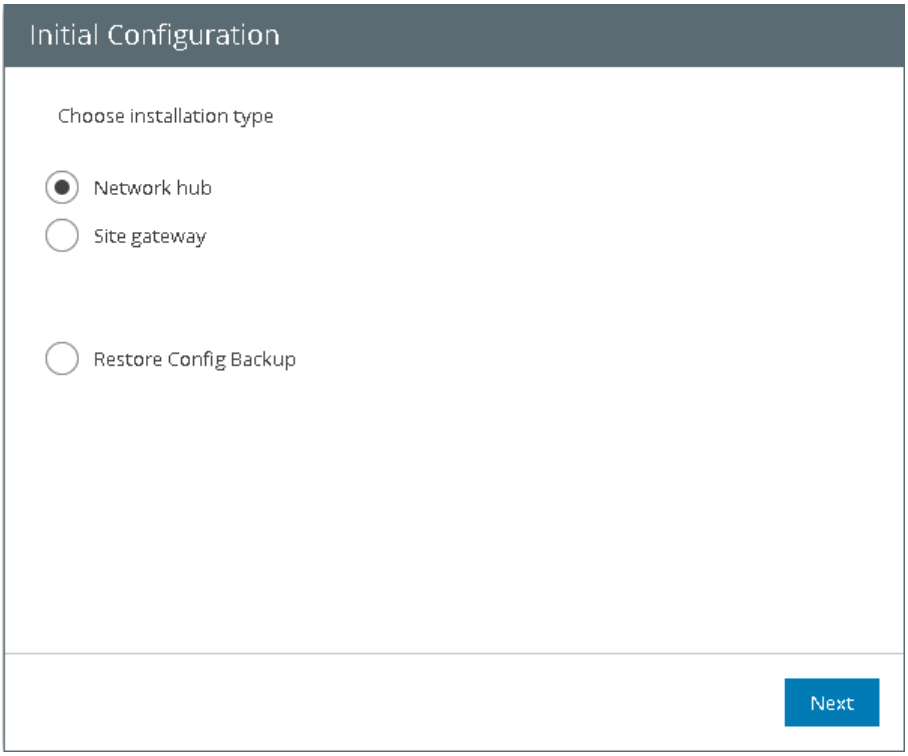
   Click **Login**.



4. After you log in to the portal for the first time, Veeam PN will offer you to change the password for the built-in account. On the displayed screen, enter the old and new password and click **Change**.



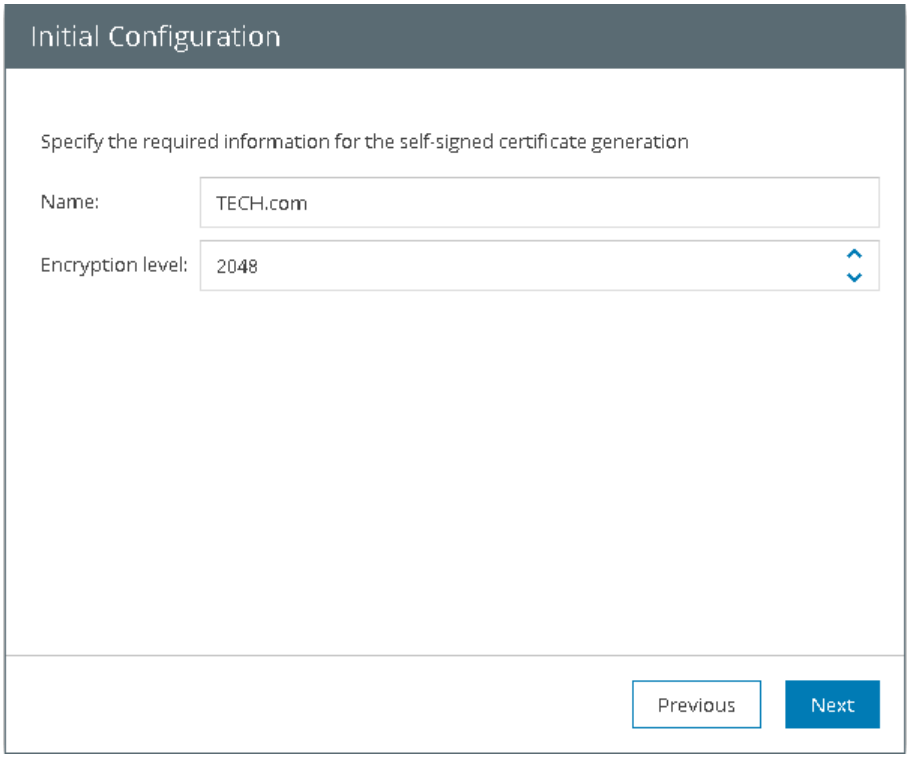
5. At the first step of the **Initial Configuration** wizard, select **Network hub**.
6. Click **Next**.



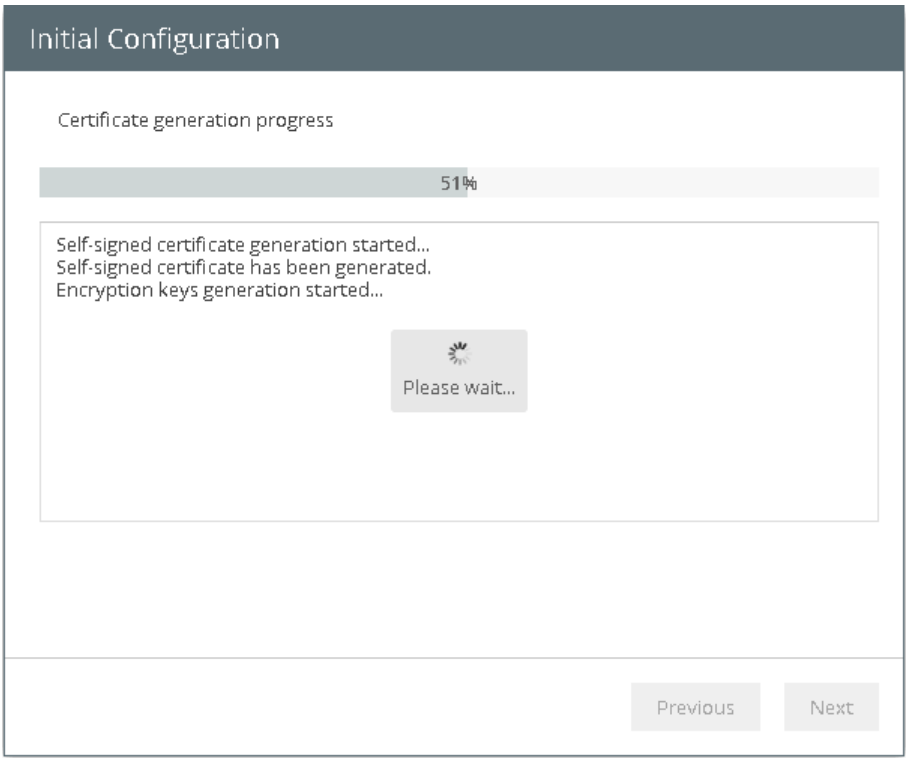
7. Veeam PN uses a self-signed SSL certificate to ensure secure data communication in the VPN. Specify the certificate key length.
8. Click **Next**.

NOTE:

By default, Veeam PN generates a 2048-bit certificate. If you select a key of a greater size, the process of certificate generation may take a long time.



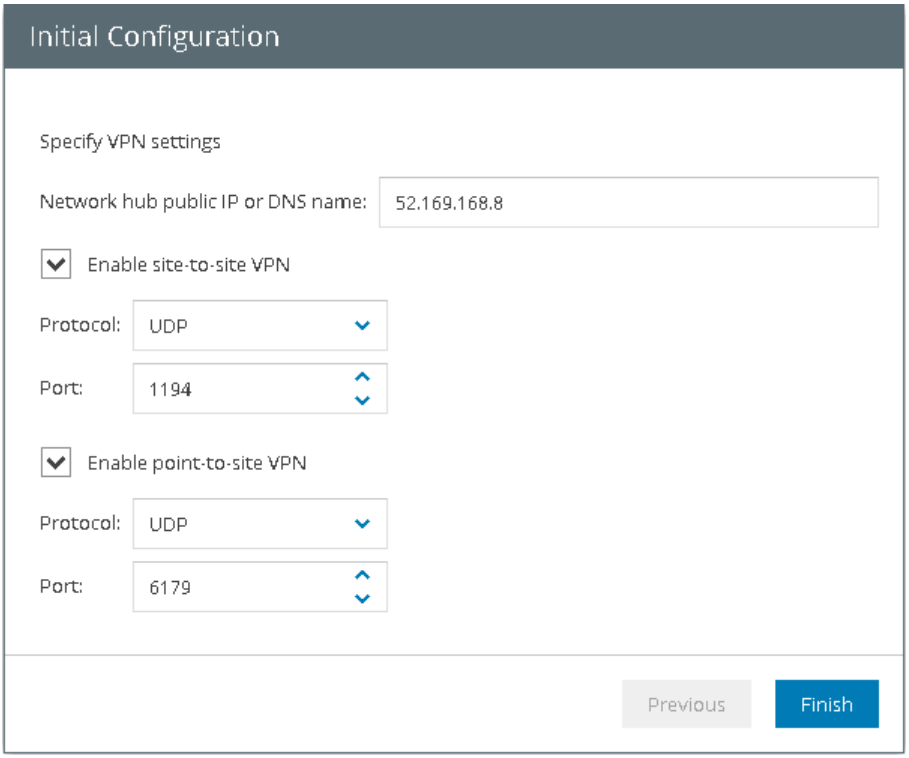
9. Veeam PN will generate a self-signed SSL certificate with the specified parameters. After the certificate is generated, click **OK**, then click **Next** to proceed to the network hub setup.



10. Specify VPN settings for the network hub:
    - In the **Network hub public IP or DNS name** field, specify an IP address or full DNS name for the network hub. The IP address or DNS name must be public and accessible from all networks that you add to the VPN, and by all remote users who must have access to the VPN.
    - Select the **Enable site-to-site VPN** check box if you want to implement the site-to-site VPN scenario. In the **Protocol** field, specify the protocol that must be used for communication between VPN components: UDP or TCP. In the **Port** field, specify a port on which the network hub must listen for site gateway connections. By default, port 1194 is used.
    - Select the **Enable point-to-site VPN** check box if you want to implement the point-to-site VPN scenario. In the **Protocol** field, specify the protocol that must be used for communication between VPN components: UDP or TCP. In the **Port** field, specify a port on which the network hub must listen for standalone computer connections. By default, port 6179 is used.

NOTE:

It is recommended that you use the UDP protocol. While TCP guarantees delivery of data packets, UDP ensures faster data transmission since it does not require any data flow control.



11. Click **Finish**.

Step 3. Configure Clients

After you configure the network hub, you must perform the following steps:

- You must log in to the network hub portal and configure settings for clients — on-premises networks (site-to-site scenario) and standalone computers (point-to-site scenario). For more information, see Configuring Clients.
- If necessary, you can change the network hub settings, for example, configure alerts, enable SSH access to the network hub appliance and so on. For more information, see Configuring Network Hub Settings.

Configuring Network Hub Settings

You can configure the following settings for the network hub:

- Enable and disable Veeam PN services
- Configure VPN settings
- Enable and disable DNS
- Configure Microsoft Azure settings
- Configure Amazon AWS settings
- Enable and disable SSH access
- Reset network hub settings
- Set the network hub reboot time

Enabling and Disabling Veeam PN Services

Veeam PN provides the following services:

- Site-to-Site — this service enables site-to-site communication between remote networks.
- Point-to-Site — this service enables remote users to access the VPN.
- Azure Setup — this service enables the network hub to run in Microsoft Azure and provide on-premises networks and remote users with access to resources and services in Microsoft Azure.
- AWS Setup — this service enables the network hub to run in Amazon AWS and provide on-premises networks and remote users with access to resources and services in Amazon AWS.

If you do not plan to use some services, for example, do not want to provide standalone computers with access to the VPN, you can disable this service.

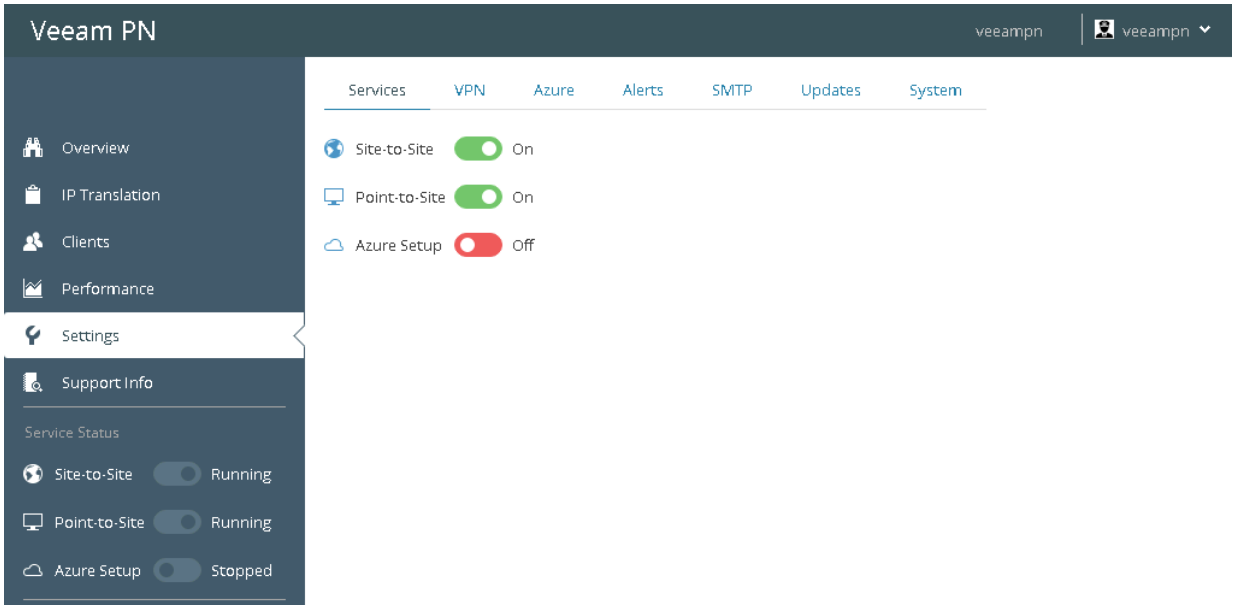
To disable a Veeam PN service:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. In the **Services** list, set the toggle of the service to the **Off** position.

To enable a previously disabled service:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. In the **Services** list, set the toggle of the service to the **On** position.

> **NOTE:**
>
> Before you enable the Azure service, you must configure Azure settings in the network hub portal. For more information, see Configuring Microsoft Azure Settings.



Configuring VPN Settings

When you deploy the network hub, you configure network hub settings. If necessary, you can modify these settings.

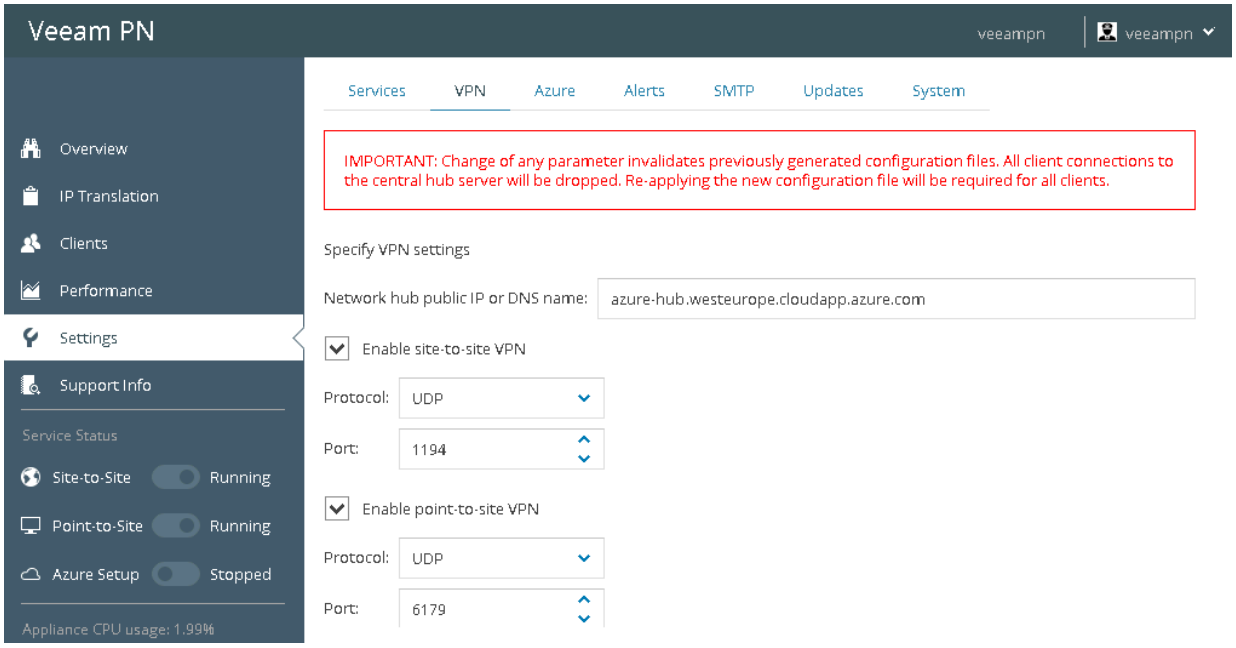
> **IMPORTANT!**
>
> If you modify network hub settings, you must download configuration files for all Veeam PN clients and re-deploy them on site gateways and standalone computers. If you do not download and re-deploy configuration files, clients will lose a connection to the VPN. For more information, see Modifying Clients Settings.

To configure network hub settings:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. Click the **VPN** tab.
4. In the **Network hub public IP or DNS name** field, enter an IP address or full DNS name of the network hub. The IP address or DNS name must be public.
5. Select the **Enable site-to-site VPN** check box to enable site-to-site communication between remote networks. In the fields below, specify settings for the site-to-site scenario:
   - From the **Protocol** list, select a protocol over which sites will communicate with each other: UDP or TCP.
   - In the **Port** list, specify a port on which the network hub must listen for site gateway connections. By default, port 1194 is used.
6. Select the **Enable point-to-site VPN** check box to enable point-to-site communication for standalone computers. In the fields below, specify settings for the point-to-site scenario:
   - From the **Protocol** list, select a protocol over which standalone computers will communicate with the network hub: UDP or TCP.
   - In the **Port** list, specify a port on which the network hub must listen for standalone computers connections. By default, port 6179 is used.
7. Click **Apply** to save modified settings.

NOTE:

It is recommended that you use the UDP protocol. While TCP guarantees delivery of data packets, UDP ensures faster data transmission since it does not require any data flow control.



Changing Advanced VPN Server Settings

In some cases, you may need to change advanced VPN settings. To do this, you can edit VPN configuration files manually.

IMPORTANT!

You must edit VPN configuration files only after you configure the network hub appliance with Veeam PN Web UI.

To change advanced VPN settings:

1. Enable SSH access to the network hub appliance. For more information, see Enabling and Disabling SSH Access.
2. Connect to the network hub appliance over an SSH client.
3. Edit the following configuration files:
   - `/etc/veeampn/SiteOVPN.cfg` — site-to-site VPN configuration files.
   - `/etc/veeampn/EndpointOVPN.cfg` — VPN configuration files for standalone clients.
4. After you edit configuration files, disable and re-enable the site-to-site and/or point-to-site services. For more information, see Enabling and Disabling Veeam PN Services.
5. Disable SSH access to the network hub appliance if you no longer need it.

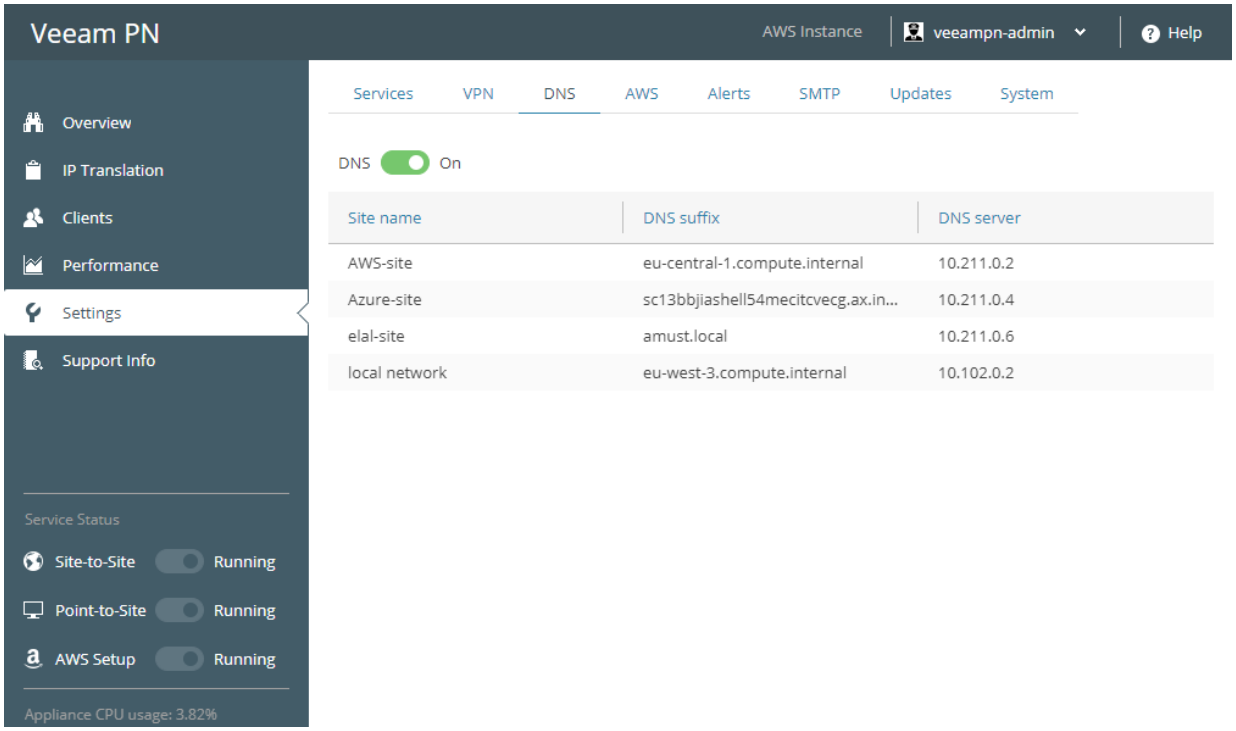
The most popular example of advanced VPN settings is pushing DHCP options to standalone clients, like DNS/WINS server configuration. For more information, see https://openvpn.net/index.php/open-source/documentation/howto.html#dhcp.

Enabling and Disabling DNS

In the network hub portal, you can see the list of configured sites, DNS suffixes and DNS servers.

If you want to disable DNS on a network hub, do the following:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. Click the **DNS** tab.
4. Click the **DNS** toggle to switch it to the **Off** state.

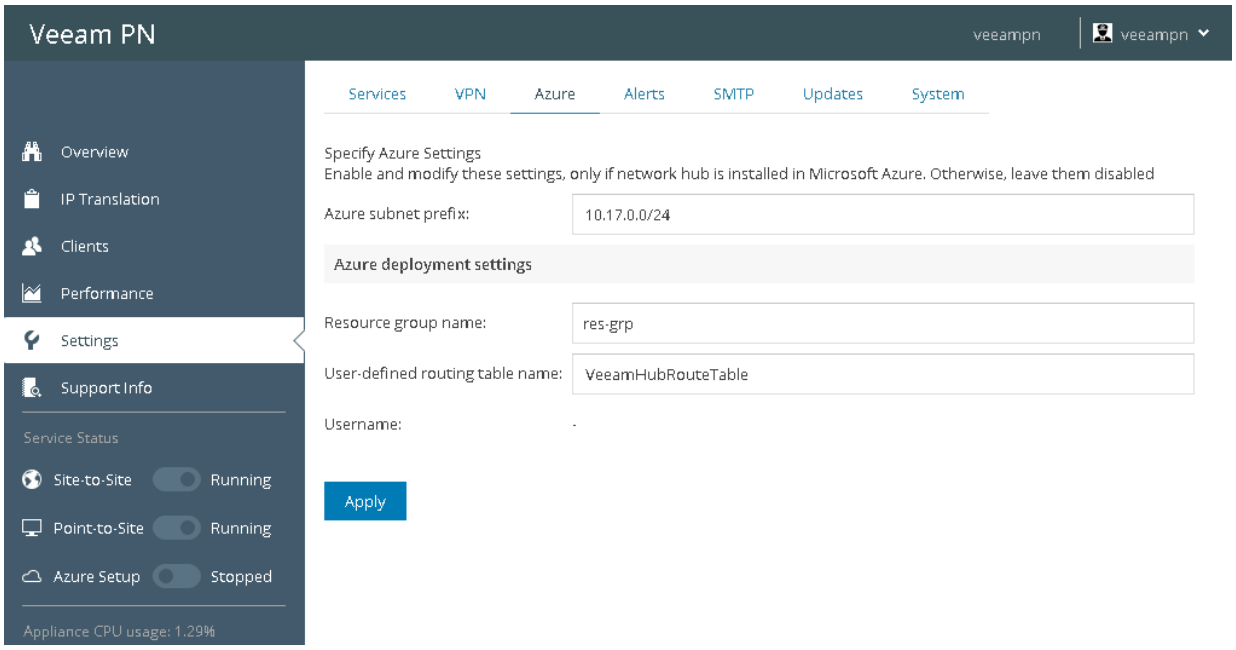


Configuring Microsoft Azure Settings

When you deploy the network hub in Microsoft Azure, you configure general network hub settings. If necessary, you can modify these settings.

To configure Microsoft Azure settings for the network hub, do the following:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. Click the **Azure** tab.
4. In the **Azure subnet prefix** field, specify an address of the Microsoft Azure network to which the network hub must be connected. To specify the address, use the CIDR notation.
5. In the **Resource group name** field, specify a name of the resource group that you specified when you deployed the network hub in Microsoft Azure.
6. In the **User-defined routing table name** field, specify a name of the routing table. Veeam PN will add to this table routes describing how traffic must travel in the VPN.
7. Click **Apply** to save modified Microsoft Azure settings.

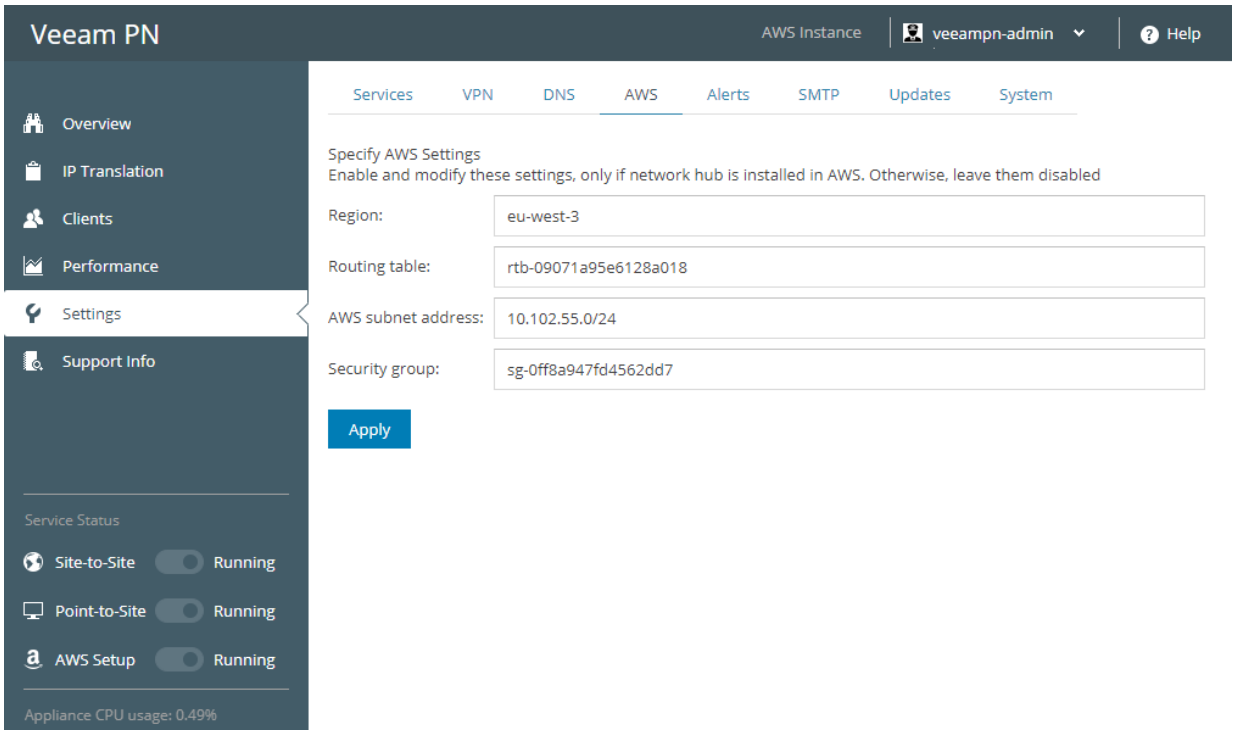


Configuring Amazon AWS Settings

When you deploy the network hub on Amazon AWS, you configure general network hub settings. If necessary, you can modify these settings.

To configure Amazon AWS settings for the network hub, do the following:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. Click the **AWS** tab.
4. In the **Region** field, specify a code of the Amazon EC2 region where you want to place your stack resources. For details, see the Regions and Availability Zones section of the Amazon Elastic Compute Cloud User Guide.
5. In the **Routing Table** field, specify the route table which defines where network traffic from your subnet is directed. For details, see the Route Table section of the Amazon Virtual Private Cloud User Guide.
6. In the **AWS subnet address** field, specify an address of the Amazon AWS network to which the network hub must be connected. To specify the address, use the CIDR notation.
7. In the **Security group** field, specify a security group for your VPC. A security group acts as a firewall for your instance to control inbound and outbound traffic. For details, see the Security Groups section of the Amazon Virtual Private Cloud User Guide.
8. Click **Apply** to save modified AWS settings.



Enabling and Disabling SSH Access

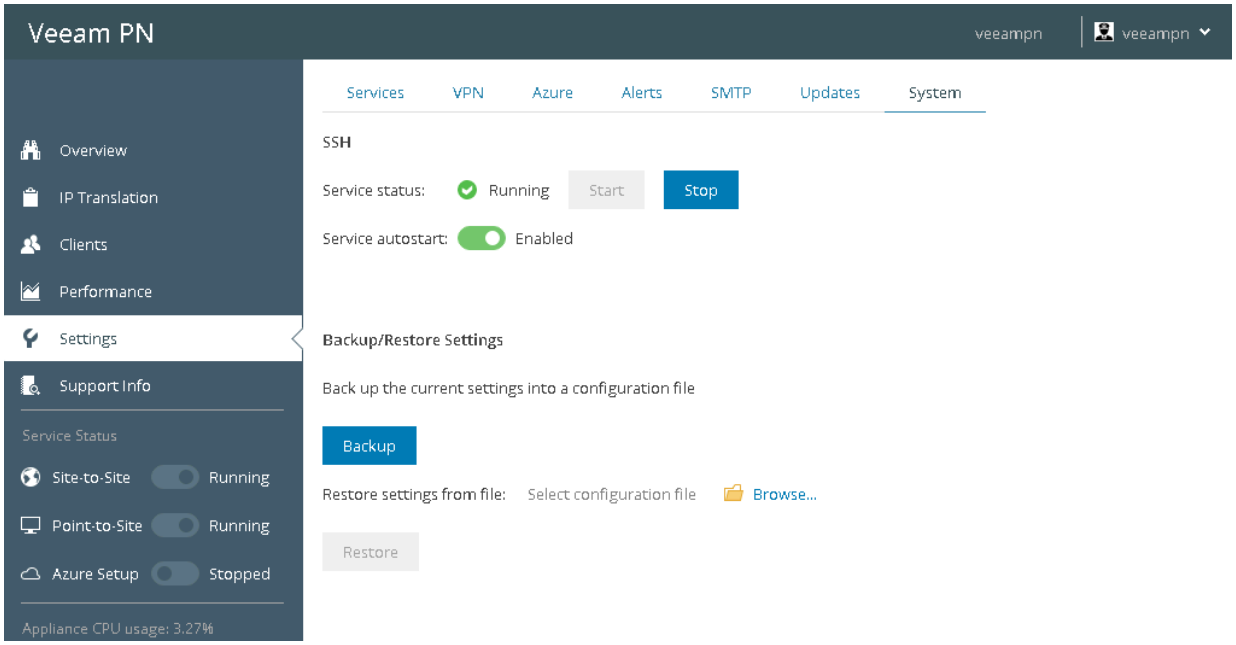
By default, you cannot access the network hub appliance over SSH. If necessary, you can enable SSH access to the appliance.

To enable SSH access to the network hub appliance:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. Click the **System** tab.
4. In the **Service autostart** field, set the toggle to the **On** position. The SSH service will be automatically started when the network hub appliance is powered on.
5. To start the SSH service and provide SSH access to the network hub appliance during the current work session, click **Start**.

To disable SSH access to the network hub appliance:

1. In the **Service autostart** field, set the toggle to the **Off** position.
2. To disable SSH access to the network hub appliance during the current work session, click **Stop**.

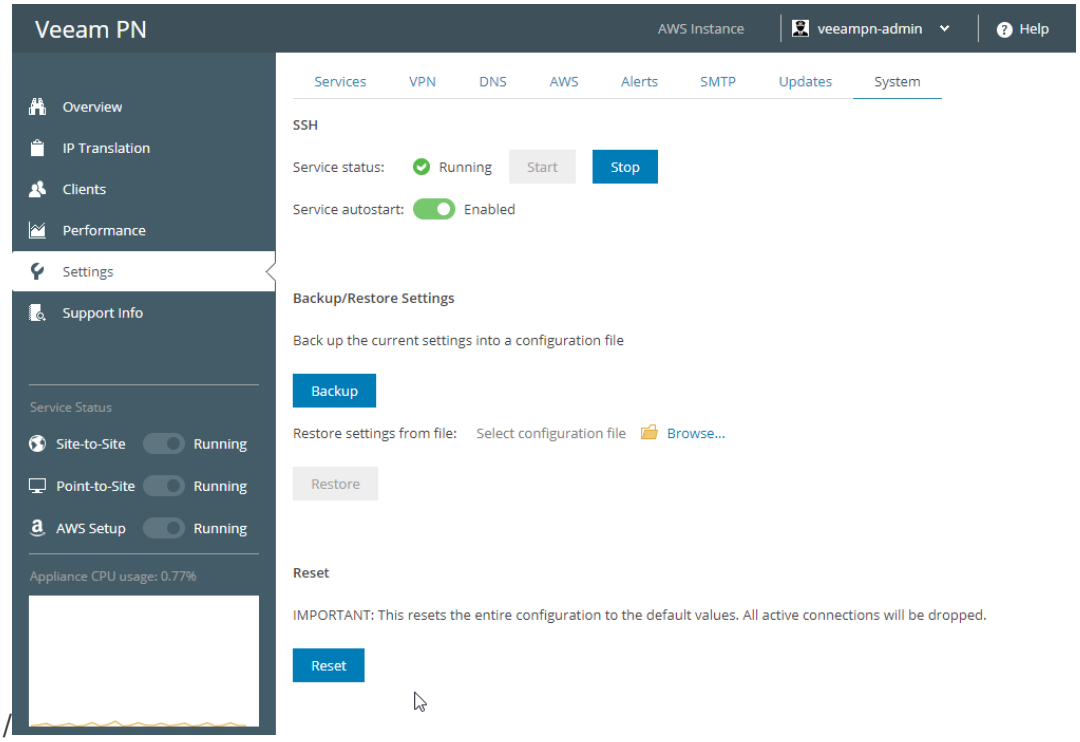


Resetting Network Hub Settings

If necessary, you can reset network hub settings. When you reset the network hub settings, you discard all changes that you have made since you deployed the network hub appliance. The appliance is rolled back to the impersonalized state, and you can configure network hub settings anew with the **Initial Configuration** wizard.

To reset network hub settings:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. Click the **System** tab.
4. Click **Reset**.



Setting Network Hub Reboot Time

By default, the network hub appliance is configured to apply security updates automatically, and is rebooted at 2:00 AM UTC after updates installation, if needed. You can change the default reboot time for the appliance.

To change the default reboot time:

1. Enable SSH access to the network hub appliance. For more information, see Enabling and Disabling SSH Access.
2. Connect to the network hub appliance over an SSH client.
3. Open the `/etc/apt/apt.conf.d/50unattended-upgrades` configuration file for editing.
4. Modify the following line as required (keep in mind that the reboot time is provided in UTC):

```
Unattended-Upgrade::Automatic-Reboot-Time "02:00"
```

Configuring Clients

After you deploy the network hub, you must register clients that must have access to the VPN in the network hub portal. Veeam PN lets you register the following types of clients:

- Entire sites — if you want to implement the site-to-site scenario, you must specify settings for all on-premises networks that you want to add to the VPN.
- Standalone computers — if you want to implement the point-to-site scenario, you must configure VPN settings for all standalone computers that must have access to the VPN.
- HUB site — if the network hub is deployed on a local site and you want to provide connectivity to machines on this site, you must specify settings for this site.

When you register a client, Veeam PN generates a configuration file that contains VPN connection settings for the client. You must use the configuration file to set up a site gateway in the on-premises network, configure a VPN connection on a standalone computer. For more information, Deploying Site Gateways and Configuring Standalone Computers.

Registering Clients

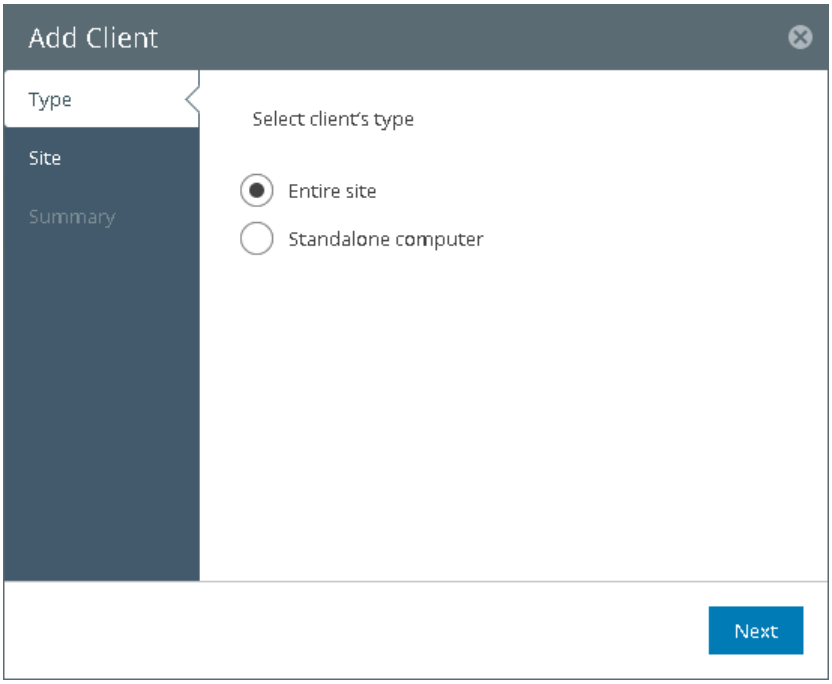
You can register two types of clients in the network hub portal:

- Entire sites
- Standalone computers
- Hub site

Registering Entire Sites

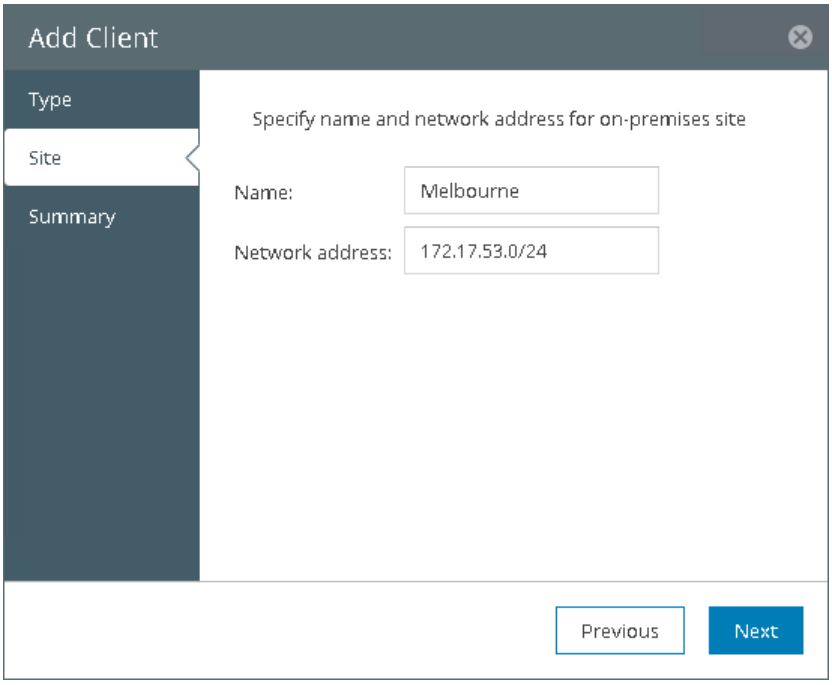
To register an entire site:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Clients**.
3. At the top of the clients list, click **Add**.
4. At the **Type** step of the wizard, select **Entire site**.



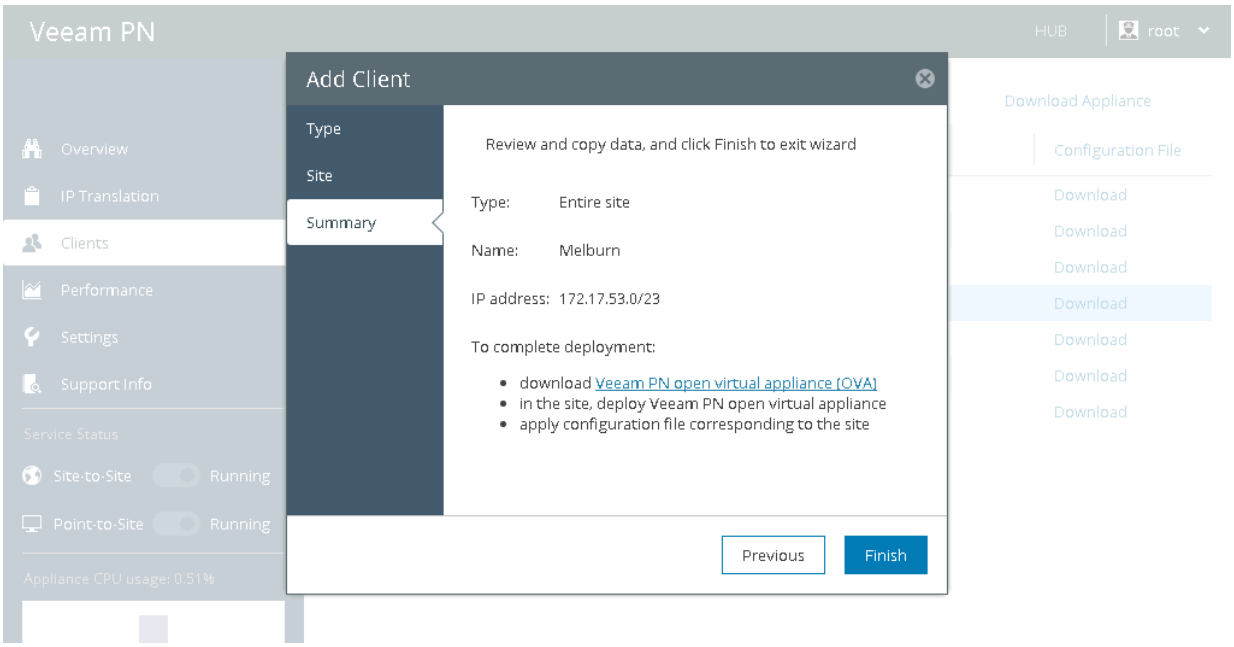
5. At the **Site** step of the wizard, enter details for the on-premises site:
   - In the **Name** field, enter a name for the site. The site name will be displayed in the list of clients.
   - In the **Network address** field, enter the address of the remote network using the CIDR notation.

> **IMPORTANT!**
>
> The site name must not contain space characters.



6. At the **Summary** step of the wizard, review details of the site and click **Finish** to close the wizard.

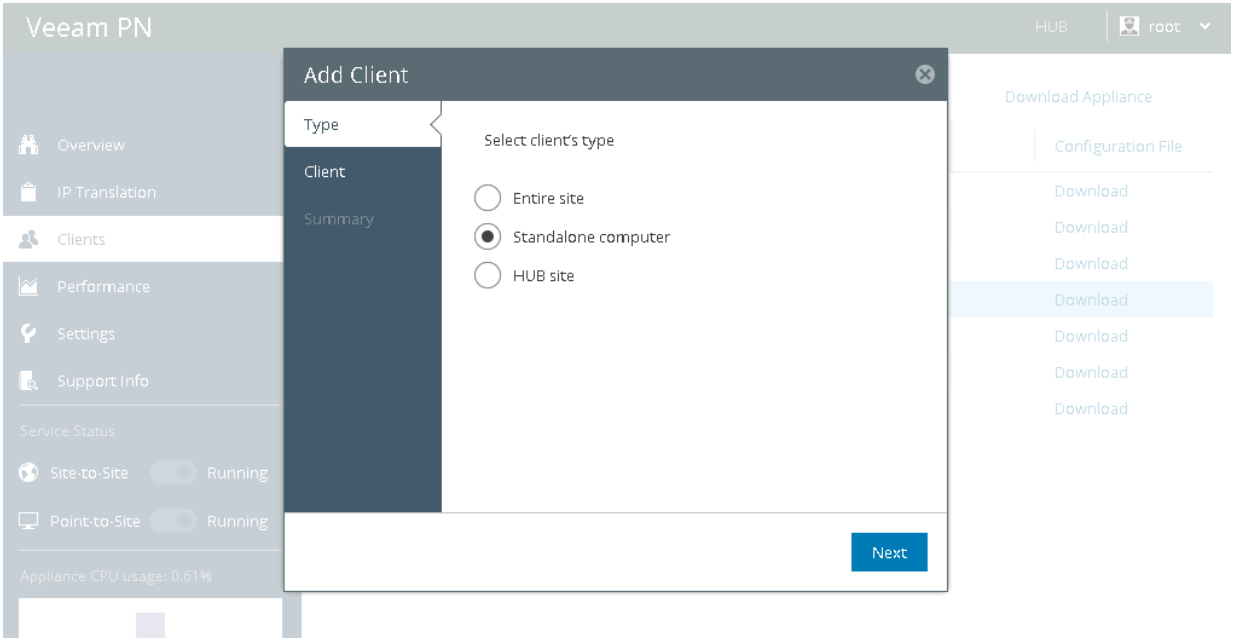
   After you click **Finish**, Veeam PN will generate an XML file with VPN settings for the on-premises site. The XML file will be automatically downloaded to the default downloads folder. Do not delete the downloaded file: you will need it to configure a site gateway in the on-premises network.



Registering Standalone Computers

To register a standalone computer:

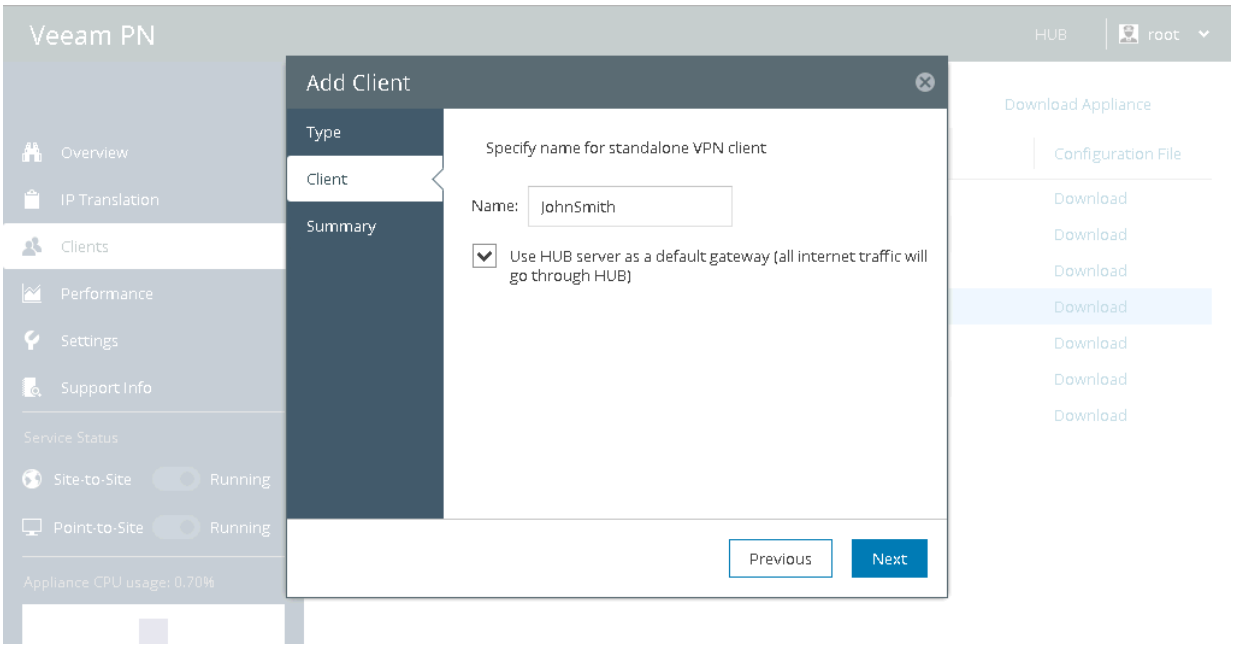
1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Clients**.
3. At the top of the clients list, click **Add**.
4. At the **Type** step of the wizard, select **Standalone computer**.



5. At the **Client** step of the wizard, enter a name for the standalone computer. The computer name will be displayed in the list of clients.

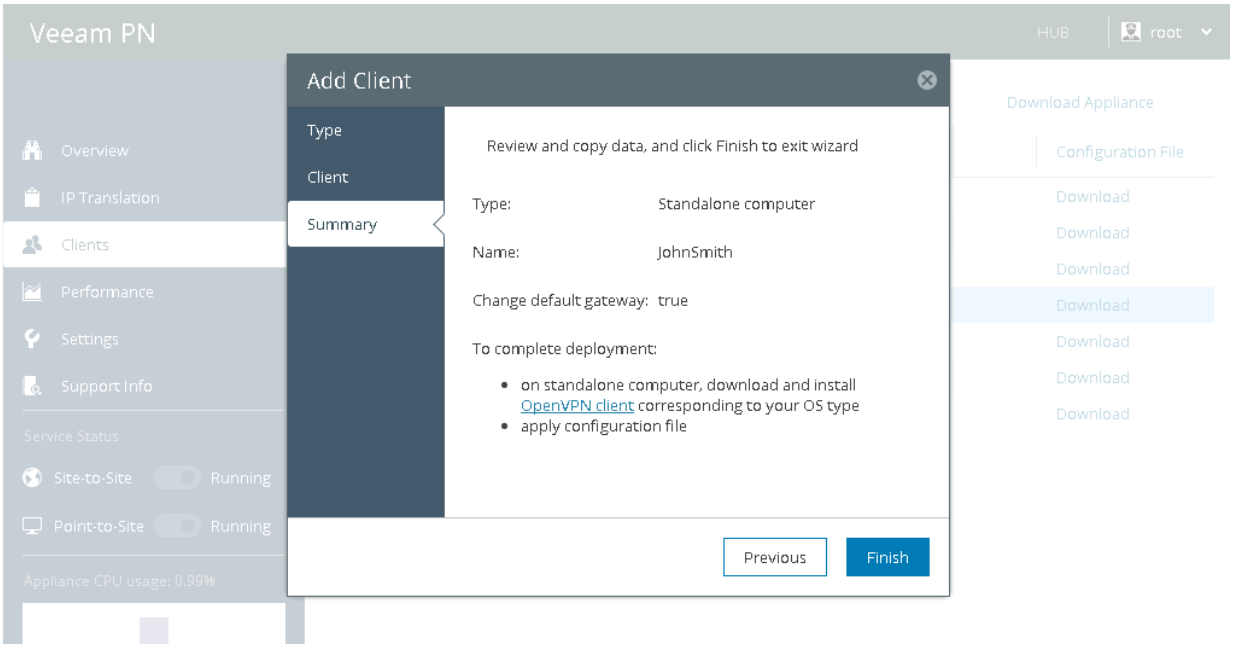
> **IMPORTANT!**
>
> The client name must not contain space characters.

6. Select the **Use HUB server as a default gateway** check box. With this option enabled, Veeam PN will use the network hub as a default gateway and route all Internet traffic for the client over the network hub.



7. At the **Summary** step of the wizard, review details of the client and click **Finish** to close the wizard.

   After you click **Finish**, Veeam PN will generate an OVPN file with VPN settings for the registered client. The OVPN file will be automatically downloaded to the default downloads folder. Do not delete the downloaded file: you will need it to configure VPN connection settings on the standalone computer.



Registering Hub Site

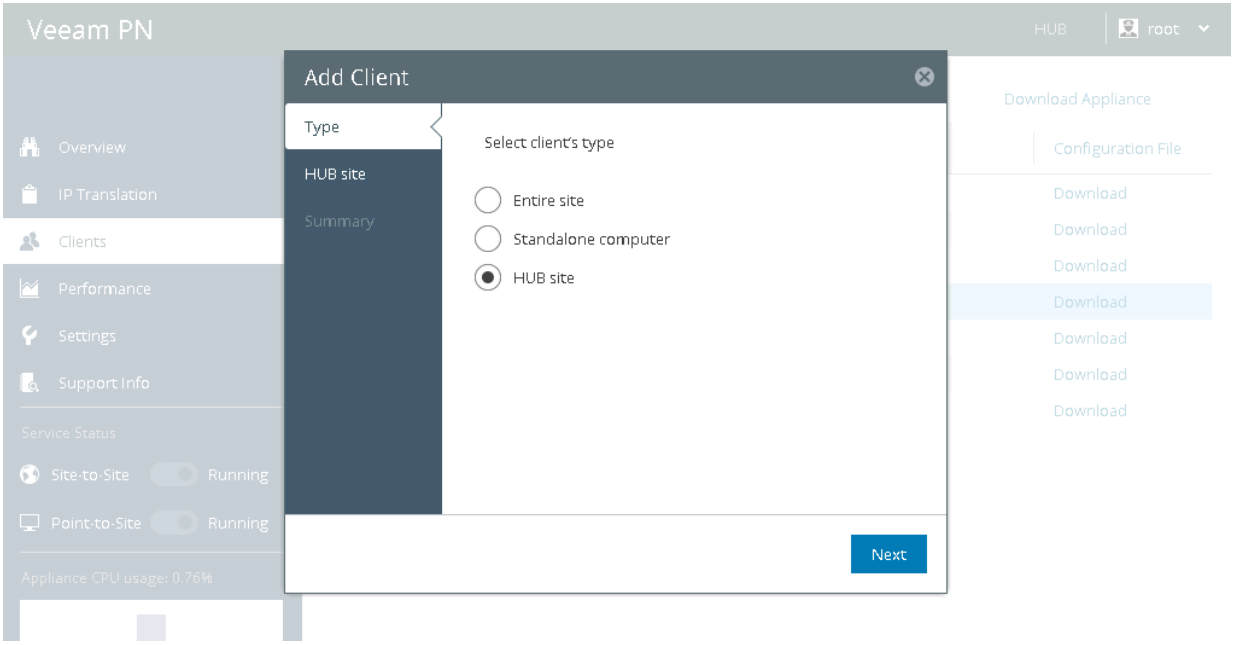
If you set up the network hub in a local site and want to make machines in this site accessible over the VPN, you must register this local site as a client in the network hub portal.

For example, you want to unite 3 sites over the VPN: *Site A*, *Site B* and *Site C*. In *Site A*, you deploy the network hub. If you do not add *Site A* as a client to the network hub portal, machines from *Site B* and *Site C* will not be able to communicate with machines in *Site A*; they will only be able to communicate with each other, routing traffic over the network hub deployed in *Site A*. If you add *Site A* as a client, machines from *Site A*, *Site B* and *Site C* will be able to communicate with each other, routing traffic over the network hub in *Site A*.

> **IMPORTANT!**
>
> After you register a hub site as a client, you do not need to perform additional configuration actions: download a configuration file and set it up (as for entire site and standalone computer clients). Bear in mind that the hub site client always remains in the *Disconnected* state, which is an expected behaviour.

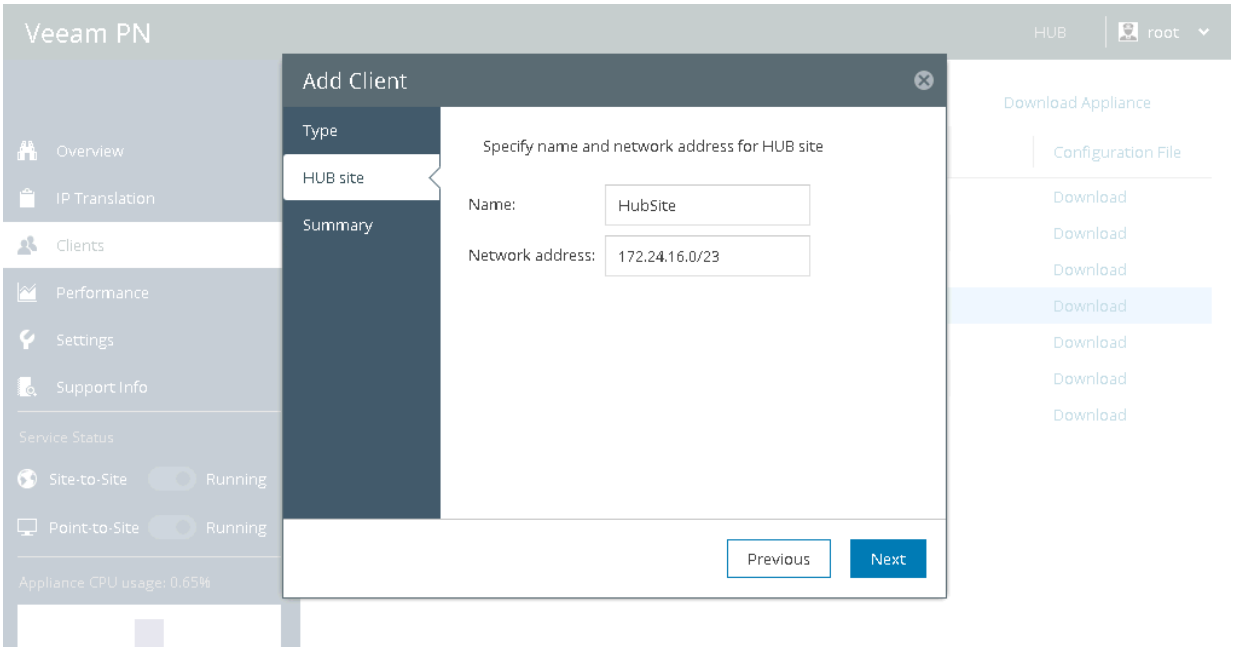
To register a hub site client:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Clients**.
3. At the top of the clients list, click **Add**.
4. At the **Type** step of the wizard, select **HUB site**.

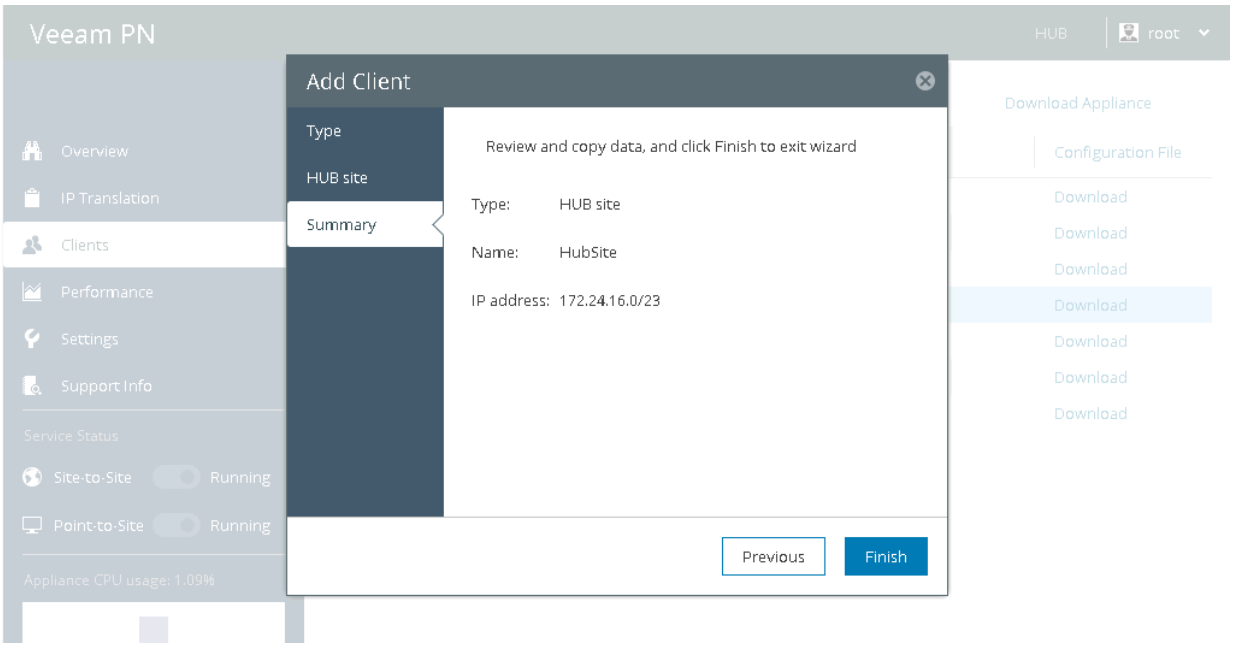


5. At the **Site** step of the wizard, enter details for the site where the network hub is deployed:
   - In the **Name** field, enter a name for the site. The site name will be displayed in the list of clients.
   - In the **Network address** field, enter the address of the network where the network hub is deployed using the CIDR notation.

> **IMPORTANT!**
>
> The site name must not contain space characters.



6. At the **Summary** step of the wizard, review details of the site and click **Finish** to close the wizard.



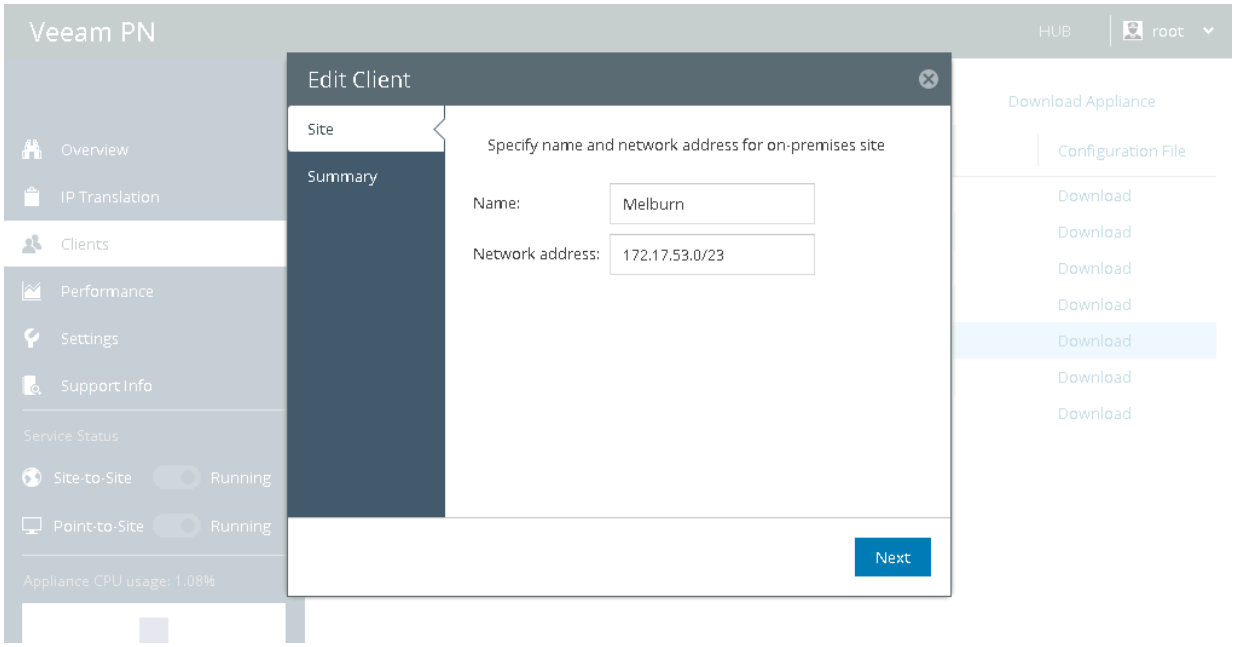
Modifying Clients Settings

If necessary, you can modify settings of a client registered in the Veeam PN portal. For example, you may want to change the network address of an on-premises site.

When you modify client settings, Veeam PN generates a new configuration file. You must download a new version of the configuration file and set it up on the site gateway or standalone computer. If you do not re-deploy the configuration file, the client will lose a connection to the VPN.

To modify client settings:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Clients**.
3. In the clients list, select the client and click **Edit** at the top of the list.
4. Modify client settings as required and save the modified settings.
5. In the **Configuration File** column of the clients list, click **Download** to get a configuration file for the client.
6. Use the configuration file to update VPN connection settings on the client side. For more information, see Re-Deploying Configuration Files and Configuring Standalone Computers.



Disabling and Enabling Clients

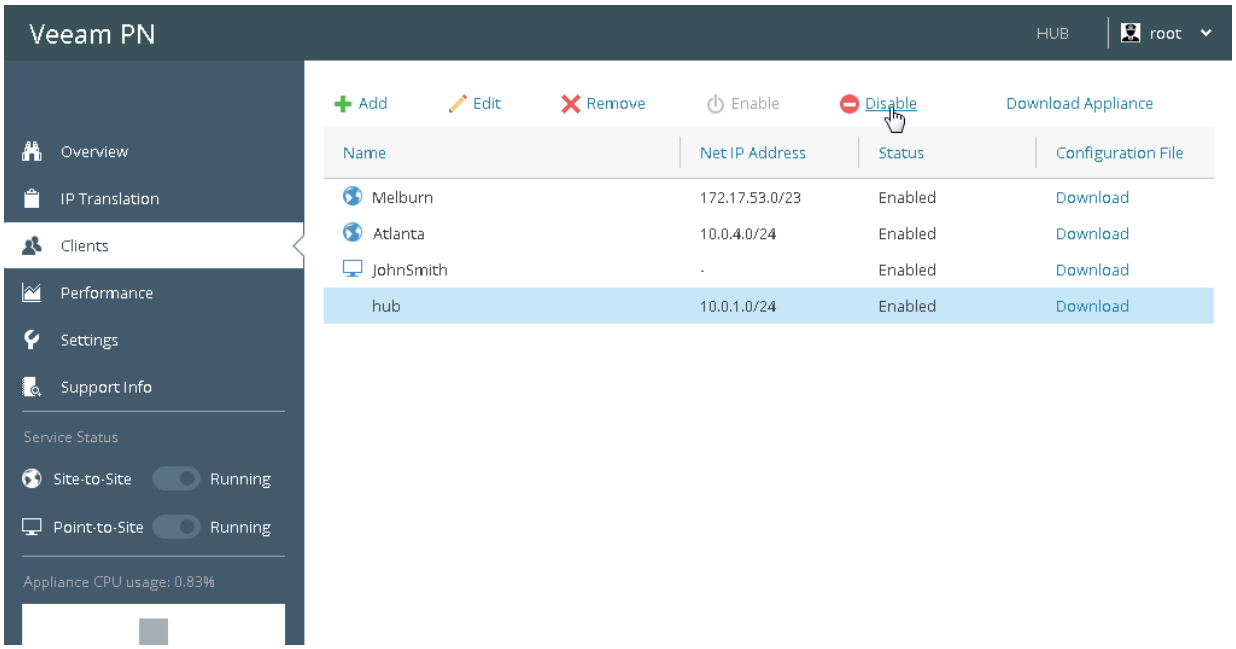
You can disable Veeam PN clients, for example, if you want to temporary prevent a standalone computer from accessing the VPN.

To disable a client:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Clients**.
3. In the clients list, select the client and click **Disable** at the top of the list.

To enable a previously disabled client:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Clients**.
3. In the clients list, select the client and click **Enable** at the top of the list.

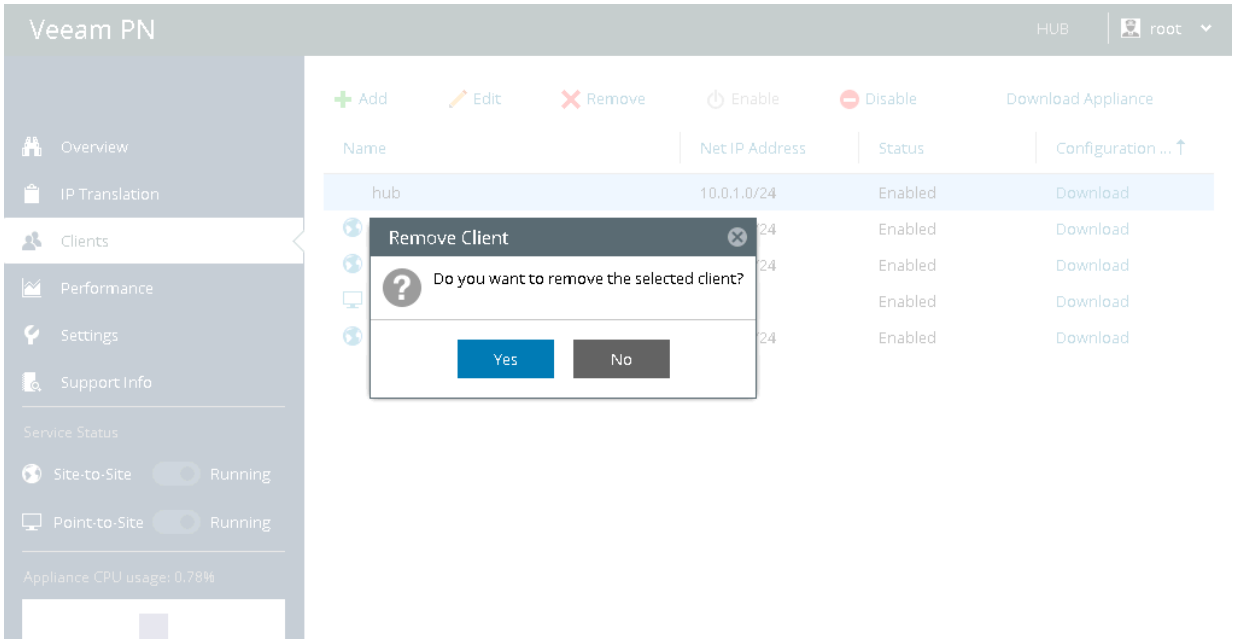


Removing Clients

If a client no longer requires accessing the VPN, you can remove the client from the network hub portal.

To remove a client:

1. Log in to the network hub portal as a Portal Administrator.
2. In the configuration menu on the left, click **Clients**.
3. In the clients list, select the client and click **Remove** at the top of the list.



Deploying Site Gateways

To implement the site-to-site scenario, you must deploy one site gateway in every remote network that you plan to add to the VPN (except the network where the network hub is deployed). The site gateway is a virtual appliance that establishes a VPN tunnel with the network hub, which lets the VPN traffic travel securely between sites.

Setting Up Site Gateways

To set up a site gateway, you must deploy a Veeam PN appliance in the VMware vSphere environment. The Veeam PN appliance is distributed as an OVA package. The package contains a pre-configured 64-bit Linux virtual appliance on which Veeam PN components are set up.

To deploy a site gateway, you must perform the following steps:

1. Deploy a Veeam PN appliance from the OVA package.
2. Configure initial site gateway settings.

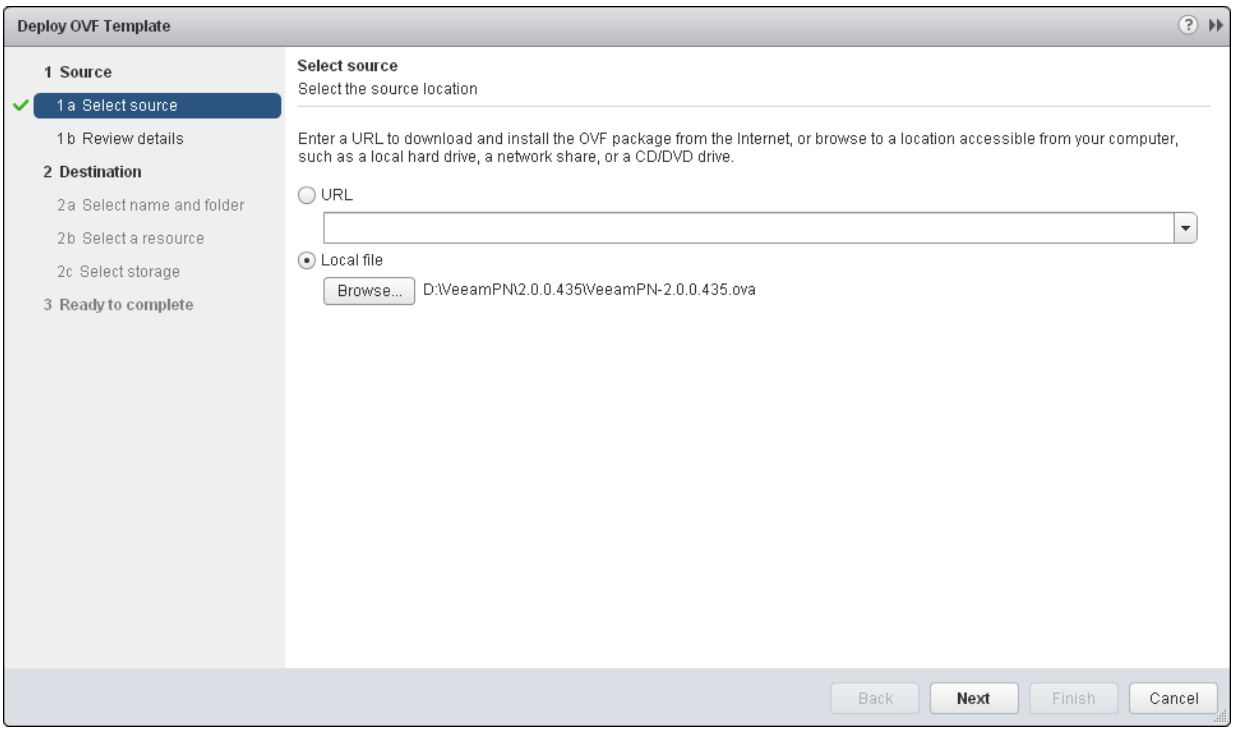
Before You Begin

Before you deploy a site gateway, you must register the on-premises network, in which the gateway will reside, in the network hub portal, and obtain a configuration file for this network. For more information, see Registering Clients.

Deploying Veeam PN Appliance

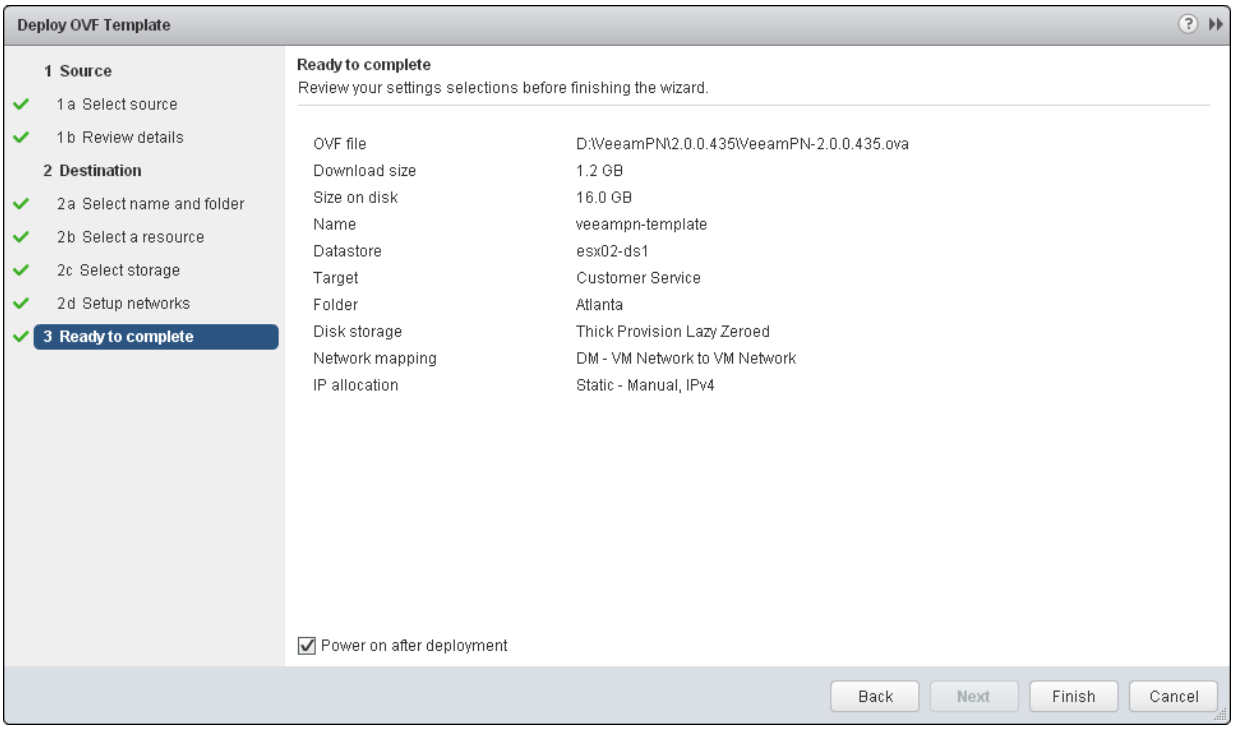
To deploy a Veeam PN appliance from the OVA package:

1. Download the Veeam PN OVA package from: https://www.veeam.com/downloads.html and save it in a network shared folder.
2. In VMware vSphere Web Client, open the hosts and clusters inventory list and select a host on which you want to deploy the appliance.
3. From the menu at the top of the working area, select **Actions** > **Deploy OVF Template**.
4. At the **Select source** step of the wizard, select **Local file**, click **Browse** and browse to the Veeam PN OVA package.



5. Follow the next steps of the wizard and specify appliance deployment settings: datastore on which the appliance VM disk must be placed, disk format, network to which the appliance must be connected and so on.

6. At the last step of the wizard, select the **Power on after deployment** check box and click **Finish**.



VMware vSphere will deploy the Veeam PN appliance on the selected host. The deployment process typically takes several minutes. Wait for the process to complete and proceed to the site gateway configuration.

Configuring Initial Site Gateway Settings

Right after deployment, the virtual appliance is impersonalized. To configure a site gateway, you must customize the appliance and configure initial gateway settings on it.

To configure a site gateway:

1. In VMware vSphere Web Client, navigate to the **Summary** tab and get an IP address of the deployed appliance.

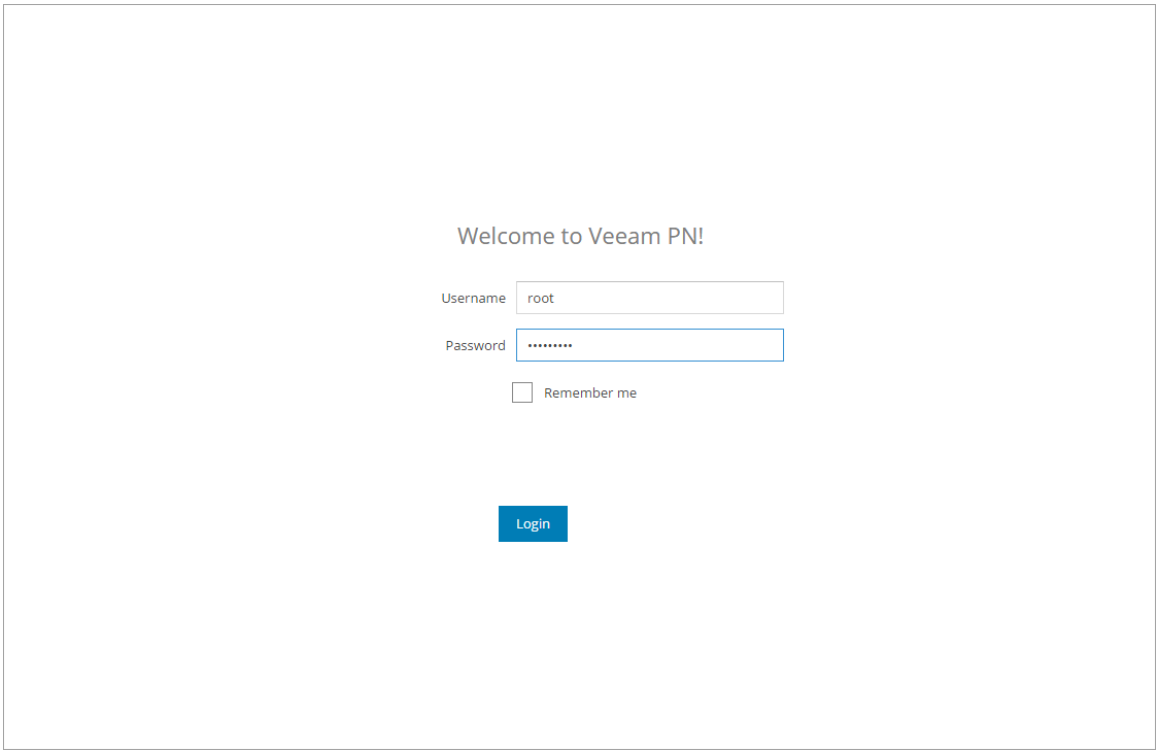
2. In a web browser, access the site gateway portal by the following address: `https://<applianceIPaddress>`, where `applianceIPaddress` is the IP address of the deployed appliance.

   When you access the site gateway portal in the web browser, the browser will display a warning notifying that the connection is untrusted. Ignore the warning and agree to proceed to the portal.

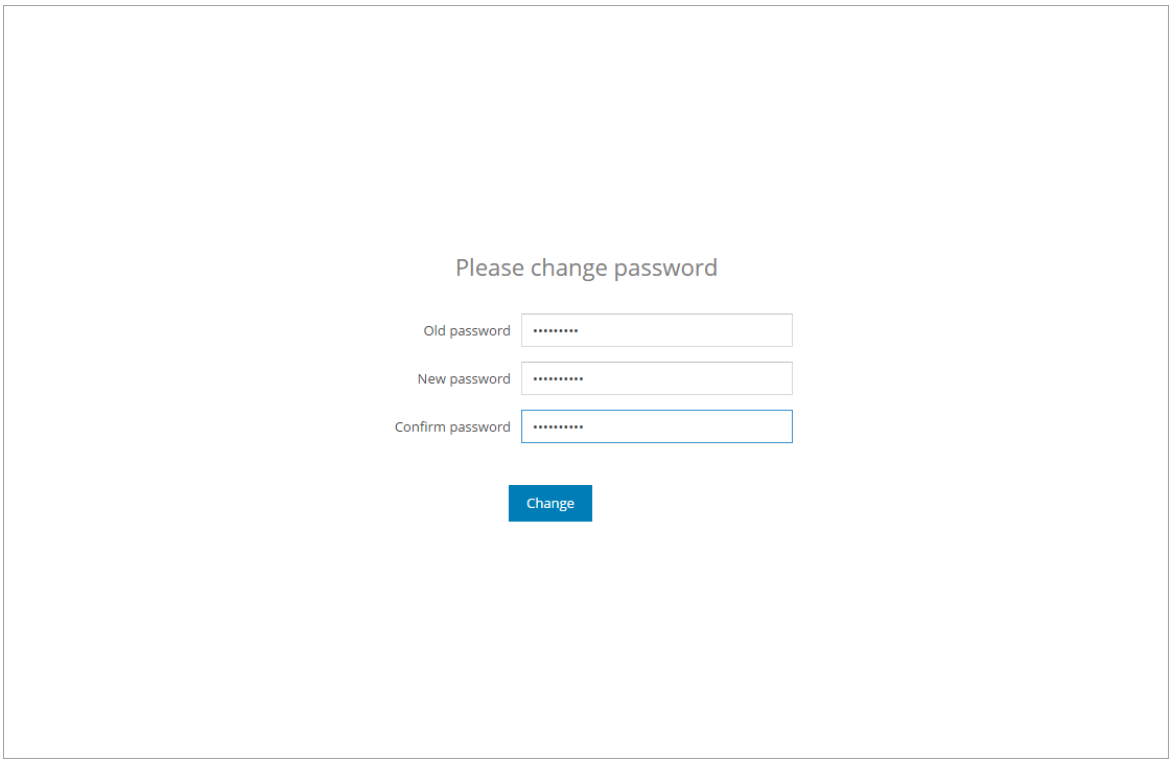
3. At the **Welcome to Veeam PN** screen of the portal, log in to the site gateway portal under the in-built Administrator account. The Administrator account has the following credentials:

   - Username: *root*
   - Password: *VeeamPN*

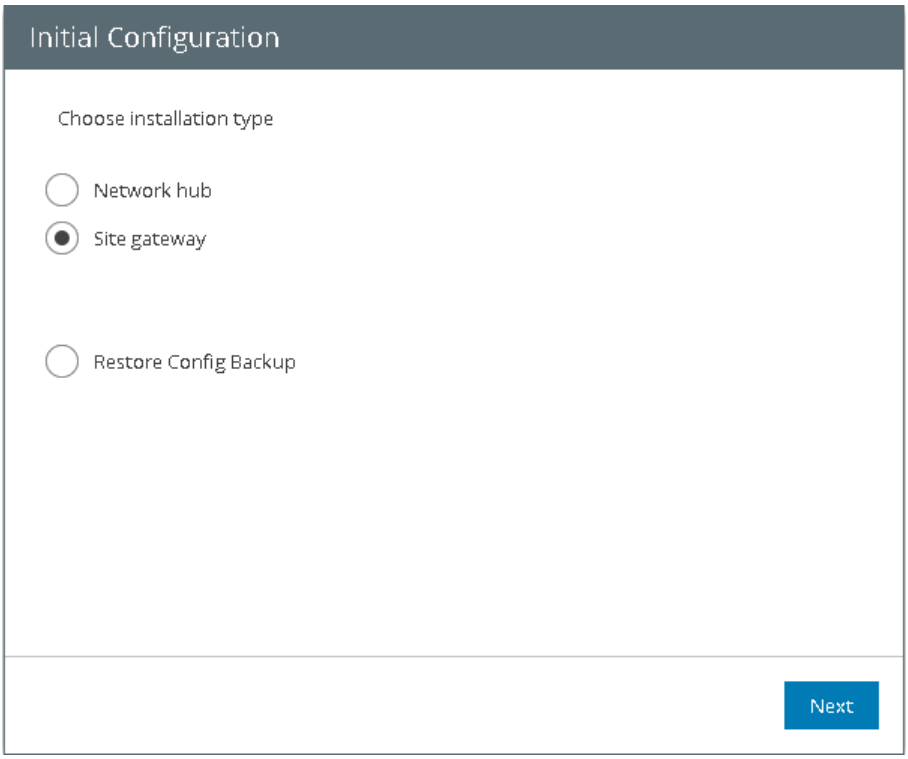
   Click **Login**.



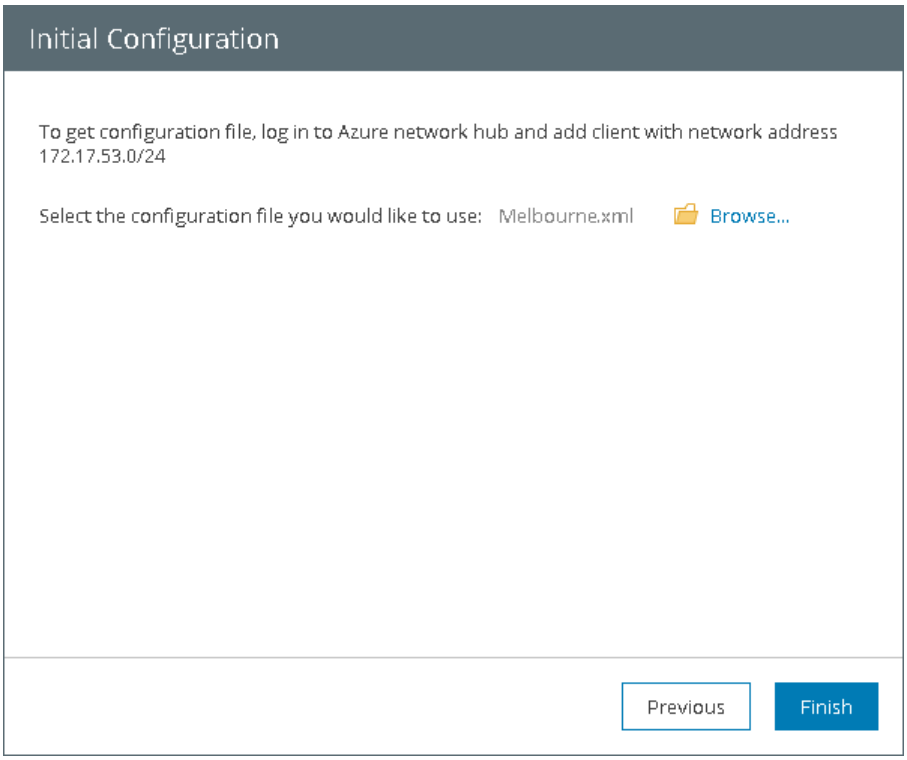
4. After you log in to the portal for the first time, Veeam PN will offer you to change a password for the built-in account. On the displayed screen, enter the old and new passwords and click **Change**.



5. At the first step of the **Initial Configuration** wizard, select **Site gateway**.



6. Click **Browse** and browse to the configuration file generated in the network hub portal.



7. Click **Finish**. Veeam PN will configure the gateway appliance and display the site gateway portal.

What You Do Next

After you deploy a site gateway, you must perform the following steps:

- [For network hub deployed in on-premises network] You must add a new route on the default gateway in the on-premises network where you set up the site gateway. The route must destine all outgoing traffic to the site gateway. For more information, see Adding Static Routes on Default Gateways.
- If necessary, you can change gateway settings, for example, configure alerts, enable SSH access to the gateway appliance and so on. For more information, see Configuring Site Gateway Settings.

Adding Static Routes on Default Gateways

In the VPN, Veeam PN routes traffic through a site-to-site VPN tunnel. To make sure that the traffic goes to a proper destination, you need to let both sides of the VPN tunnel know how to route traffic between each other.

When you register an on-premises network in the network hub portal and deploy a site gateway in this on-premises network, you 'tell' Veeam PN that this site gateway will be responsible for this on-premises network. As soon as the network hub receives traffic designated for this network, it forwards this traffic through the VPN tunnel established between the network hub and the site gateway.

However, machines in on-premises networks also need to know where they must send traffic so that it is routed over the VPN tunnel. Since machines in one remote network use default gateways to communicate with machines in other networks, you need to add static routes on default gateways. These static routes will destine the traffic to the Veeam PN appliance — the network hub or site gateway, that, in their turn, will route traffic through the VPN tunnel established between two remote sites.

For example, you want to add two sites to the VPN. The network hub is deployed in *Site* A and a site gateway is deployed in *Site B*.

- **Site A**: 10.1.0.0/24

  Network mask: 255.255.255.0/24

  Network hub IP address: 10.1.0.2

  Default gateway IP address: 10.1.0.1

  Client machine IP address: 10.1.0.12

- **Site B**: 192.168.0.1/24

  Network mask: 255.255.255.0/24

  Site gateway IP address: 192.168.0.2

  Default gateway IP address: 192.168.0.1

  Client machine IP address: 192.168.0.14

In such configuration, if a client machine in *Site A* needs to communicate with a client machine in *Site B*, the traffic will first be sent to the default gateway 10.1.0.1 in *Site A*. The default gateway must then route the traffic to the network hub that, in its turn, will route the traffic through the VPN tunnel between remote networks. For this reason, you must add the following route on the default gateway 10.1.0.1: if the traffic is designated for 192.168.0.0, the next hop must be the network hub 10.1.0.2.

```
route add 192.168.0.0 mask 255.255.255.0 10.1.0.2
```

In a similar manner, you must add a route on the default gateway 192.168.0.1 in *Site B*. If the traffic is designated for 10.1.0.0, the next hop must be the site gateway 192.168.0.2:

```
route add 10.1.0.0 mask 255.255.255.0 192.168.0.2
```

NOTE:

If the network hub is deployed in Microsoft Azure, Veeam PN automatically adds all necessary routes for machines in remote networks to the user-defined routing table.

Configuring Site Gateway Settings

After you deploy a site gateway, you can configure the following settings for it:

- Enable and disable the site-to-site service
- Re-deploy the configuration file
- Enable and disable SSH access
- Modify site gateway settings
- Reset site gateway settings

Enabling and Disabling Site Service

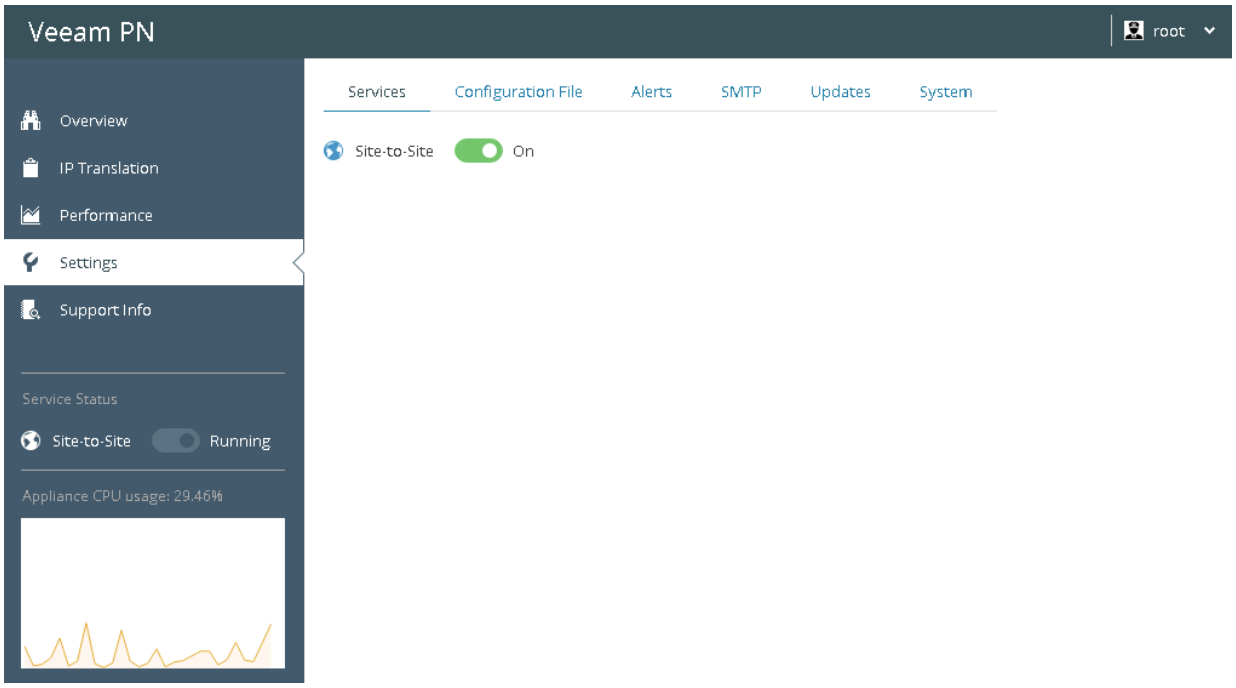
If necessary, you can disable the site-to-site service for a site gateway. When you disable the site-to-site service, the network in which the site gateway is deployed gets disconnected from the network hub, and all machines residing in this network lose access to the VPN.

To disable the site-to-site service:

1. Log in to the site gateway portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. In the **Services** list, set the toggle of the Site-to-Site service to the **Off** position.

To enable the previously disabled service:

1. Log in to the site gateway portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. In the **Services** list, set the toggle of the Site-to-Site service to the **On** position.



Re-Deploying Configuration Files

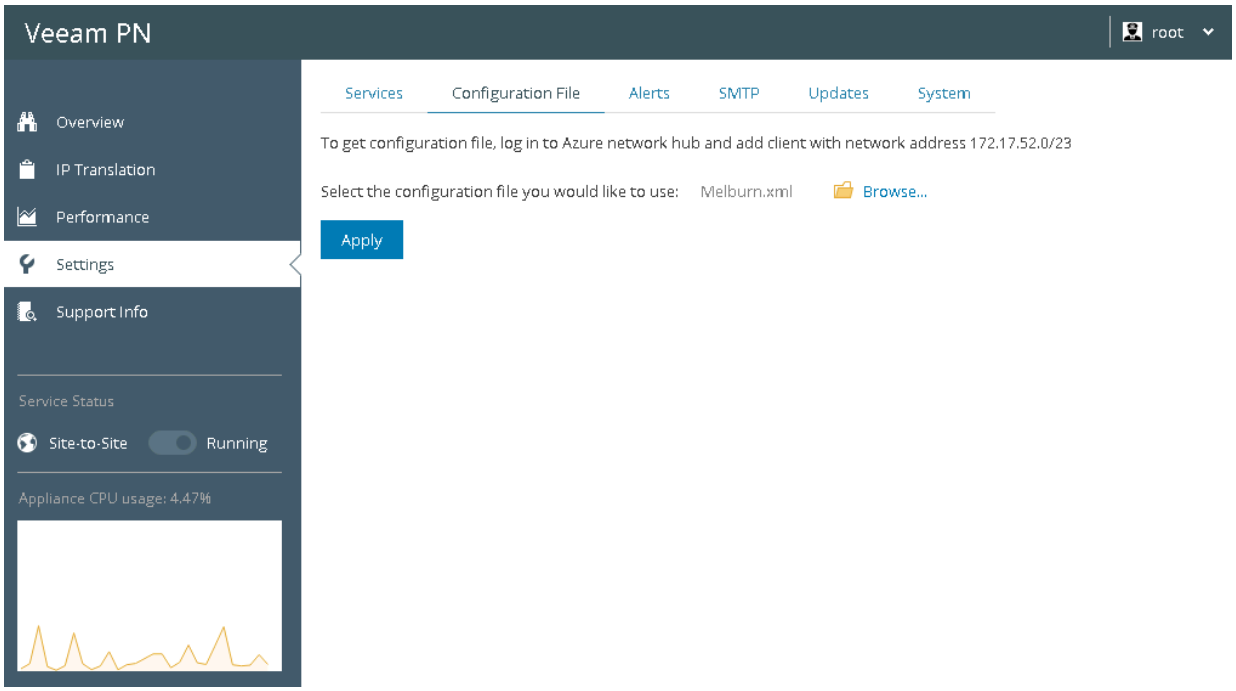
To set up a site gateway, you need a configuration file generated by the network hub. The configuration file contains VPN settings and lets you easily configure the site gateway in the remote network.

In some situations, you may need to re-deploy configuration files on the site gateway side. This can happen if you change network hub settings. In this case, you will need to re-generate configuration files for all clients registered in the Veeam PN portal and re-deploy these configuration files on site gateway appliances.

> **NOTE:**
>
> You do not need to re-deploy configuration files when you add new remote networks to the VPN. You must re-deploy configuration files only when you change settings of the network hub such as IP address, communication ports, protocol and so on.

To re-deploy the configuration file on a site gateway appliance:

1. Log in to the site gateway portal.
2. In the configuration menu on the left, click **Settings**.
3. Click the **Configuration File** tab.
4. Click **Browse** and browse to the configuration file.
5. Click **Apply**.



Enabling and Disabling SSH Access

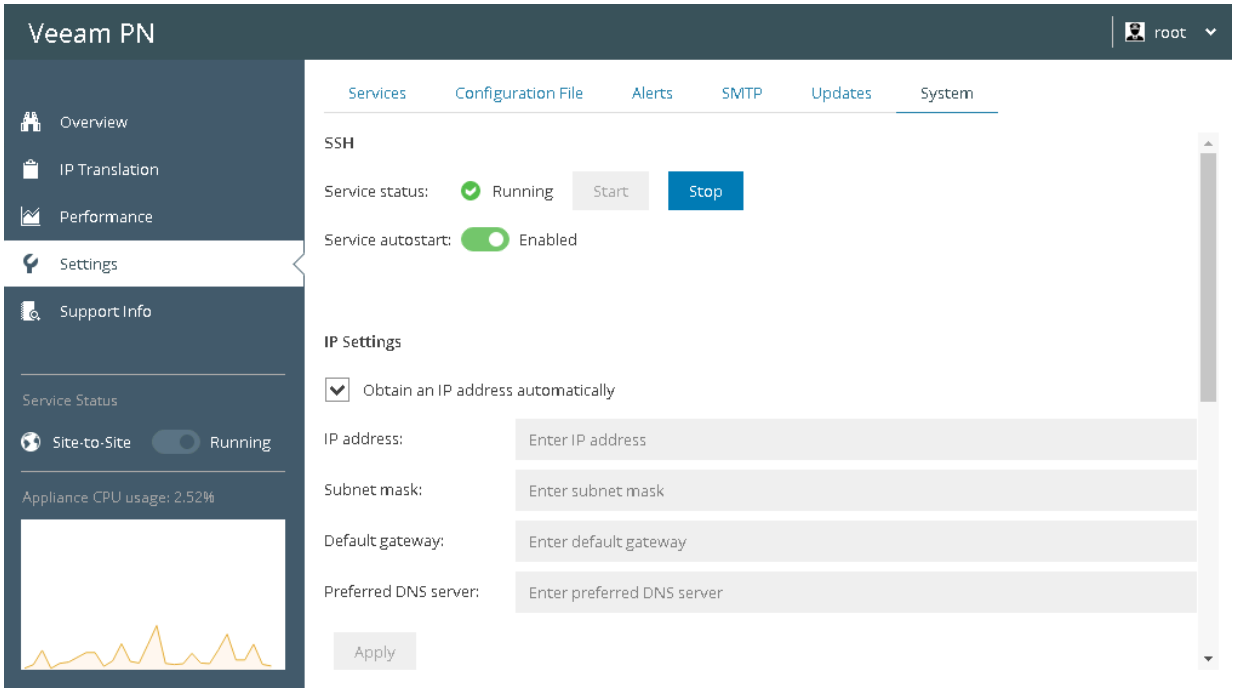
By default, you cannot access a site gateway appliance over SSH. If necessary, you can enable SSH access to the appliance.

To enable SSH access:

1. Log in to the site gateway portal.
2. In the configuration menu on the left, click **Settings**.
3. Click the **System** tab.
4. In the **Service autostart** field, set the toggle to the **On** position. The SSH service will be automatically started when the site gateway appliance is powered on.
5. To start the SSH service and provide SSH access to the appliance during the current work session, click **Start**.

To disable SSH access to the site gateway appliance:

1. In the **Service autostart** field, set the toggle to the **Off** position.
2. To disable SSH access to the appliance during the current work session, click **Stop**.

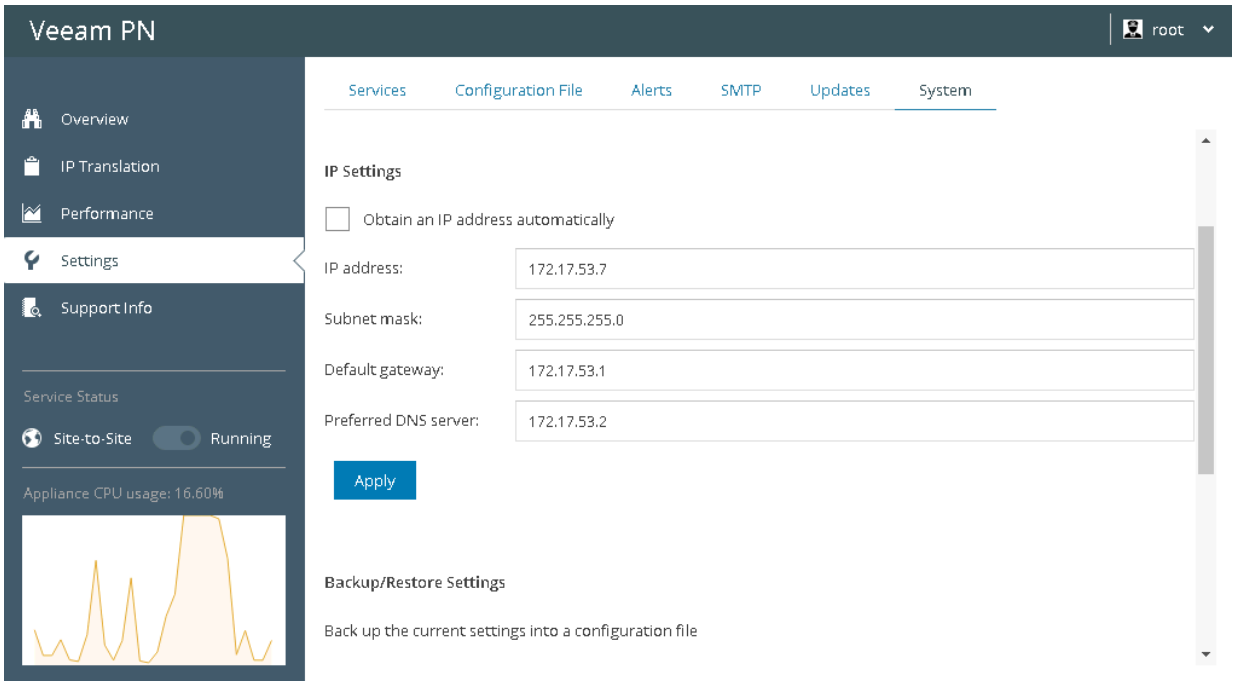


Modifying Site Gateway Settings

If necessary, you can modify site gateway settings, for example, change an IP address of the appliance.

To modify site gateway settings:

1. Log in to the site gateway portal.
2. In the configuration menu on the left, click **Settings**.
3. Click the **System** tab.
4. By default, a site gateway appliance automatically obtains networking information from DHCP. If there is no DHCP server in the network where the appliance resides or you want to manually configure IP settings for the appliance, clear the **Obtain an IP address automatically** check box and configure IP settings:
    a. In the **IP address** field, specify an IP address of the site gateway appliance.
    b. In the **Subnet mask** field, specify a mask of the network where the appliance resides.
    c. In the **Default gateway** field, specify an IP address of the default gateway in the network where the appliance resides.
    d. In the **Preferred DNS server** field, specify an IP address of the DNS server in the network where the appliance resides.
5. Click **Apply**.

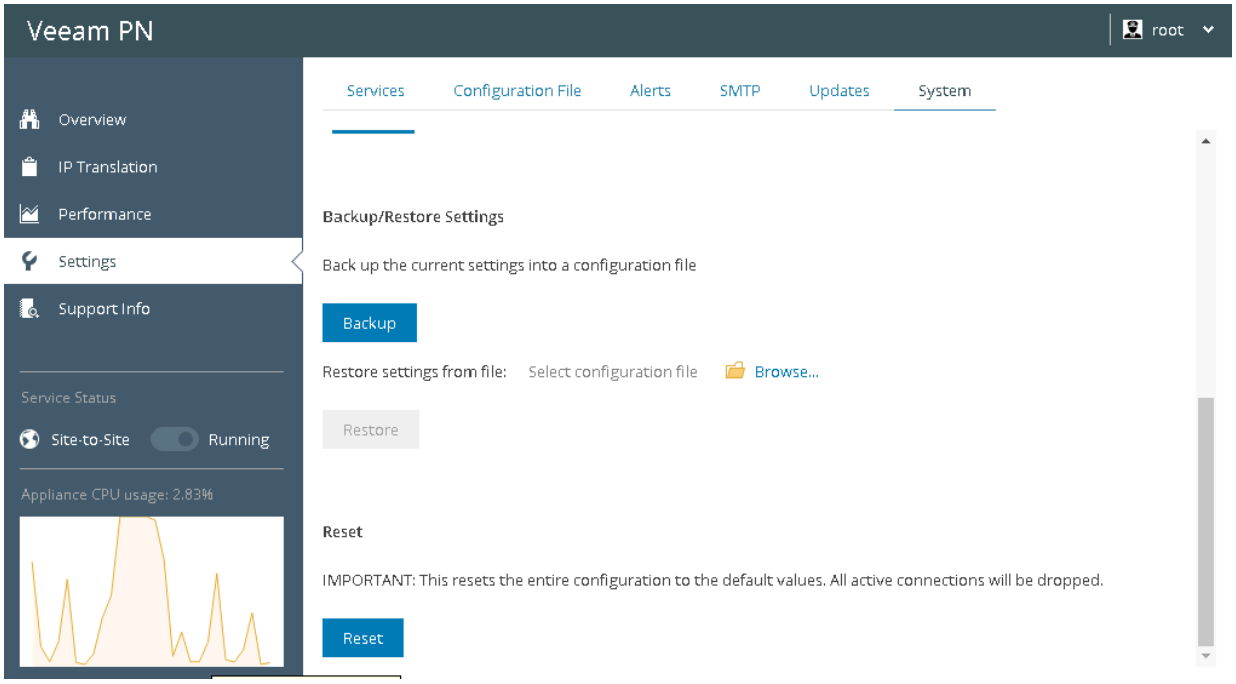


Resetting Site Gateway Settings

If necessary, you can reset site gateway settings. When you reset gateway settings, you discard all changes that you have made since you deployed the site gateway appliance. The appliance is rolled back to the impersonalized state, and you can configure site gateway settings anew with the **Initial Configuration** wizard.

To reset site gateway settings:

1. Log in to the site gateway portal.
2. In the configuration menu on the left, click **Settings**.
3. Click the **System** tab.
4. In the **Reset** field, click **Reset**.



Configuring Standalone Computers

After you set up the network hub, you can configure standalone computers (for the point-to-site scenario). A standalone computer is a machine that is able to connect to the VPN and use its resources.

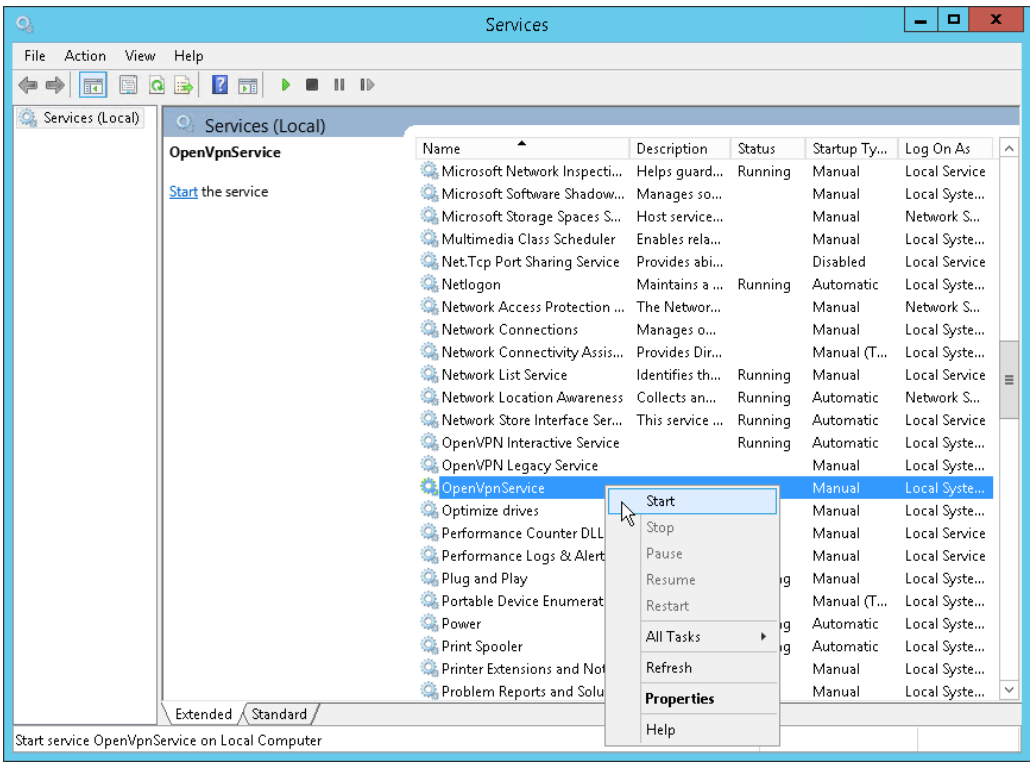
To allow a standalone computer to access the VPN, Veeam PN utilizes OpenVPN. You must install OpenVPN client software on the computer, and use an OVPN file configured by the network hub to set up the VPN connection settings.

> **NOTE:**
>
> Veeam PN lets you set up VPN access from any OS supported by OpenVPN. This section demonstrates OpenVPN client setup for Microsoft Windows OS. For information about OpenVPN setup for other OSes, see https://openvpn.net/index.php/access-server/docs/admin-guides-sp-859543150/howto-connect-client-configuration.html.

Before you configure VPN settings on a standalone computer, you must register the standalone computer in the network hub portal and obtain a configuration file for the computer. For more information, see Registering Clients.

To configure a standalone computer:

1. Download the OpenVPN setup file for the necessary OS from: https://openvpn.net/index.php/open-source/downloads.html.
2. Run the OpenVPN setup file and install the product on the computer with default installation settings.
3. On the standalone computer, place the client configuration file generated by the network hub in a folder where OpenVPN configuration files are stored (by default, `C:\Program Files\OpenVPN\config`).
4. From the Microsoft Windows start menu, select **Control Panel** > **Administrative Tools** > **Services** and start the OpenVPN Service.



Establishing VPN Connection

By default, the OpenVPN Service is set up to start manually. To easily establish a VPN connection for the standalone computer in future, you can do one of the following:

- Connect to the VPN using openVPN GUI
- Create a shortcut for the VPN connection
- Create a script file for the VPN connection
- Configure the openVPN service to start automatically

Connecting to VPN Using openVPN GUI

You can connect to the VPN using the openVPN GUI. Keep in mind that you must run the OpenVPN GUI with administrator privileges so that it can add routes to the routing table that are pulled from the OpenVPN server.

To connect to the VPN, right-click the **OpenVPN** shortcut on the Desktop and select **Run as administrator**.

Creating Shortcut for VPN Connection

You can create a shortcut for the VPN connection. To do this, right-click the **OpenVPN** shortcut on the Desktop. In the **Target** field of the **OpenVPN GUI Properties** window, specify the following string:

```
"C:\Program Files\OpenVPN\bin\openvpn-gui.exe" -- connect "C:\Program
Files\OpenVPN\config\client.ovpn"
```

where:

- `C:\Program Files\OpenVPN\bin\openvpn-gui.exe` is a path to the OpenVPN GUI executable file
- `C:\Program Files\OpenVPN\config\client.ovpn` is a path to the configuration file generated by the network hub

To establish a VPN connection, double-click the shortcut.

> **IMPORTANT!**
>
> The OpenVPN command must be run with the *'Run as Administrator'* privileges. If you have created a shortcut for the OpenVPN connection, right-click the shortcut and select **Properties**. On the **Shortcut** tab, click **Advanced** and select the **Run as administrator** check box.

Creating Script File for VPN Connection

You can create a batch file with the following command:

```
"openvpn-gui.exe" -- connect "C:\Program Files\OpenVPN\config\client.ovpn"
```

where:

- `C:\Program Files\OpenVPN\bin\openvpn-gui.exe` is a path to the OpenVPN GUI executable file
- `C:\Program Files\OpenVPN\config\client.ovpn` is a path to the configuration file generated by the network hub

To establish a VPN connection, execute the script.

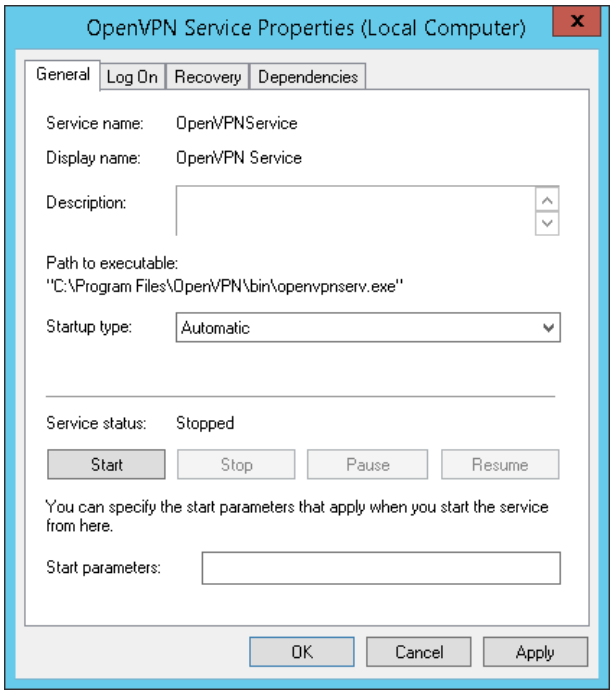
> **IMPORTANT!**
>
> The OpenVPN command must be run with the *'Run as Administrator'* privileges. If you have created a batch file, you must use the Run as administrator command to execute the file.

Configuring openVPN Service to Start Automatically

You can configure the openVPN service to start automatically so that it runs on Microsoft Windows startup. To do this:

1. In the Microsoft Windows **Start** menu, click in the **Start Search** box, type `services.msc` and press **[ENTER]**.
2. In the details pane, right-click the openVPN service and select **Properties**.
3. On the **General** tab, in the **Startup type** list, select *Automatic*.

For more information, see the Running OpenVPN as a Windows Service section at https://openvpn.net/index.php/open-source/documentation/install.html?start=1.



Accessing Veeam PN Portal

Veeam PN offers two types of web-based portals:

- **Network hub portal** is an administrative console on the network hub. The network hub portal is intended for Veeam PN Administrators managing the VPN organized with the help of Veeam PN. Veeam PN Administrators can use the portal to register and manage clients, configure general application settings, set up alerts, monitor network activities and so on.
- **Site gateway portal** is an administrative console on a site gateway appliance. Administrators of networks in which site gateways are deployed can use the gateway portals to configure local network settings, set up alerts, monitor network activities and so on.

Veeam PN portals are deployed when you set up the network hub and site gateways. Veeam PN portals are accessible over HTTPS. You can use any supported web browser to work with portals remotely.

> **NOTE:**
>
> Veeam PN does not provide a portal for managing standalone computers (point-to-site scenario). Standalone computer settings are configured directly on these computers. For more information, see Configuring Standalone Computers.

Accessing Network Hub Portal

To access the network hub portal:

1. In the address bar of a web browser, enter the address of the network hub portal:

   - [For Microsoft Azure deployment] `https://<networkhub>/`

     where `<networkhub>` is the public IP address or full DNS name of the Microsoft Azure appliance hosting the network hub, for example: `https://veeampn.northeurope.cloudapp.azure.com`.

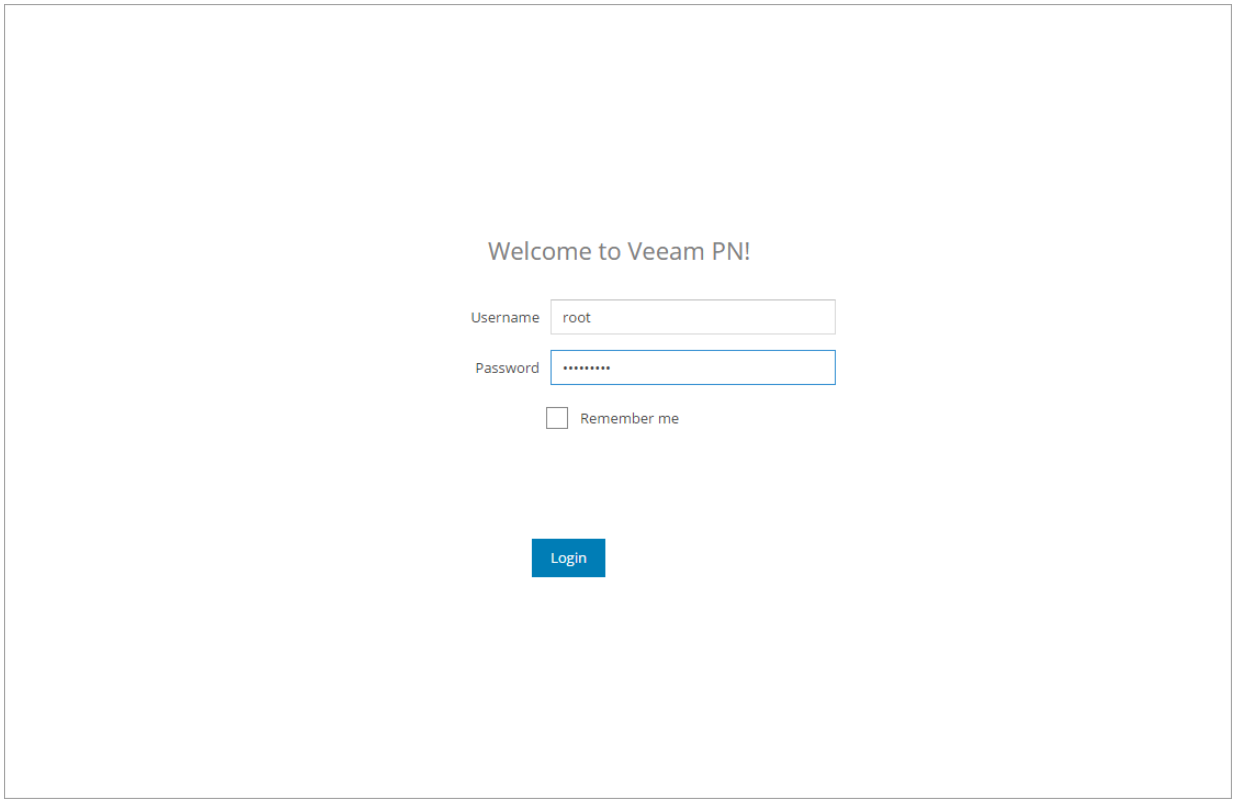
   - [For on-premises deployment] `https://<networkhub>:443/`

     where `<networkhub>` is the public IP address or full DNS name of the network hub appliance and 443 is the default port for communication with the network hub portal, for example: `https://172.17.53.12:443`.

2. In the **Username** and **Password** fields, specify credentials of a user account with Portal Administrator permissions.

3. Select the **Remember me** check box. If you enable this option, you will not have to re-log in to the portal (unless you perform manual logout). If you do not enable this option, you will have to re-log in to the portal if the work session remains idle for 10 minutes.

4. Click **Login**.



Accessing Site Gateway Portal

To access the site gateway portal:

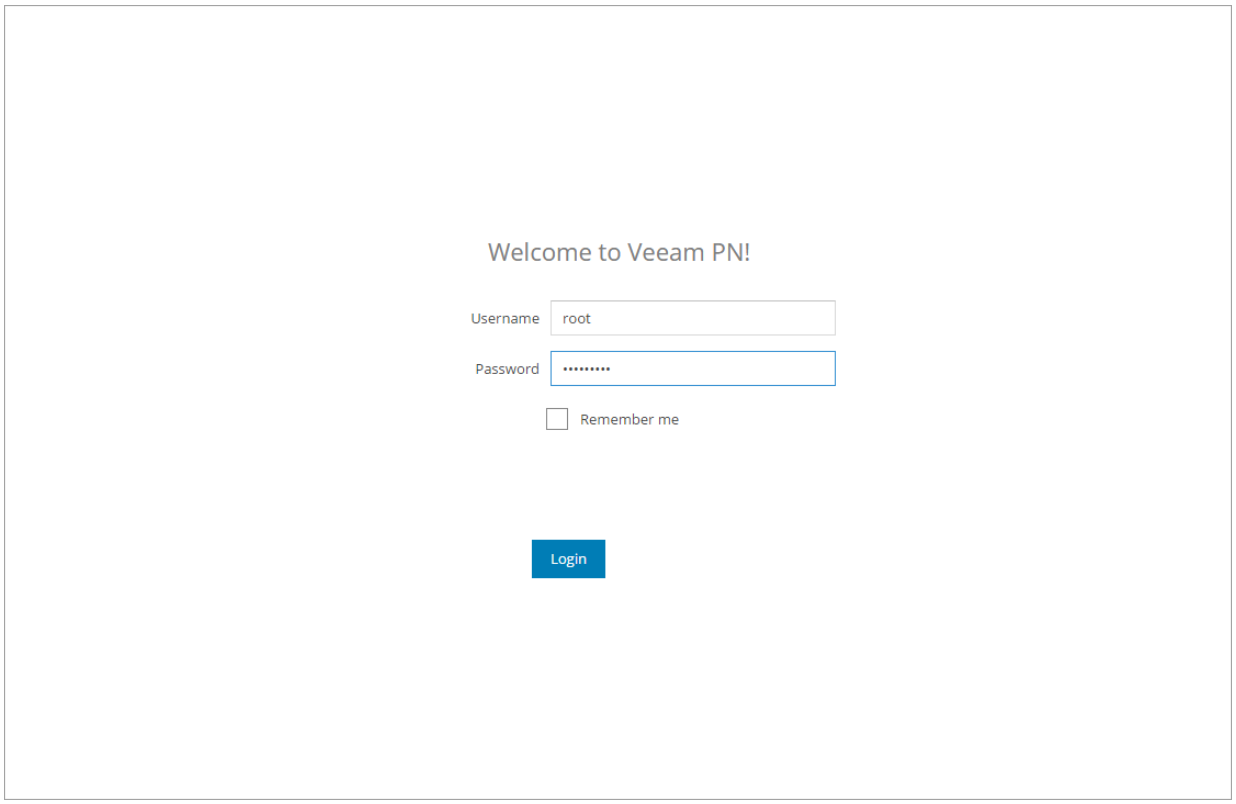
1. In the address bar of a web browser, enter the address of the site gateway portal: `https://<sitegateway>:443/`,

   where `<sitegateway>` is the public IP address or full DNS name of the site gateway appliance and `443` is the default port for communication with the site gateway portal, for example: `https://172.17.53.110:443`.

2. In the **Username** and **Password** fields, specify credentials of a user account with Portal Administrator permissions.

3. Select the **Remember me** check box. If you enable this option, you will not have to re-log in to the portal (unless you perform manual logout). If you do not enable this option, you will have to re-log in to the portal if the work session remains idle for 10 minutes.

4. Click **Login**.



Configuring Alerts

To help you track important events and notify you about operational problems, Veeam PN uses alerts. Alerts are generated when a specific condition occurs, for example, the CPU usage is high, and you need take some action to resolve it. Alerts can also be generated if some state changes, and you need to be aware of it.

Veeam PN comes with the following predefined alerts:

Alert name	Description
Client disconnected	The client has disconnected from the VPN.
Client connected	The client has connected to the VPN.
High CPU utilization	The level of CPU utilization on the server is above normal.
Fatal VPN failure	The Veeam PN daemon has failed.
VeeamPN update available	A newer version of Veeam PN is available.

You can configure alerts in the network hub and site gateway portals.

Response Actions

If you want to perform some operation in response to alerts, you can set up alert response actions. The response action is performed when a new alert of a specific type is generated. For example, you can instruct Veeam PN to send an email to a group of administrators if the level of CPU utilization is high.

For response actions, Veeam PN uses scripts of the SH format. You can use predefined scripts or create custom scripts for response actions. By default, Veeam PN comes with the following predefined scripts:

- `send_email.sh` — this script lets you send an email notification at the specified email address. To send email notifications, you must configure SMTP server settings. For more information, see Configuring SMTP Settings.
- `sample_script.sh` — this script lets you display information about a generated alert in the shell on the network hub or site gateway.

To manage alerts and response actions, you can perform the following tasks:

- Set response actions for alerts
- Create response actions
- Edit response actions
- Remove response actions

Configuring SMTP Settings

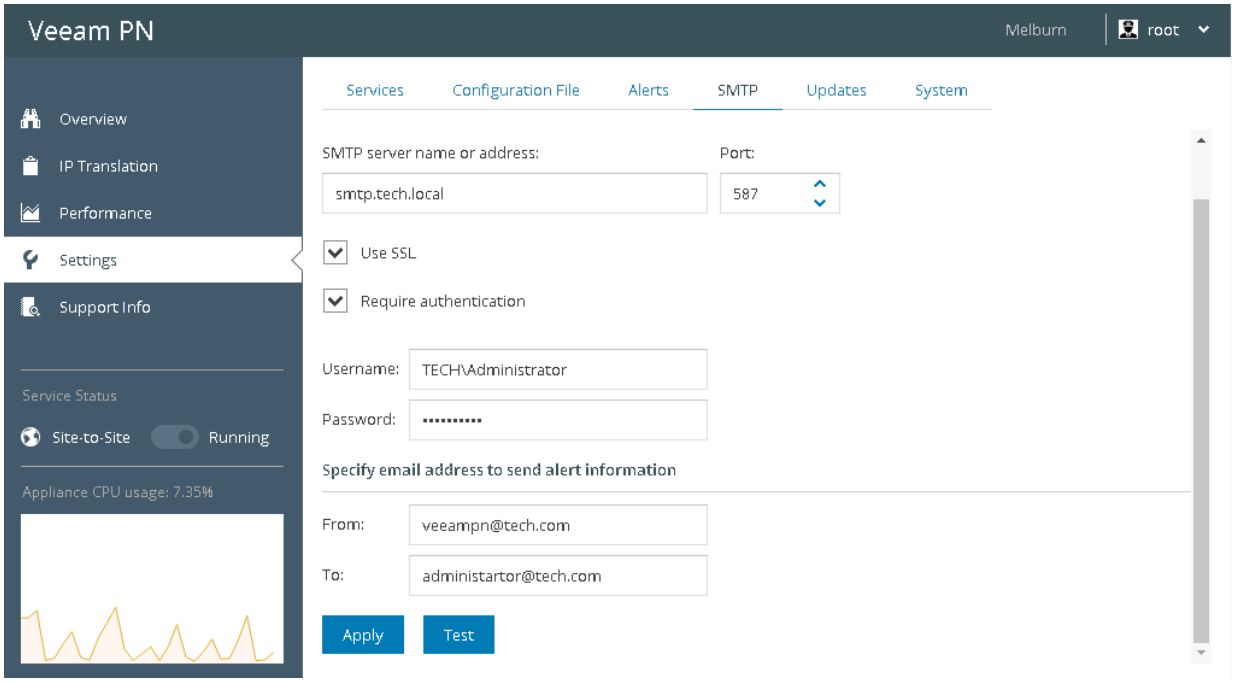
If you want to send notifications about generated alerts by email, you must configure SMTP server settings in the network hub or site gateway portal.

To configure SMTP server settings:

1. Log in to the Veeam PN portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. Click the **SMTP** tab.
4. In the **SMTP server name or address** field, specify a DNS name or IP address of the SMTP server.
5. If required, in the **Port** field change the SMTP communication port. By default, Veeam PN uses port 587 for communication with the SMTP server.
6. If you want to enable data encryption for the SMTP server with SSL support, select the **Use SSL** check box.
7. If the SMTP server requires authentication, select the **Require authentication** check box. In the **Username** and **Password** fields, specify the authentication credentials.
8. In the **From** field, specify an email address from which email notifications must be sent.
9. In the **To** field, specify an email address at which email notifications must be sent. To specify several email addresses, use semicolon.
10. Click **Apply**.

TIP:

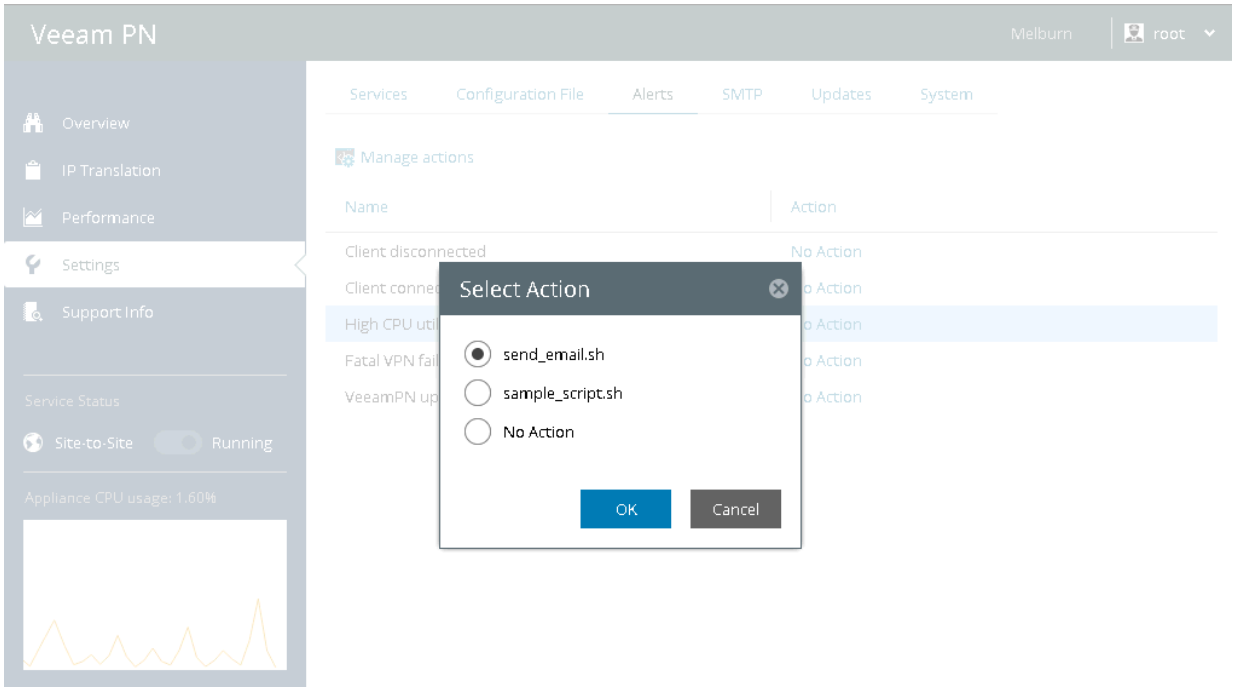
To verify if you have configured SMTP server settings correctly, click **Test**. Veeam PN will send a test email at the specified email address(es).



Setting Response Actions for Alerts

By default, alerts in Veeam PN are not associated with any response actions. To set a response action for an alert:

1. Log in to the Veeam PN portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. Click the **Alerts** tab.
4. In the **Action** column for the necessary alert, click **No Action**.
5. In the **Select Action** window, choose a script that Veeam PN must execute when the alert is generated. The list of scripts contains scripts that are currently used for response actions. If necessary, you can create custom scripts. For more information, see Creating Response Actions.



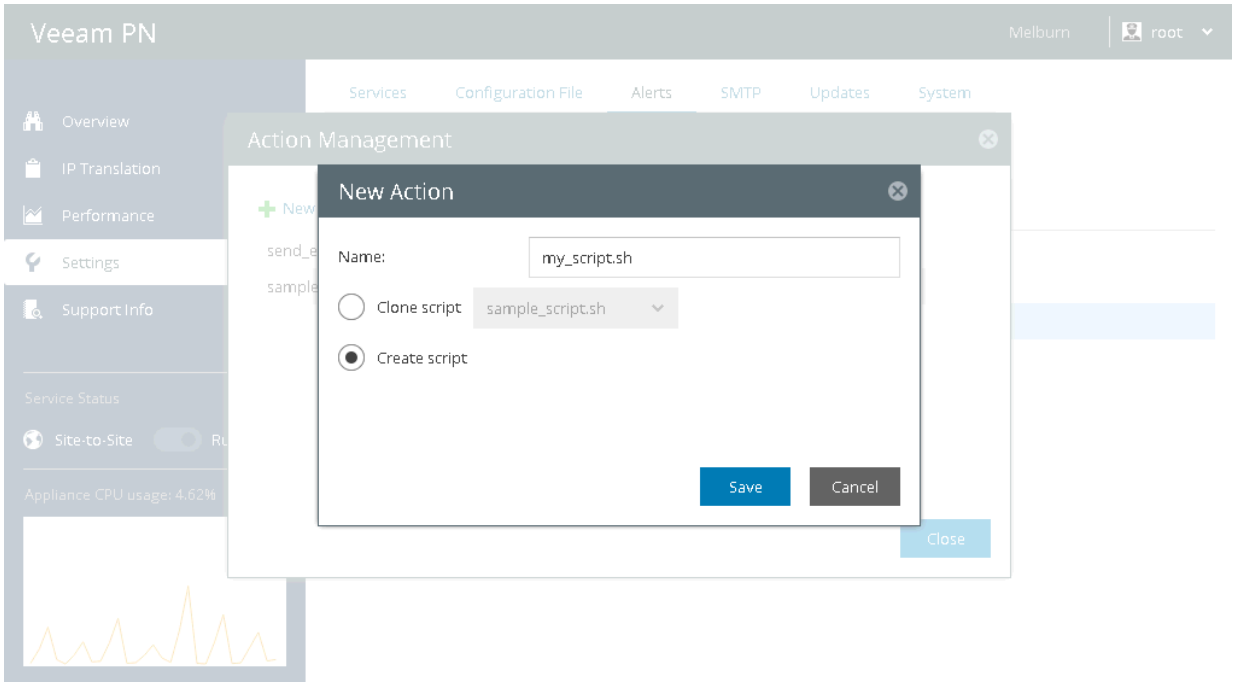
Creating Response Actions

You can create new response actions, for example, if you want to execute a custom script when some alert is generated.

To create a new response action:

1. Log in to the Veeam PN portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. Click the **Alerts** tab.
4. At the top of the alerts list, click **Manage actions**.
5. In the **Action Management** window, click **New**.
6. In the **New Action** window, specify settings for the new response action:
   a. In the **Name** field, specify a name for the new script, for example, `my_script.sh`.
   b. To create a new script on the basis of an existing one, select **Clone script** and choose an existing script from the list on the right. To create a new empty script file, select **Create script**. You can then edit the created script in Veeam PN. For more information, see Editing Response Actions.
7. Click **Save**, then click **Close**.

> **NOTE:**
>
> Veeam PN uses the bash interpreter to execute scripts for response actions. For this reason, scripts must always start with the following heading line:
> `#!/bin/bash`



Editing Response Actions

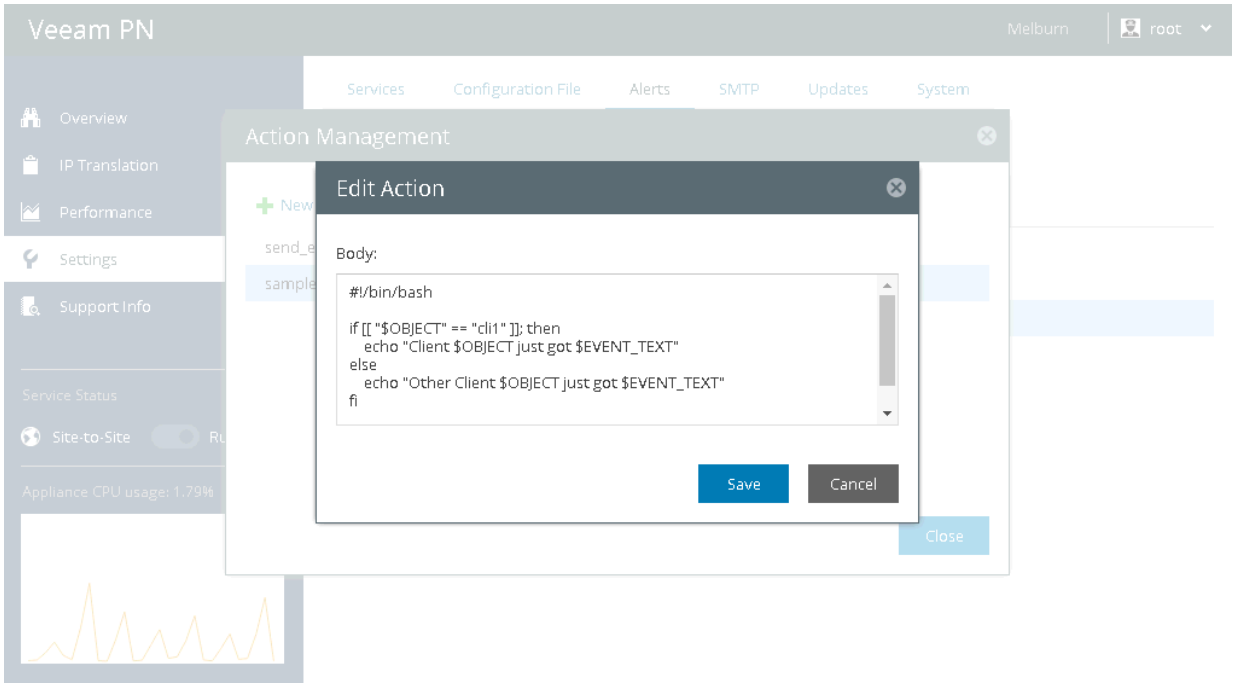
You can edit response actions, for example, if you need to change some parameters in the script. You can also use the edit functionality to add content to scripts newly created in Veeam PN.

To edit a response action:

1. Log in to the Veeam PN portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. Click the **Alerts** tab.
4. At the top of the alerts list, click **Manage actions**.
5. In the **Action Management** window, select an existing script and click **Edit**.
6. In the **Edit Action** window, edit the script content as required.
7. Click **Save**, then click **Close**.

To rename a response action, in the **Action Management** window click **Rename** and enter a new name for the response action.

> **NOTE:**
>
> Veeam PN uses the bash interpreter to run scripts for response actions. For this reason, scripts must always start with the following heading line:
> `#!/bin/bash`

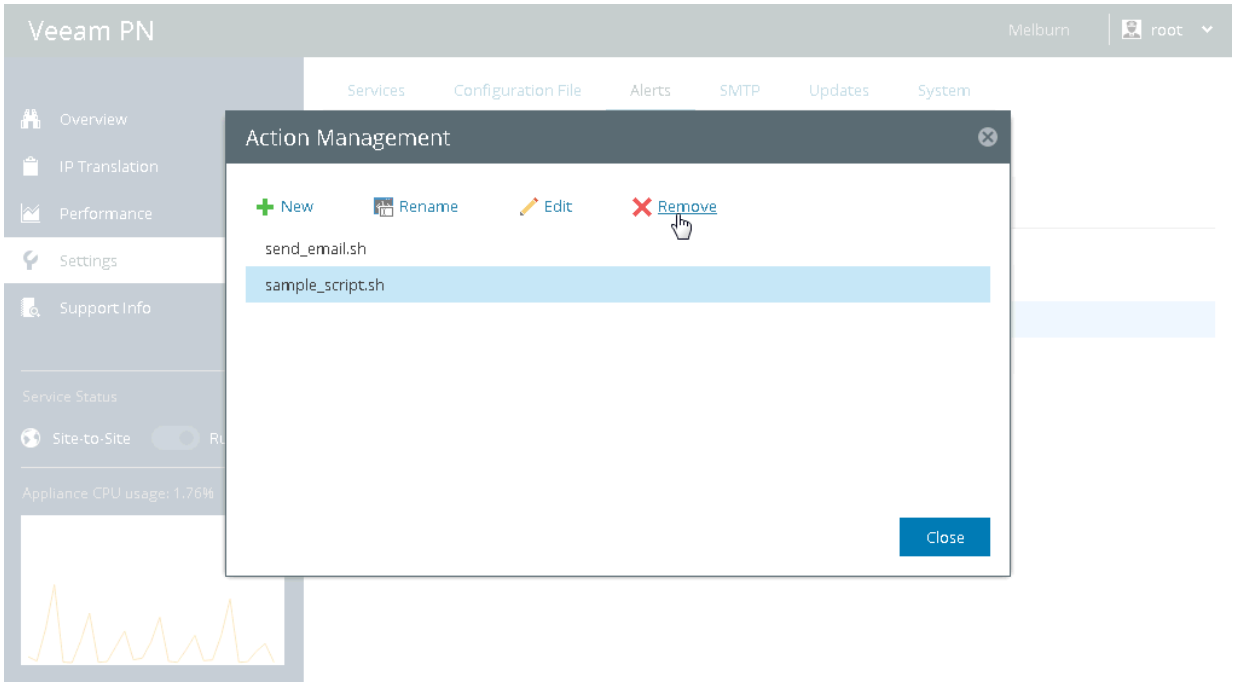


Removing Response Actions

You can remove response actions that you do not plan to use.

To remove a response action:

1. Log in to the Veeam PN portal as a Portal Administrator.
2. In the configuration menu on the left, click **Settings**.
3. Click the **Alerts** tab.
4. At the top of the alerts list, click **Manage actions**.
5. In the **Action Management** window, select the response action and click **Remove**.
6. Click **Close**.



Monitoring Clients

You can monitor the state of clients connected to the VPN, get information about the amount of sent and received traffic and so on. Veeam PN provides the following monitoring views:

- **Veeam PN Overview** lets you get an at-a-glance view of the VPN infrastructure and clients.
- The **Performance** view lets you get granular information on specific clients and view specific network metrics.

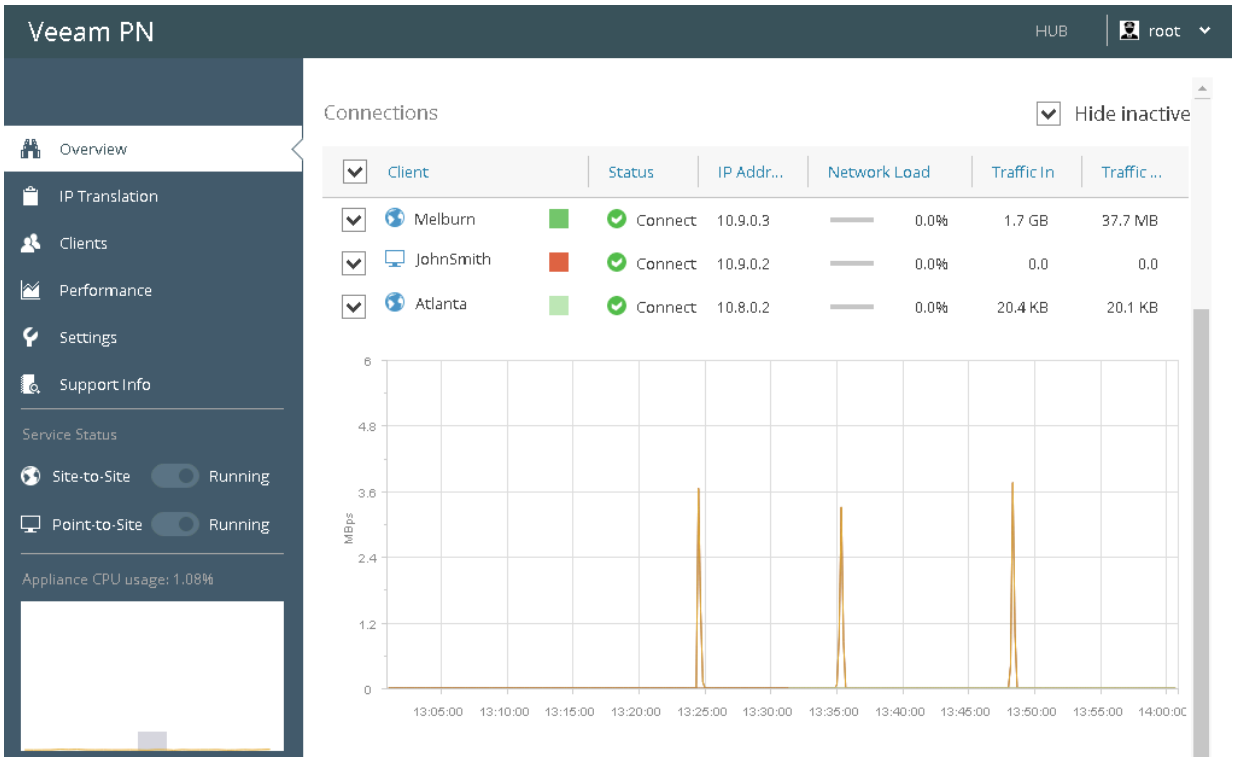
Monitoring views are available in the network hub and site gateway portals. The network hub portal provides monitoring data for all Veeam PN clients. The site gateway portal lets you monitor the state of the on-premises network where the site gateway resides.

Veeam PN Overview

Veeam PN Overview is displayed when you access the Veeam PN portal. You can use this view to monitor the state of clients, network load, incoming and outgoing traffic and get information about events that have occurred in the VPN.

By default, Veeam PN displays information for all Veeam PN clients. If necessary, you can display information about specific clients or clients that are currently connected to the network hub:

- To display information about specific clients, select check boxes next to them in the clients list.
- To display information about currently connected clients, select the **Hide inactive** check box on the right of the clients list.



Performance View

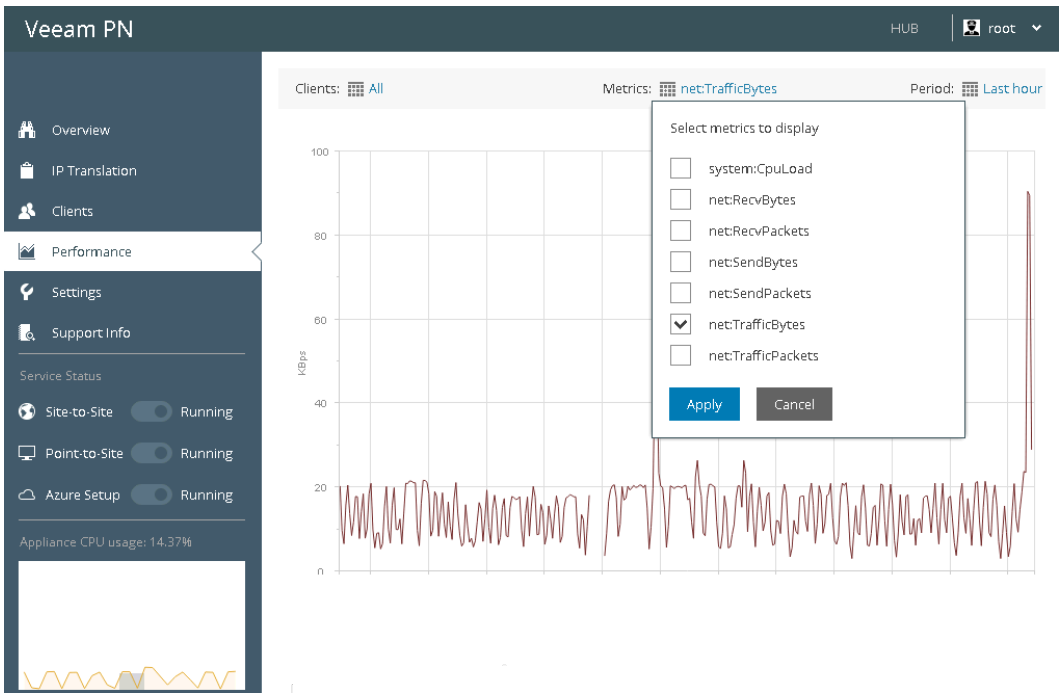
You can use the **Performance** view to get information about specific network metrics granularly for one or more Veeam PN clients.

To display the **Performance** view:

1. Log in to the Veeam PN portal.
2. In the configuration menu on the left, click **Performance**.
3. At the top of the chart, click the link next to the **Clients** field and select check boxes next to clients whose data you want to display in the chart.
4. At the top of the chart, click the link next to the **Metrics** field and select one or more network metrics that you want to display in the chart. Veeam PN tracks the following metrics:
   - *Received bytes* — amount of data (in bytes) received from the client through the VPN tunnel.
   - *Received packets* — number of packets received from the client through the VPN tunnel.
   - *Sent bytes* — amount of data (in bytes) sent to the client through the VPN tunnel.
   - *Sent packets* — number of packets sent to the client through the VPN tunnel.
   - *Traffic bytes* — total amount of traffic (in bytes) sent and received by the client through the VPN tunnel.
   - *Traffic packets* — total number of packets sent and received by the client through the VPN tunnel.

> **NOTE:**
>
> If you have chosen to chart network data for several clients, you will be able to select one network metric only.

5. At the top of the chart, click the link next to the **Period** field and select a period for which you want to chart network data: *Last hour*, *Last 6 hours*, *Last 24 hours*, *Last week* or *Last month*.



Configuring IP Translation Rules

When you migrate a machine to another site or restore/migrate a machine to Microsoft Azure or Amazon AWS, it gets a new IP address. If other machines and services communicate with this machine, you typically need to update connection settings for these machines and services so that they can work with the restored machine as before. To reduce administration overhead, you can create an IP translation rule for the restored machine.

An IP translation rule maps the IP address of the original machine to the IP address of the machine restored to Microsoft Azure or Amazon AWS. For example, a machine in a local network had an IP address 192.168.0.35, and the restored machine has an IP address 10.12.5.214. You can create an IP translation rule that will map the IP address 192.168.0.35 to the IP address 10.12.5.214. When machines in the local network need to communicate with the machine that had an IP address 192.168.0.35, Veeam PN will look up the IP translation rule record and forward the request to the machine that has the IP address 10.2.5.214 in Microsoft Azure/Amazon AWS.

IP translation rules can be configured in the network hub and site gateway portals. You can perform the following operations with IP translation rules:

- Create IP translation rules
- Modify IP translation rules
- Disable and enable IP translation rules
- Remove IP translation rules

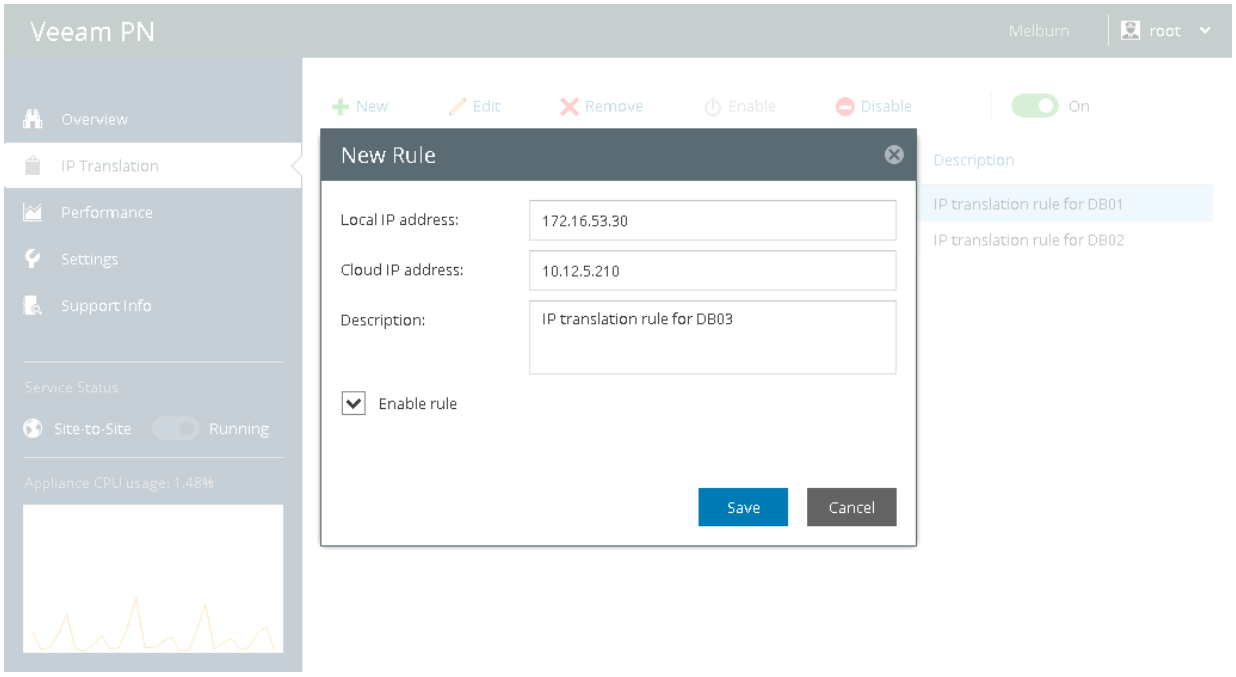
IMPORTANT!

By default, the IP translation rules functionality is disabled. To enable it, open the **IP Translation Rules** view; at the top right corner of the view set the toggle in the **Service State** field to the **On** position.

Creating IP Translation Rules

To create a new IP translation rule:

1. Log in to the Veeam PN portal.
2. In the configuration menu on the left, click **IP Translation**.
3. At the top of the IP translation rules list, click **New**.
4. In the **Local IP address** field, enter an IP address of the original machine.
5. In the **Cloud IP address** field, enter an IP address of the machine restored in Microsoft Azure.
6. In the **Description** field, provide a description for the IP translation rule.
7. Select the **Enable rule** check box to enable the created rule.
8. Click **Save**.

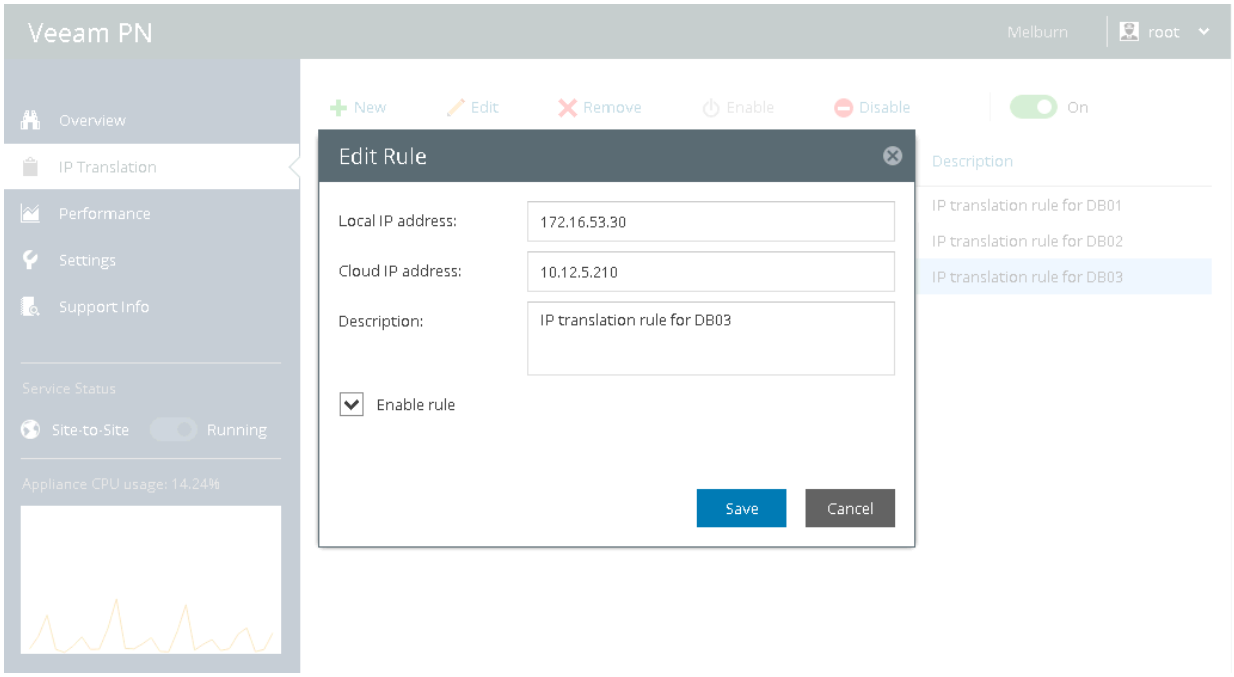


Modifying IP Translation Rules

You can modify settings of IP translation rules, for example, if the IP address of the machine restored to Microsoft Azure or Amazon AWS has changed.

To modify an IP translation rule:

1. Log in to the Veeam PN portal.
2. In the configuration menu on the left, click **IP Translation**.
3. In the IP translation rules list, select the rule.
4. At the top of the IP translation rules list, click **Edit** and modify the rule settings as required.



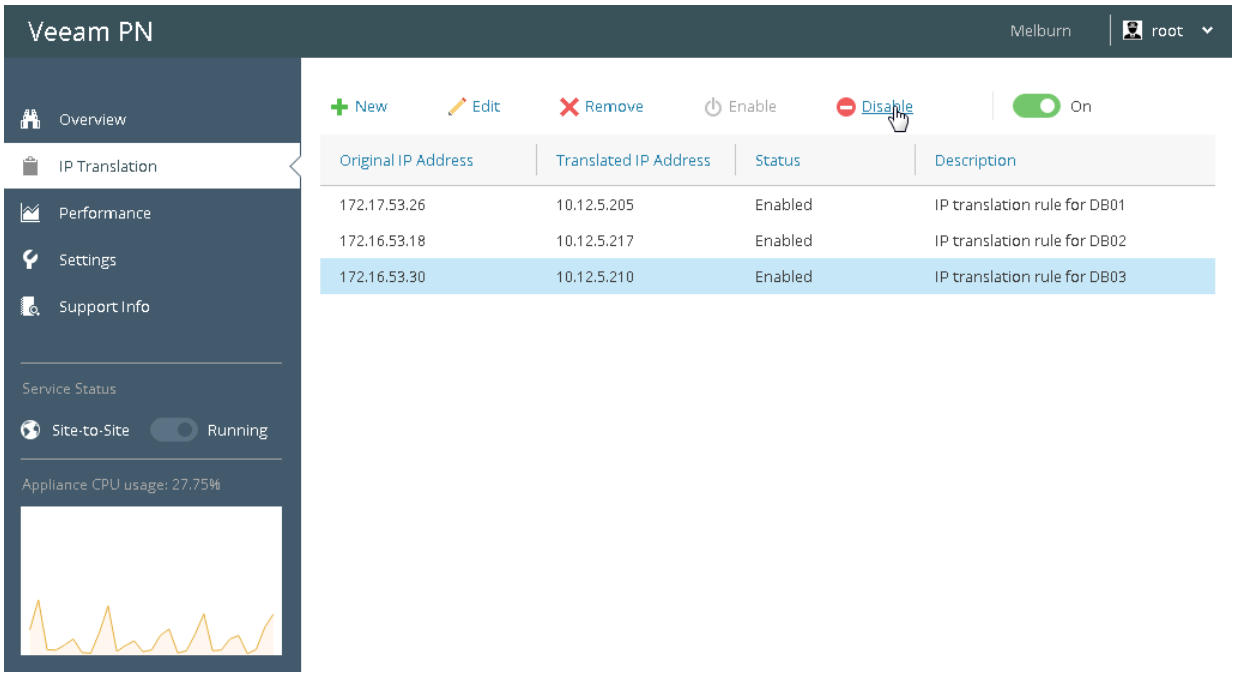
Disabling and Enabling IP Translation Rules

In some cases, you may need to put an IP translation rule 'on hold' for some time. In such situation, you do not necessarily need to delete the IP translation rule and recreate it again later. Instead, you can disable the IP translation rule.

To disable an IP translation rule:

1. Log in to the Veeam PN portal.
2. In the configuration menu on the left, click **IP Translation**.
3. In the IP translation rules list, select the rule.
4. At the top of the IP translation rules list, click **Disable**.

To enable a previously disabled IP translation rule, select it in the list and click **Enable**.

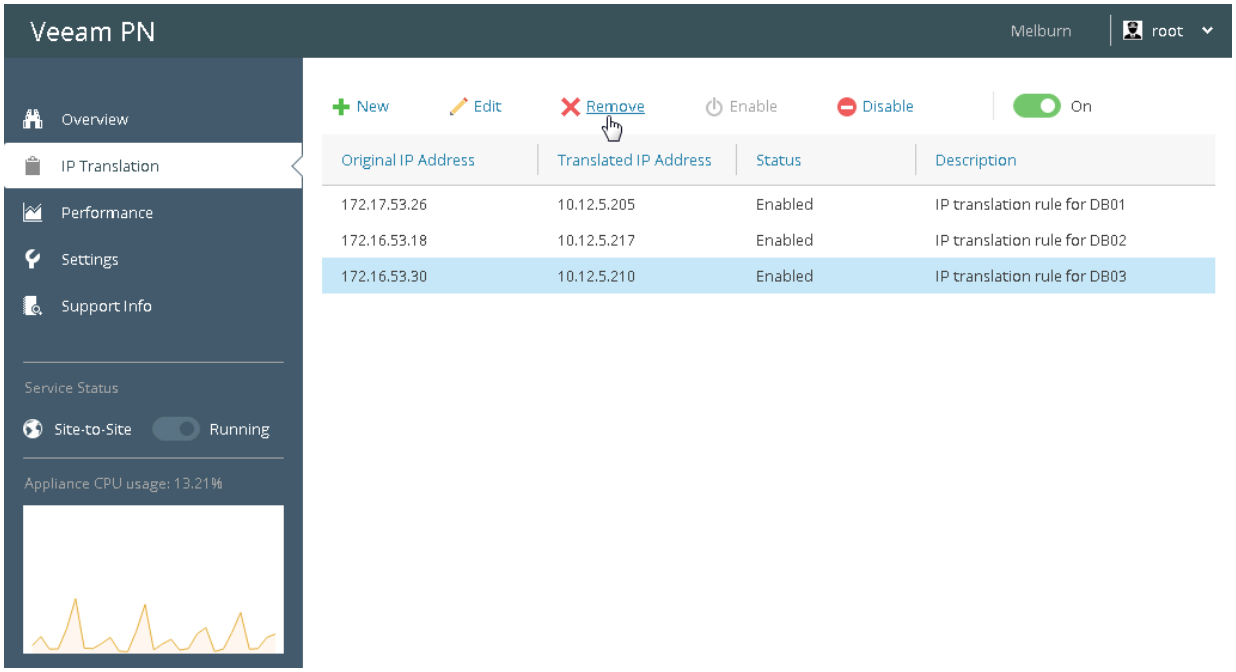


Removing IP Translation Rules

You can remove an IP translation rule, for example, if you no longer need to access a machine restored to Microsoft Azure or Amazon AWS.

To remove an IP translation rule:

1. Log in to the Veeam PN portal.
2. In the configuration menu on the left, click **IP Translation**.
3. In the IP translation rules list, select the rule.
4. At the top of the IP translation rules list, click **Remove**.



Viewing and Exporting Logs

You can view information about Veeam PN events in the network hub and site gateway portals, or export it for troubleshooting purposes.

To view information about Veeam PN events:

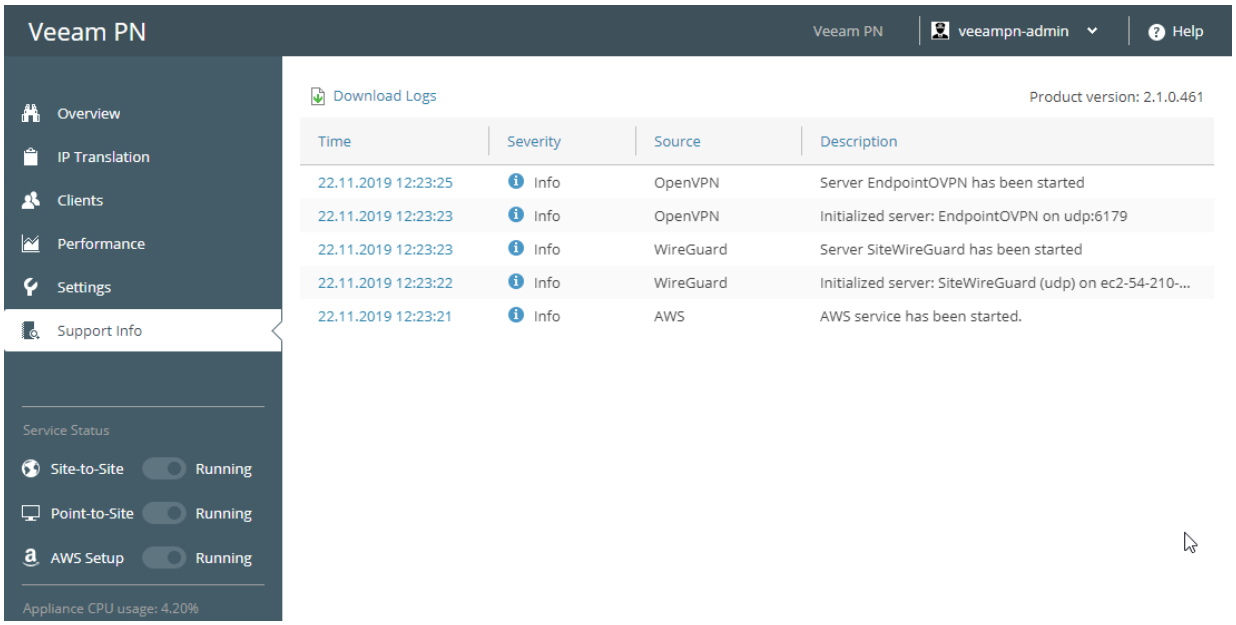
1. Log in to the Veeam PN portal.
2. In the configuration menu on the left, click **Support Info**.

Veeam PN stores event information to log files. The size of a log file cannot exceed the size of 2 MB. When the file size reaches the limit, Veeam PN creates a new log file. The maximum number of log files that can exist at the same time is 10. As soon as the number of files exceeds 10, Veeam PN automatically deletes the earliest log file from disk.

To export Veeam PN log files:

1. Log in to the Veeam PN portal.
2. In the configuration menu on the left, click **Support Info**.
3. At the top of the events list, click **Download Logs**. Veeam PN will generate a ZIP archive with log files and download it to the default downloads folder.

> **NOTE:**
>
> When you download a ZIP archive with log files, Veeam PN does not remove this archive from disk. The archive remains on disk until you generate a new ZIP archive with log files.



Performing Configuration Backup and Restore

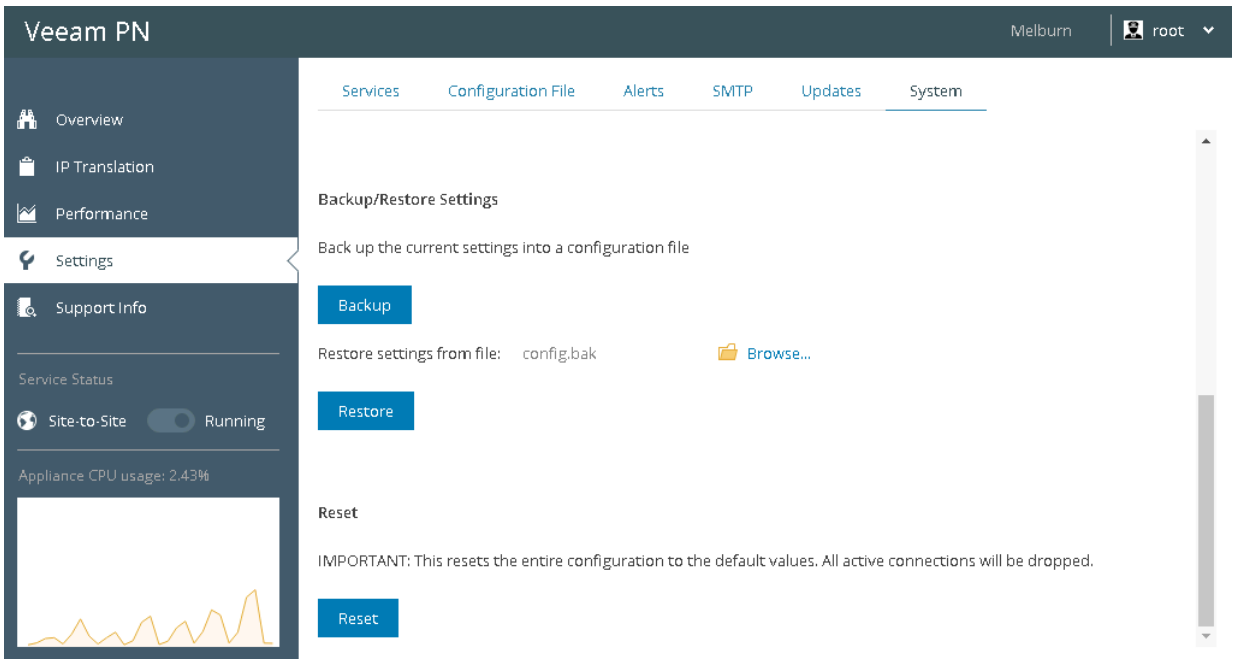
With Veeam PN, you can back up and restore configuration of Veeam PN appliances: the network hub and site gateways.

When you perform configuration backup, Veeam PN creates a file of the BAK format that contains all configuration settings you have configured for the Veeam PN appliance. You can create a configuration backup manually to capture the Veeam PN appliance state at a specific point in time. Whenever you need to roll back the Veeam PN appliance to that specific point in time, you can restore its configuration from the configuration backup file.

> **IMPORTANT!**
>
> Mind the following limitations:
>
> - When you restore from the configuration backup of Veeam PN 2.0 to Veeam PN 2.1, the **Alerts** and **SMTP** settings change to default values.
> - **Azure network hub**: You cannot restore from the configuration backup of Veeam PN 2.0 to Veeam PN 2.1.

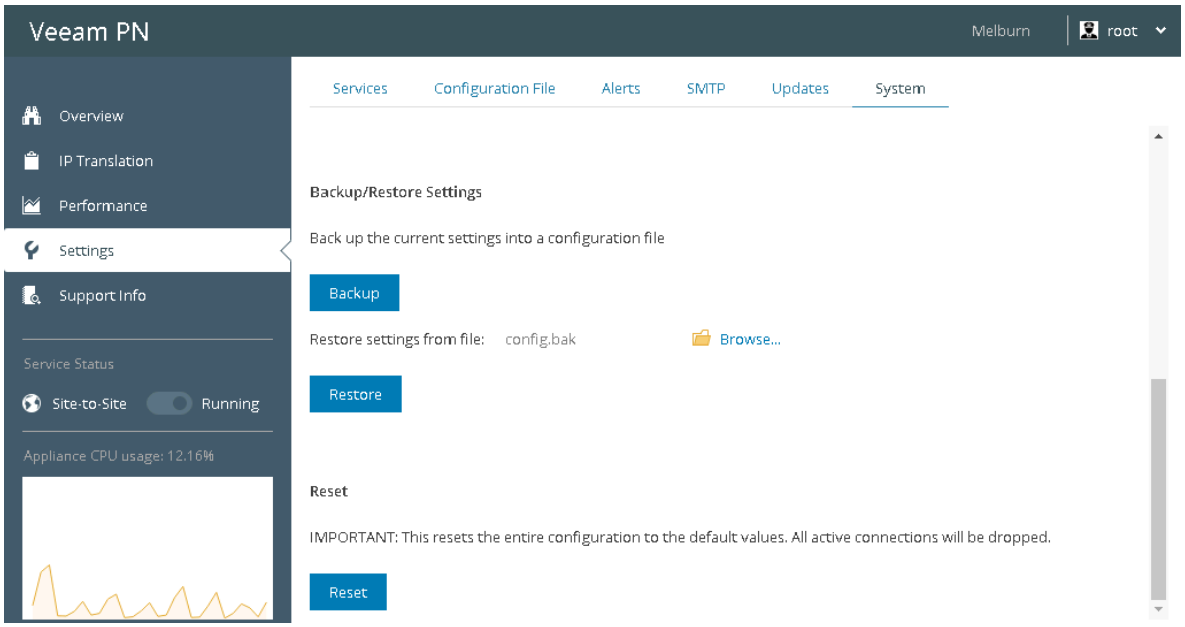
To create a configuration backup:

1. Log in to the Veeam PN portal.
2. In the configuration menu on the left, click **Settings**.
3. Click the **System** tab.
4. In the **Backup/Restore Settings** section, click **Backup**. Veeam PN will save all configured settings for the Veeam PN appliance to the config.back file and download this file to the default download location on your machine.



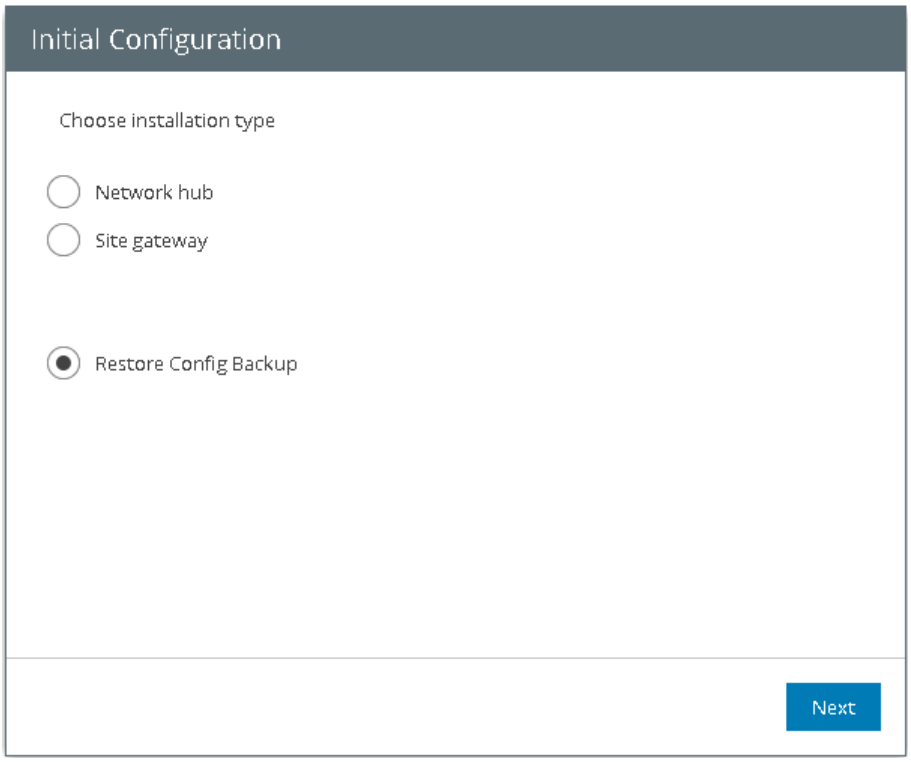
To restore a configuration backup:

1. Log in to the Veeam PN portal.
2. In the configuration menu on the left, click **Settings**.
3. Click the **System** tab.
4. In the **Backup/Restore Settings** section, click **Browse** and select a configuration backup file from which you want to restore Veeam PN settings.
5. Click **Restore**.

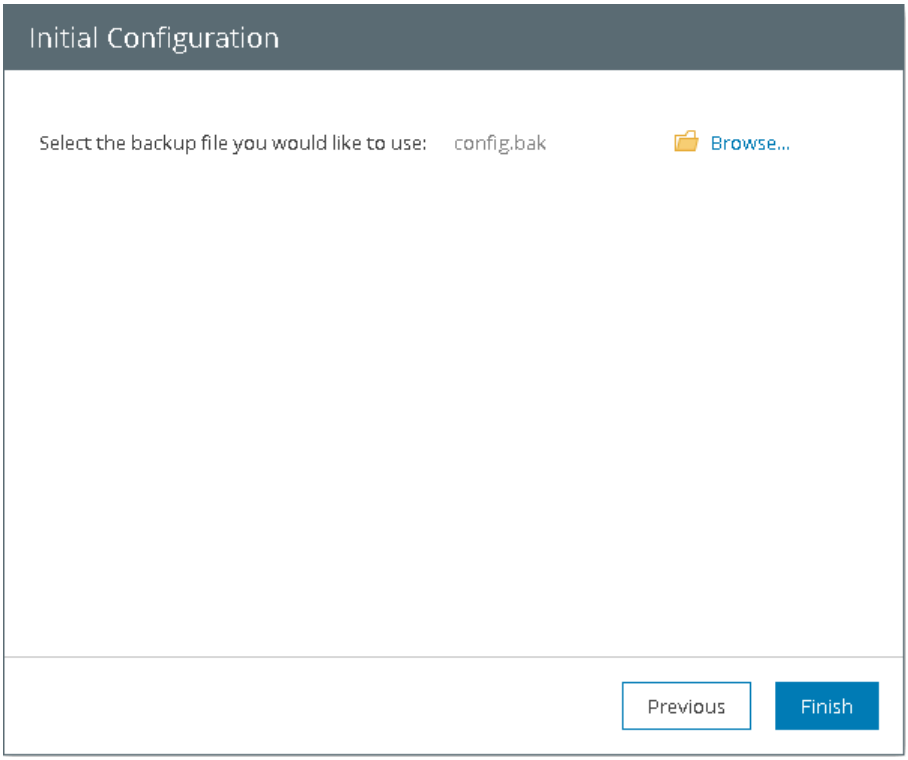


You can also use the configuration backup file to configure settings of a newly deployed Veeam PN appliance:

1. At the first step of the **Initial Configuration** wizard, select **Restore Config** and click **Next**.



2. Click **Browse** and select a configuration backup file from which you want to restore Veeam PN settings.
3. Click **Finish** to apply configuration settings to the newly deployed appliance.

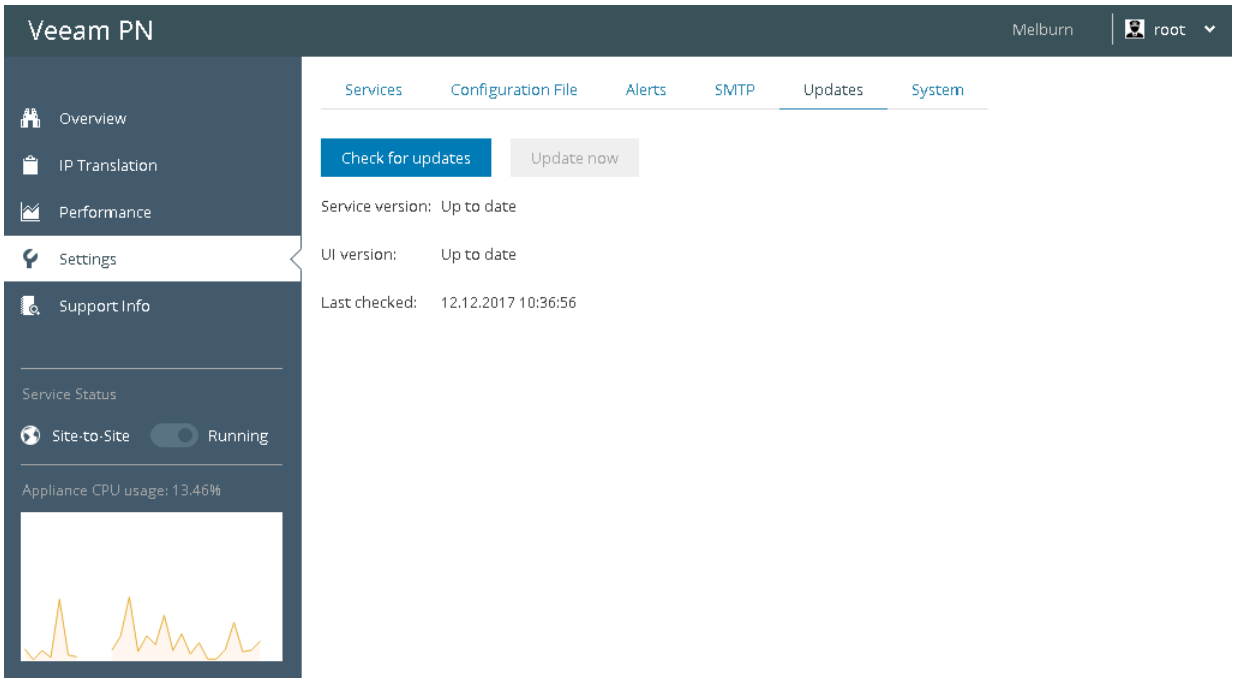


Checking for Updates

You can check for product updates and download a newer version of Veeam PN using the Veeam PN portal.

To check for product updates:

1. Log in to the Veeam PN portal.
2. In the configuration menu on the left, click **Settings**.
3. Click the **Updates** tab.
4. Click **Check for updates**. If a newer version of the product is available, Veeam PN will inform you about it. You can use the **Update now** button to download the newer product version to your machine and update the product.



How-Tos

You can use Veeam PN to implement the following scenarios:

- Set Up VPN Between Microsoft Azure Site and Local Sites
- Set Up VPN from Endpoints to Microsoft Azure
- Set Up VPN Between Remote Sites
- Set Up VPN from Endpoints to Local Site

Additional guides for Veeam PN deployment and optimization:

- Install Veeam PN on Ubuntu
- Install Veeam PN with Script
- Install Free SSL Certificate on Veeam PN Appliance Host
- Optimize Queue Length in Linux Kernel

Set Up VPN Between Microsoft Azure and Local Sites

You can use Veeam PN to set up a VPN connection between private clouds in Microsoft Azure and local company sites. This scenario can be helpful if you have moved some of your application and services to Microsoft Azure. In this case, you can join Microsoft Azure networks with local company networks over the VPN and enable secure communication between remote sites.

Reference Environment

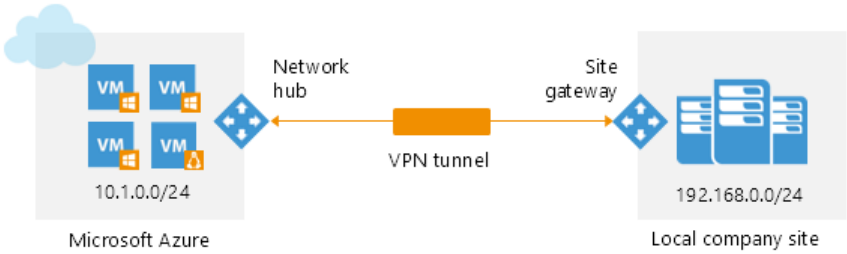
This how-to assumes that your company environment is distributed between two sites:

- Microsoft Azure: part of your applications and services are hosted in Microsoft Azure.
- Local company site: part of your applications and services are hosted on a local company site.

In this scenario, you will deploy Veeam PN components in the following way:

- Network hub will be hosted in Microsoft Azure.
- Site gateway will be hosted on the local company site.

The network hub and site gateway will produce the two terminal points of a VPN tunnel. Application and services in Microsoft Azure and on the local company site will be able to securely communicate over the VPN tunnel. Users on the local company site will be able to get access to company resources in Microsoft Azure.



Prerequisites

To follow instructions of this how-to, check the following prerequisites:

- You must have a user account in Microsoft Azure.
- You must use the Azure Resource Manager model to configure the network hub in Microsoft Azure. The classic deployment model is not supported.
- You must have a VMware vSphere host on the local company site. A site gateway is deployed as a virtual appliance and placed on the VMware vSphere host.

Step-By-Step Walkthrough

To set up a VPN connection between a private cloud in Microsoft Azure and a local company site, you will:

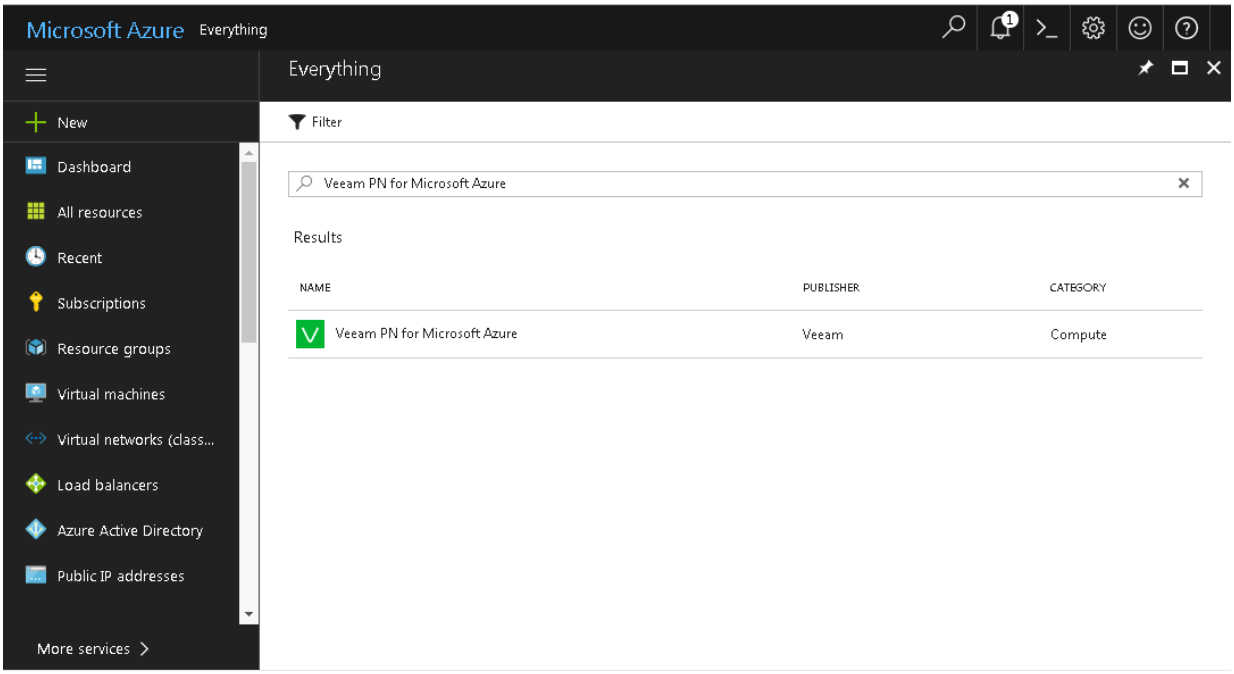
1. Deploy the network hub in Microsoft Azure.
2. Register a client for the local site network in the Veeam PN portal.
3. Deploy a site gateway in the local site network.
4. Add Static Routes for Outgoing Traffic on Default Gateways

Step 1. Deploy Network Hub in Microsoft Azure

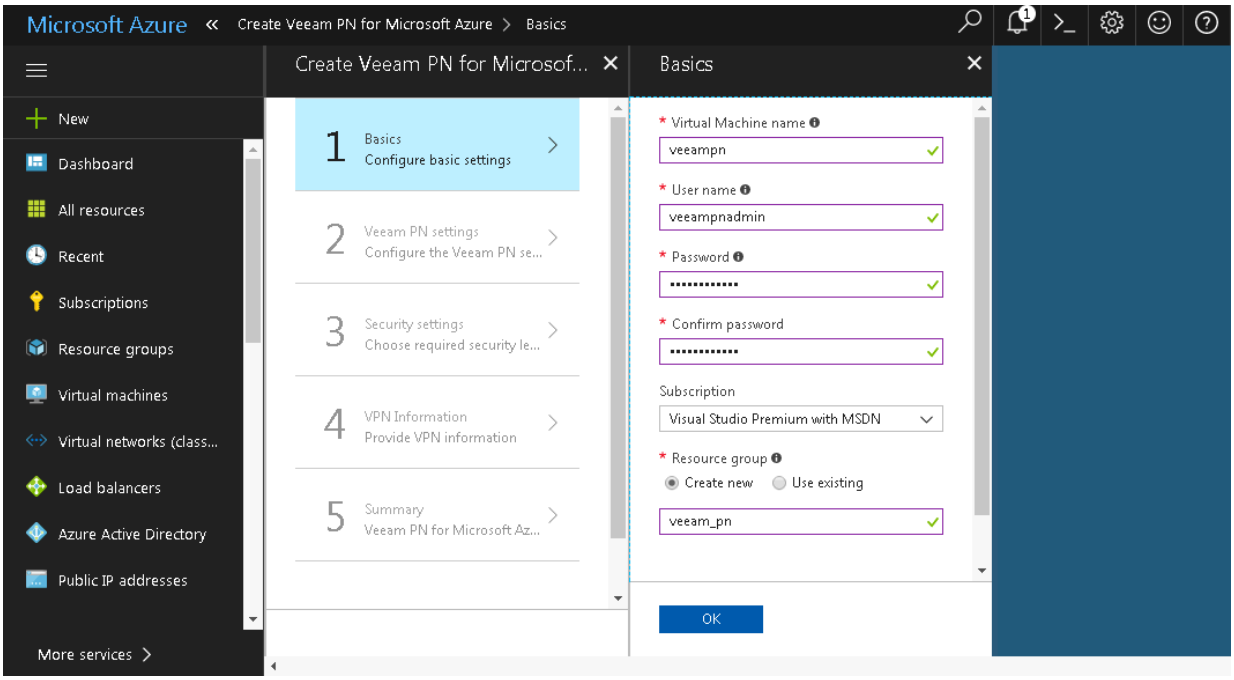
The network hub is the core of the VPN infrastructure. If you want to join a Microsoft Azure network with a local site network, you must deploy the network hub in Microsoft Azure.

To deploy the network hub:

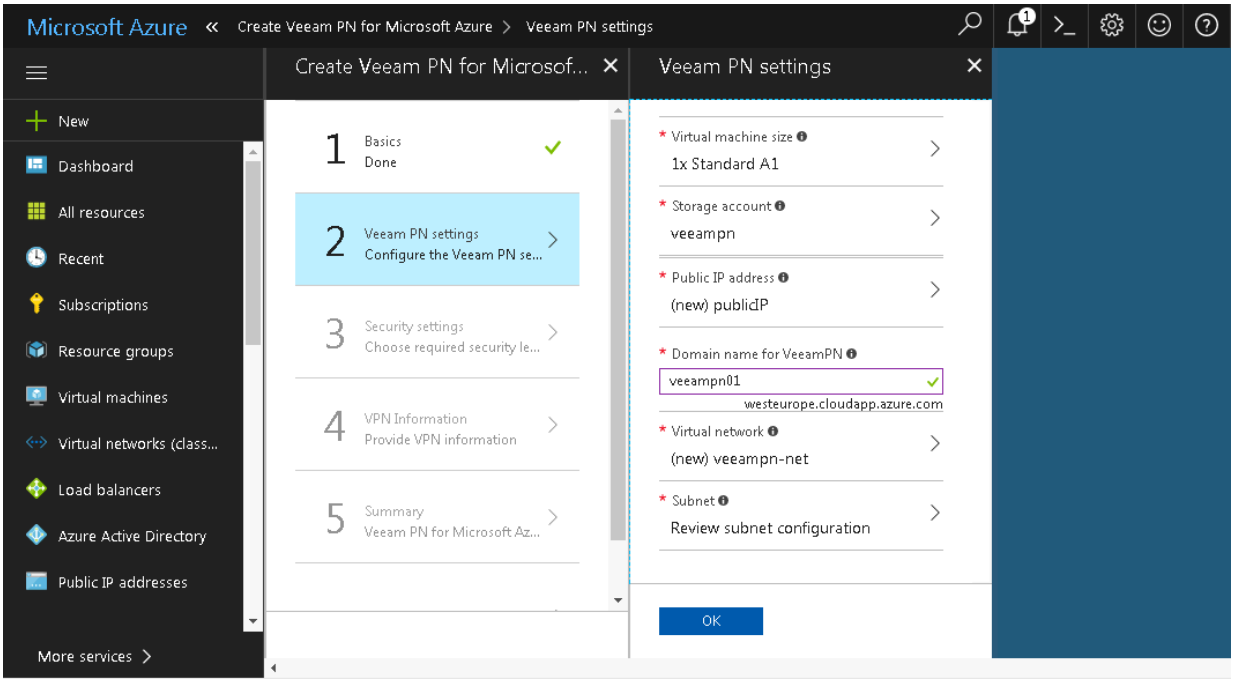
1. Sign in to the Microsoft Azure portal at https://portal.azure.com.
2. In the menu on the left, click **New**.
3. In the marketplace, search for the '*Veeam PN for Microsoft Azure*' template.
4. Select the template and click **Create**.



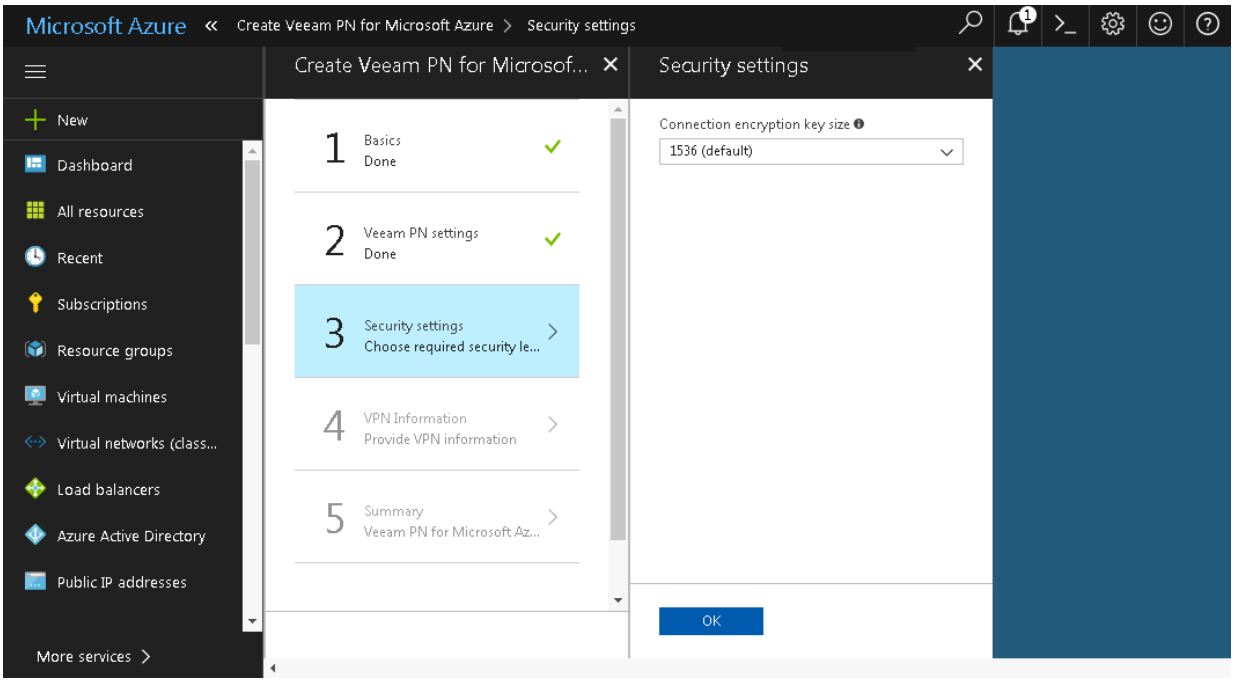
5. On the **Basics** blade, specify basic VM settings: VM name, user credentials for the network hub administrator account, subscription, resource group and location.



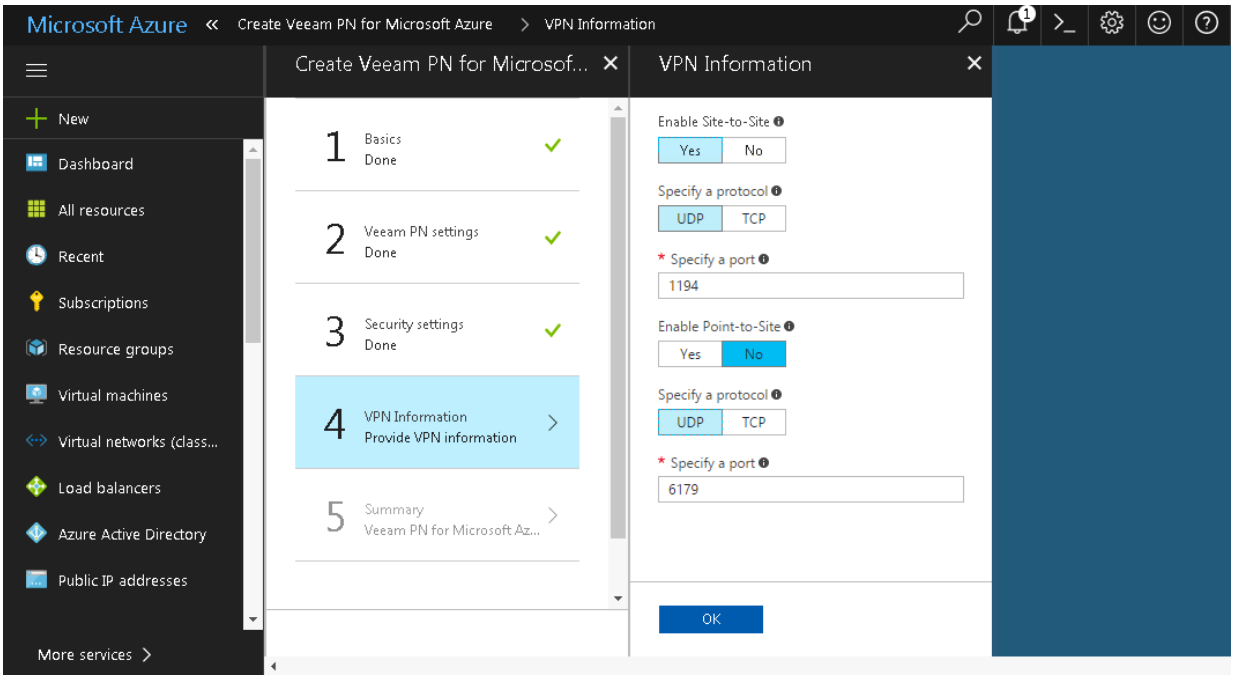
6. On the **Veeam PN settings** blade, specify basic settings for the network hub appliance: VM size (A1 size is minimum), storage account, public IP address, domain name, virtual network and subnet.



7. On the **Security settings** blade, specify parameters for the self-signed SSL certificate that Veeam PN will use to secure connection in the VPN: the certificate key length.



8. On the **VPN Information** blade, make sure that **Yes** is enabled in the **Enable Site-to-Site** field. In the **Specify a protocol** and **Specify a port** fields, leave default settings.



9. On the **Summary** blade, click **OK**.

10. On the **Buy** blade, click **Purchase**.

    Veeam PN will deploy the network hub from the Microsoft Azure template. The deployment process typically takes several minutes. Wait for this process to complete.

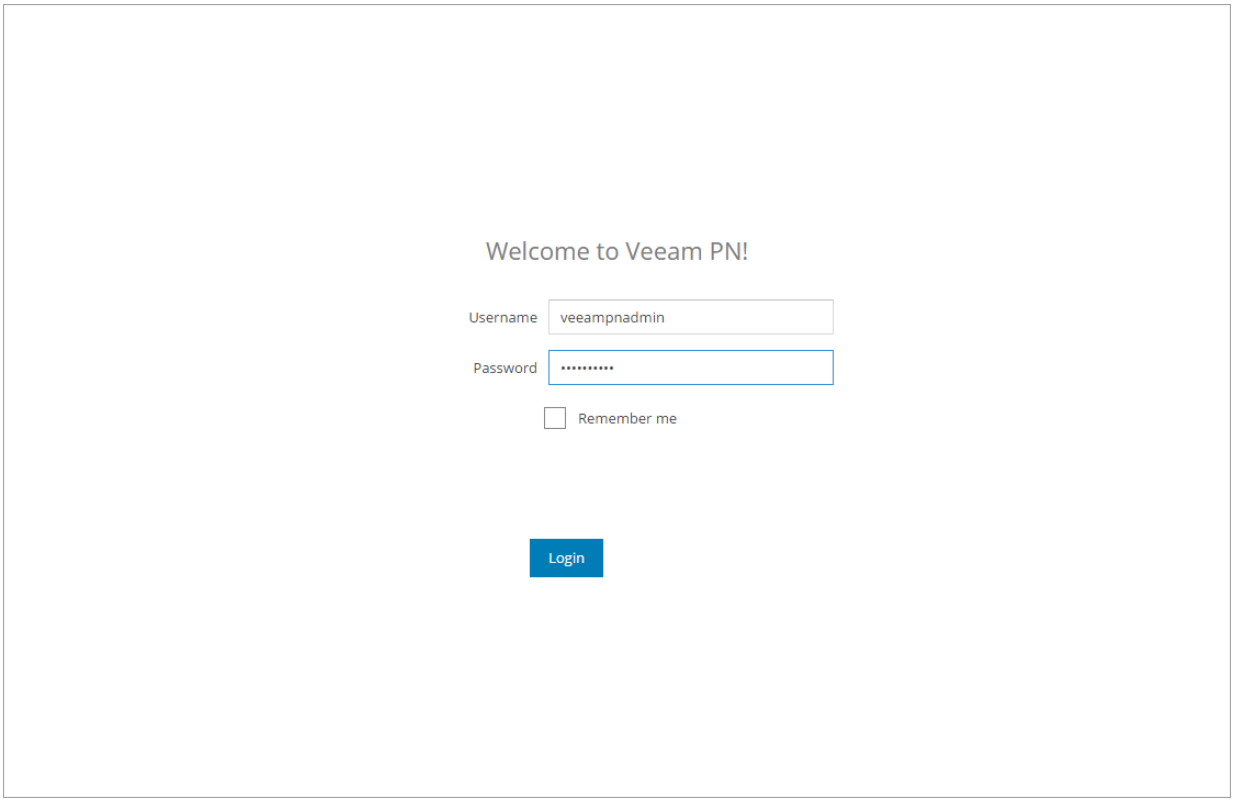
11. In the Microsoft Azure portal, open properties of the deployed appliance and get its IP address.

12. In a web browser, access the Veeam PN portal by the following address: `https://<networkhubIP>`.

    The browser will display a warning notifying that the connection is untrusted. Ignore the warning and agree to proceed to the portal.

13. At the **Welcome** screen, log in to the portal under the network hub administrator account. You specified credentials for the network hub administrator account on the **Basic** blade.

14. Click **Login**.



15. On the welcome screen of the **Azure Setup** wizard, click **Next**.

16. The **Azure Setup** wizard will display the https://aka.ms/devicelogin link and an authentication code. Copy the code to the Clipboard, open the https://aka.ms/devicelogin link in a web browser and enter the code in the code field.

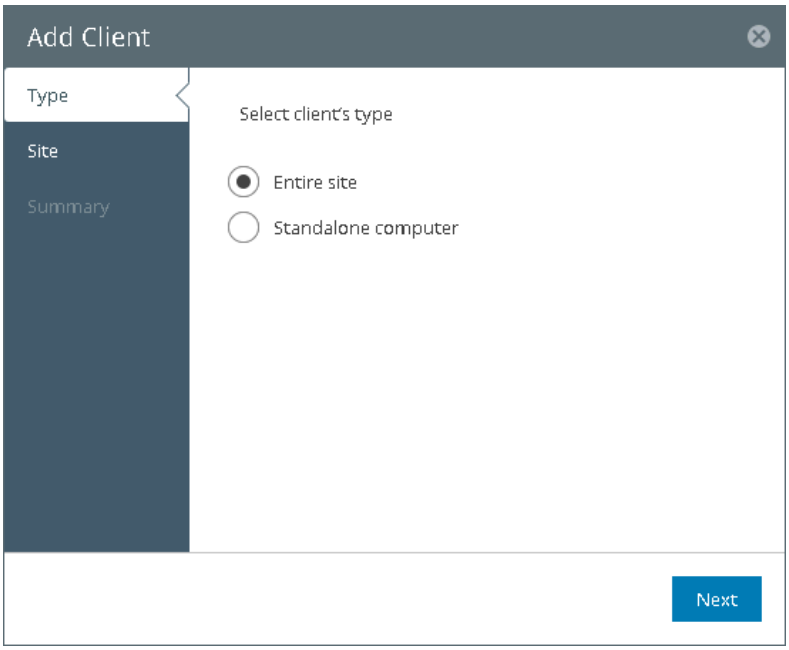
17. Click **Next**. Veeam PN will assign the Network Contributor role on the routing table in the Microsoft Azure network to the network hub administrator account. Wait for the process to complete and click **Finish**.

Step 2. Register Client for Local Site Network in Veeam PN Portal

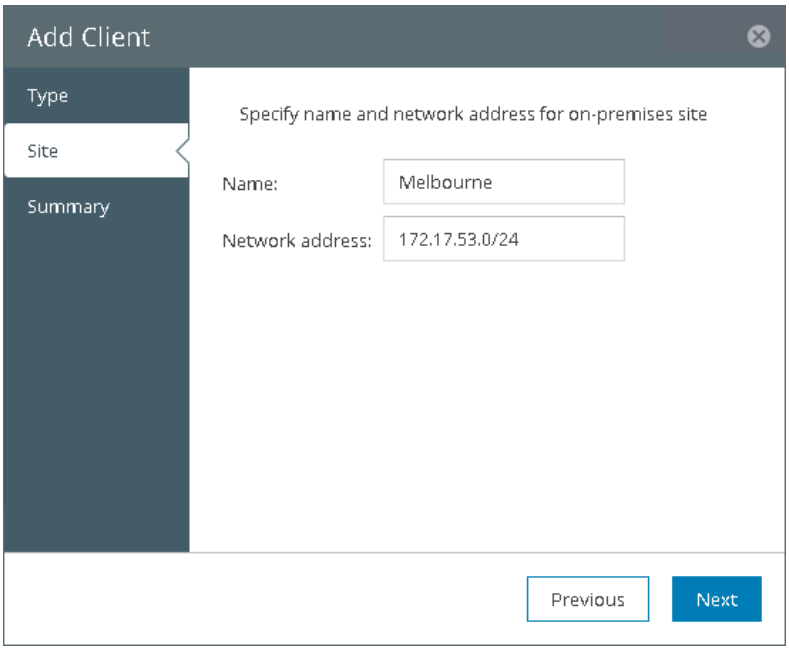
To add a local site network to the VPN, you must register a client for this local network in the Veeam PN portal. Veeam PN will generate a configuration file for the local site network. You will use the configuration file to set up a site gateway in the local site network.

To register a client for the local site network:

1. In the Veeam PN portal, in the configuration menu on the left click **Clients**.
2. At the top of the clients list, click **Add**.
3. At the **Type** step of the wizard, select **Entire site**.



4. At the **Site** step of the wizard, enter a name and address of the local site network using the CIDR notation.



5. At the **Summary** step of the wizard, click **Finish**.

   Veeam PN will generate an XML file with VPN settings for the local site network. The XML file will be automatically downloaded to the default downloads folder. Save the downloaded file in a network shared folder accessible from the local site network.

Step 3. Deploy Site Gateway in Local Site Network

When you deploy the network hub in Microsoft Azure, you configure one point of the VPN tunnel. To configure the other point of the VPN tunnel, you must deploy a site gateway on the local company site. The site gateway establishes a VPN connection with the network hub in Microsoft Azure, which lets data to travel securely over a public connection between remote sites.

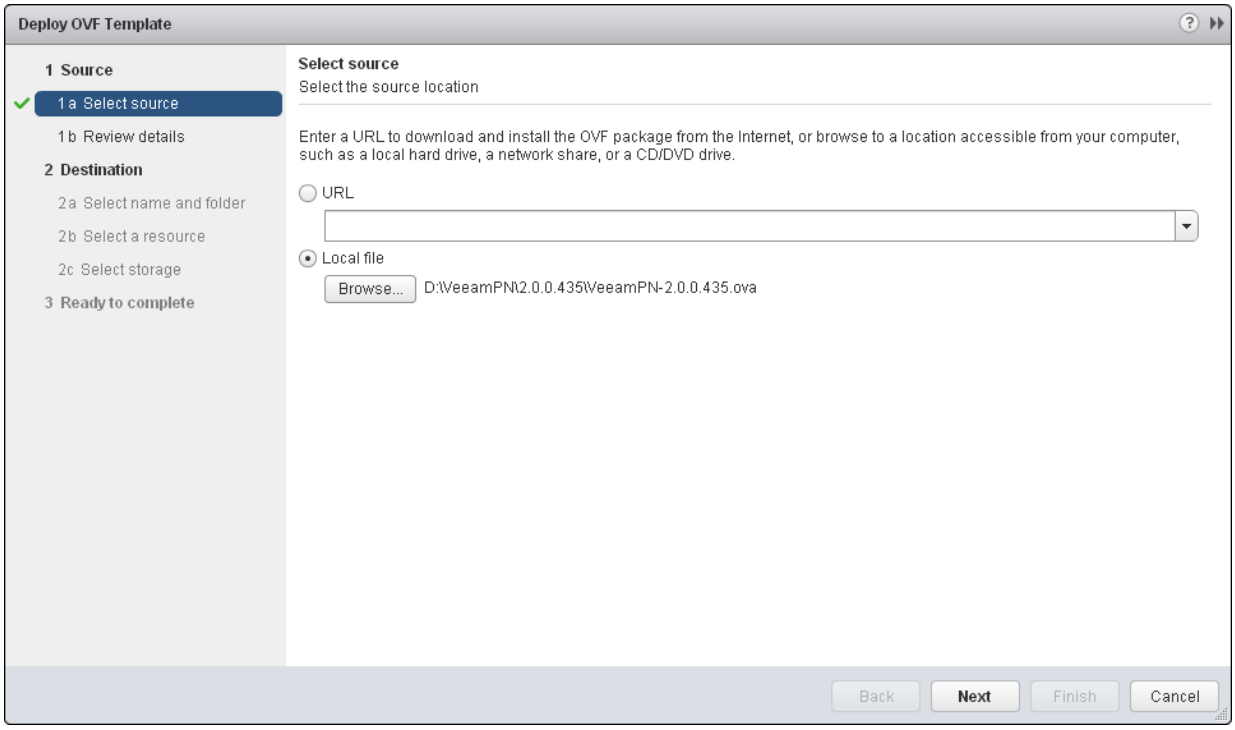
To deploy a site gateway in the local site network:

1. Download the Veeam PN OVA package from: https://www.veeam.com/downloads.html and save it in a network shared folder accessible from the local site network.

2. In VMware vSphere Web Client, open the hosts and clusters inventory list and select a host on which you want to place the site gateway.

3. From the menu at the top of the working area, select **Actions** > **Deploy OVF Template**.

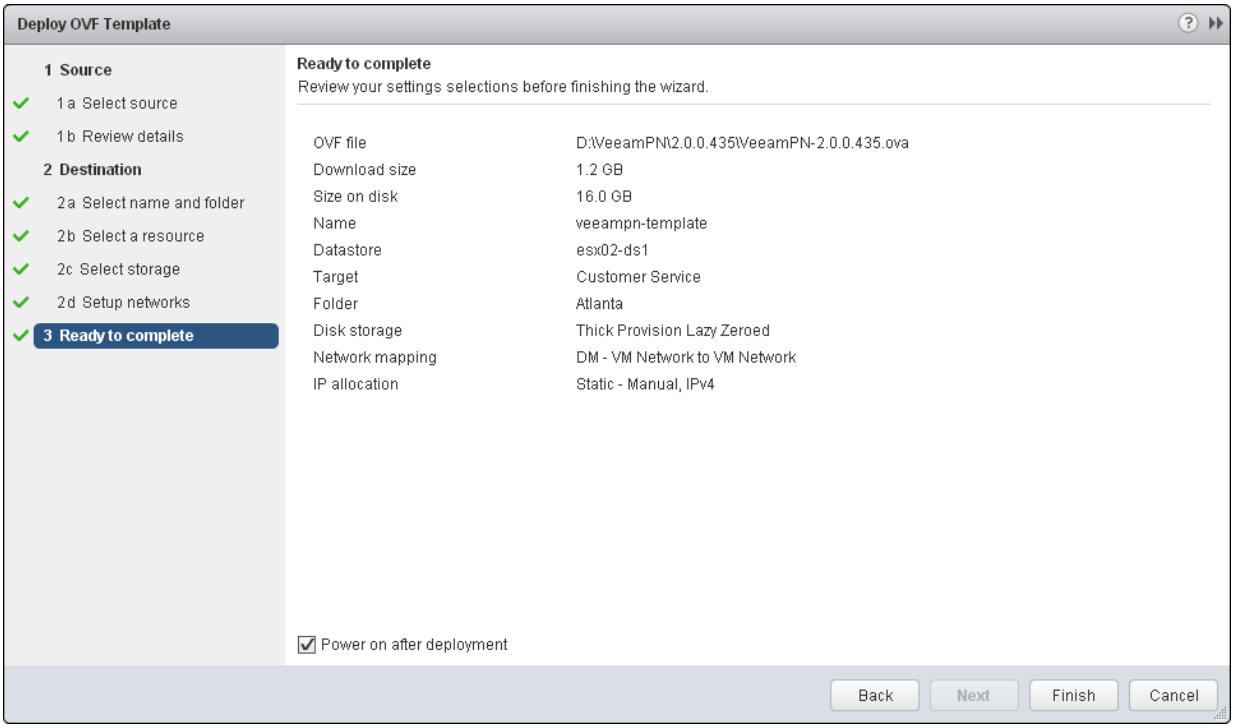
4. At the **Select source** step of the wizard, select **Local file**, click **Browse** and browse to the Veeam PN OVA package.



5. Follow the next steps of the wizard and specify site gateway settings: datastore on which the site gateway VM disk must be placed, disk format, network to which the site gateway must be connected and so on.

6. At the last step of the wizard, select the **Power on after deployment** check box and click **Finish**.

   Veeam PN will deploy the site gateway on the selected host. The deployment process typically takes several minutes. Wait for the process to complete and proceed to site gateway configuration.

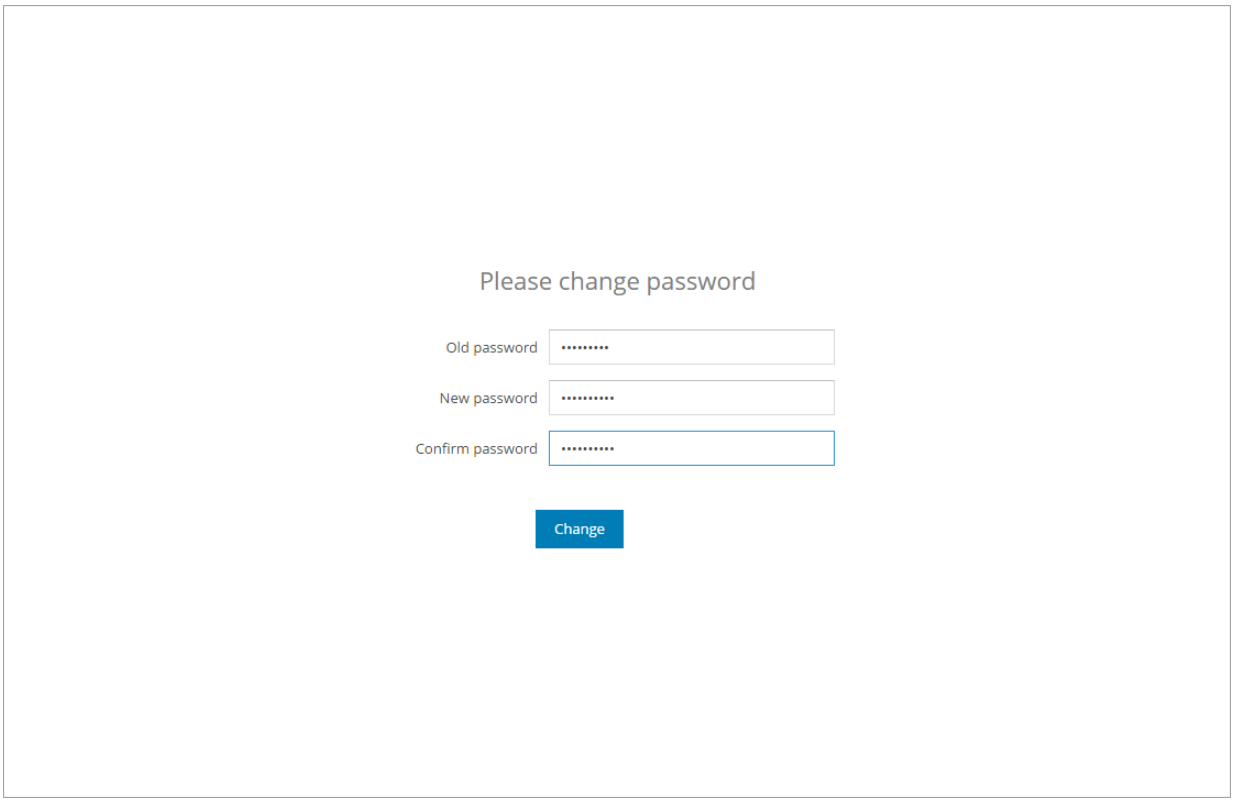


7. In VMware vSphere Web Client, navigate to the **Summary** tab and get an IP address of the deployed site gateway.

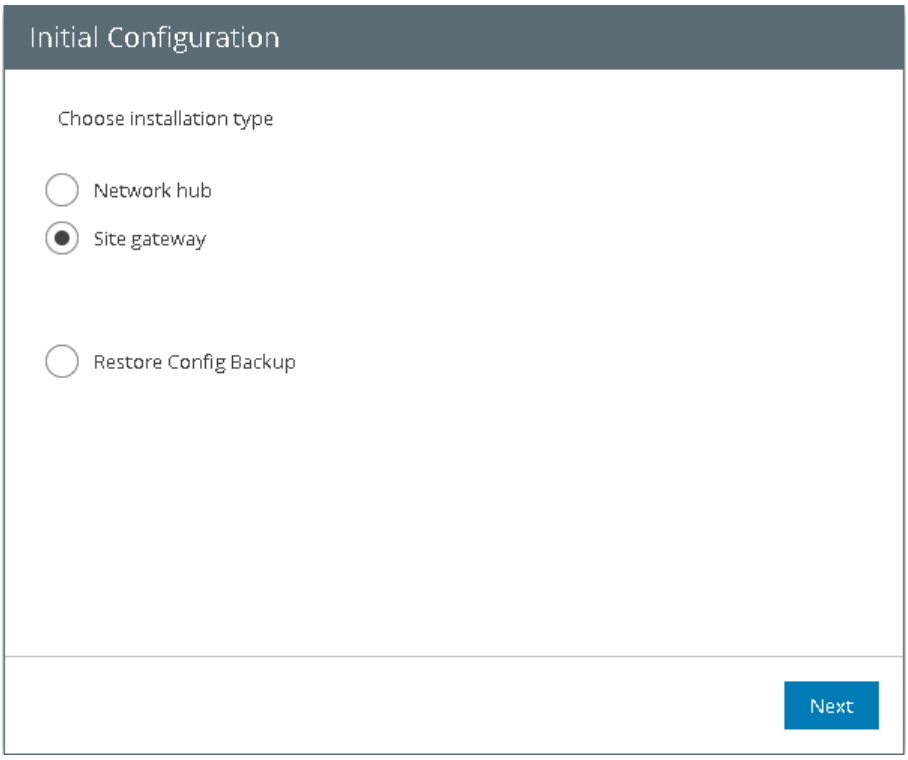
8. In a web browser, access the site gateway portal by the following address: `https://<sitegatewayIPaddress>`.

   The browser will display a warning notifying that the connection is untrusted. Ignore the warning and agree to proceed to the portal.

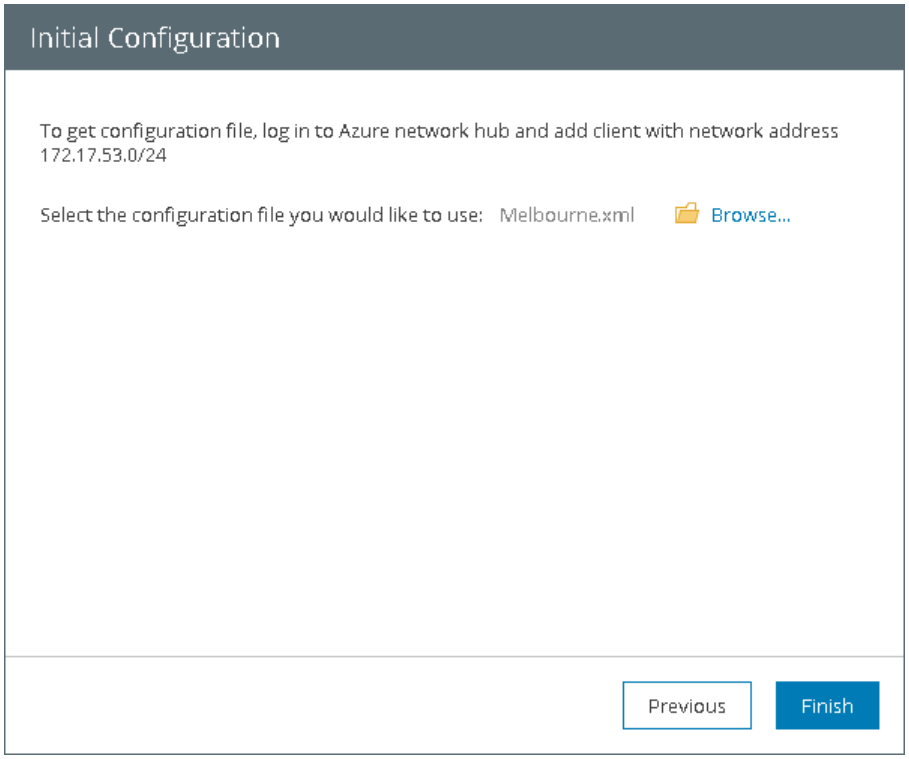
9. At the **Welcome to Veeam PN** screen of the portal, enter the credentials for the built-in administrator acount:
    - Username: *root*
    - Password: *VeeamPN*
10. Click **Login**. When prompted, change the password for the built-in administrator account.



11. At the first step of the **Initial Configuration** wizard, select **Site gateway**.



12. Click **Browse** and browse to the configuration file for the local site network generated by Veeam PN.



13. Click **Finish**.

Step 4. Add Static Routes for Outgoing Traffic on Default Gateways

By default, when a machine in one remote site needs to communicate with a machine in another remote site, it sends a request over the default site gateway. To route traffic going between sites over the VPN tunnel, you need to add static routes on default gateways on both sites. These static routes will destine the traffic from the default gateway to the Veeam PN appliance — network hub or site gateway, which, in its turn, will route traffic through the VPN tunnel between the two sites.

For example, Site A and Site B have the following configuration:

Site A: 192.168.0.0/24

- Network mask: 255.255.255.0
- Site gateway IP address: 192.168.0.2
- Default gateway IP address: 192.168.0.1
- Client machine IP address: 192.168.0.14

Site B: 172.17.53.0/24

- Network mask: 255.255.255.0
- Site gateway IP address: 172.17.53.2
- Default gateway IP address: 172.17.53.1
- Client machine IP address: 172.17.53.12

If a machine in Site A needs to communicate with a machine in Site B, the traffic will first be sent to the default gateway 192.168.0.1. The default gateway must then route the traffic to the site gateway that, in its turn, will route the traffic through the VPN tunnel. For this reason, you must add the following route on the default gateway 192.168.0.1:

```
route add 172.17.53.0 mask 255.255.255.0 192.168.0.2
```

In a similar manner, you must add a route on the default gateway 172.17.53.1 in Site B:

```
route add 192.168.0.0 mask 255.255.255.0 172.17.53.2
```

Result

You have set up a VPN connection between a Microsoft Azure network and local site network. VMs running in Microsoft Azure are now accessible from the local site network, and vice versa.

Set Up VPN from Endpoints to Microsoft Azure

You can use Veeam PN to set up a VPN connection from remote user machines to private clouds in Microsoft Azure. This scenario can be helpful if you have moved some of your application and services to Microsoft Azure. In this case, you can provide company users with access to VMs in Microsoft Azure.

Reference Environment

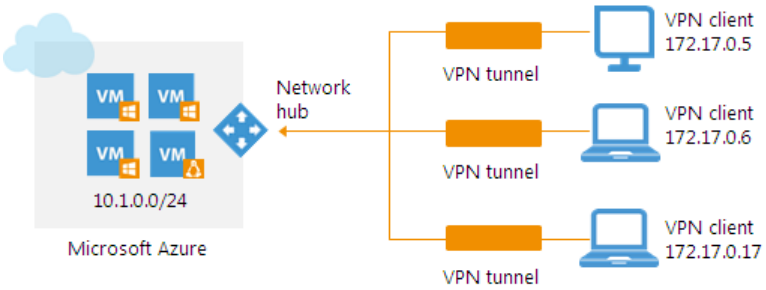
This how-to assumes that your company environment is distributed between two sites:

- Microsoft Azure: part of your applications and services are hosted in Microsoft Azure.
- Local company site: users who need to gain access to Microsoft Azure VMs are working on a local company site or remotely.

In this scenario, you will deploy Veeam PN components in the following way:

- The network hub will be hosted in Microsoft Azure.
- You will configure VPN settings on user machines with the help of OpenVPN.

Whenever users need to access VMs in Microsoft Azure, they will establish a VPN connection from their machines to the network hub in Microsoft Azure, that, in its turn, will route requests to Microsoft Azure VMs.



Prerequisites

To follow instructions of this how-to, check the following prerequisites:

- You must have a user account in Microsoft Azure.
- You must use the Azure Resource Manager model to configure the network hub in Microsoft Azure. The classic deployment model is not supported.

Step-By-Step Walkthrough

To set up a VPN connection from user machines to Microsoft Azure, you will:

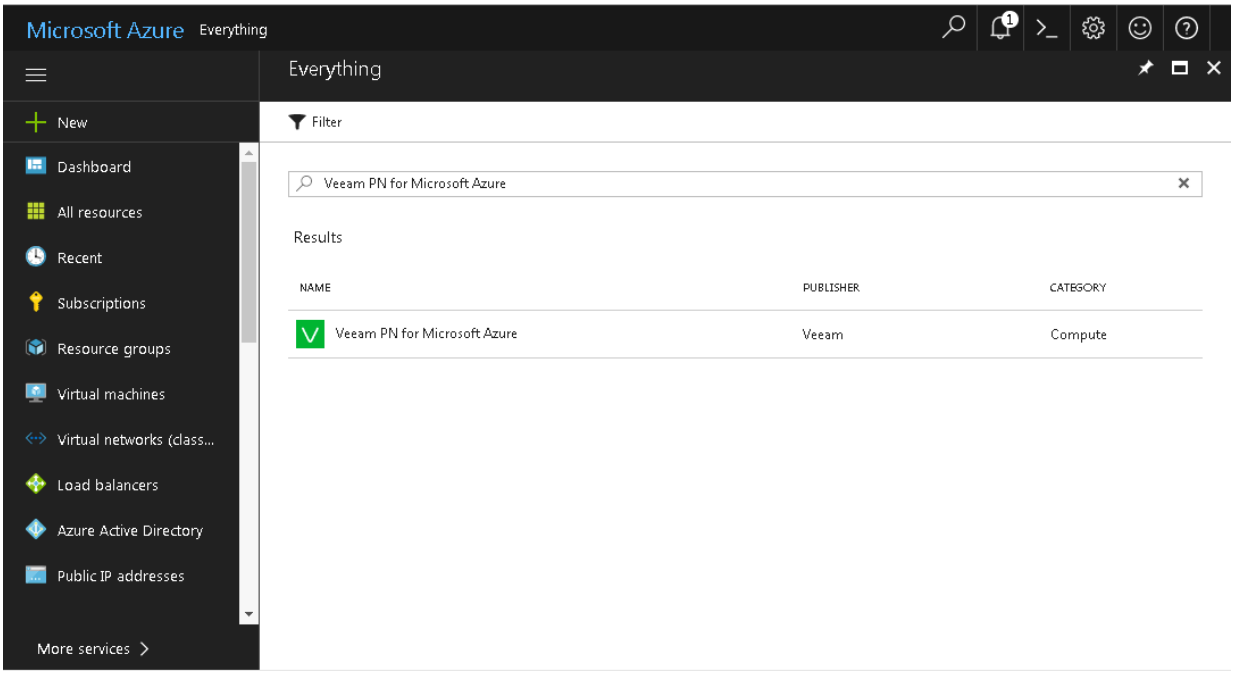
1. Deploy the network hub in Microsoft Azure.
2. Register clients for user machines in the Veeam PN portal.
3. Configure OpenVPN on user machines.
4. Establish a VPN connection from user machines to the network hub in Microsoft Azure.

Step 1. Deploy Network Hub in Microsoft Azure

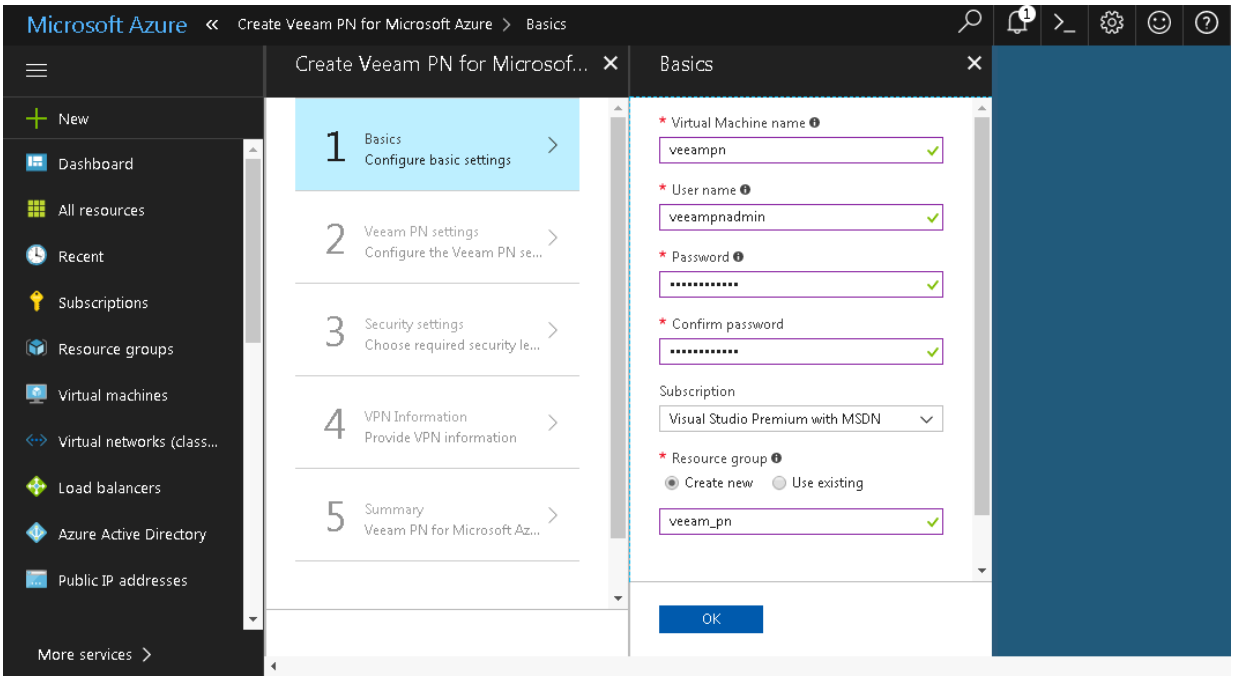
The network hub is the core of the VPN infrastructure. If you want to set up a VPN connection from user machines to VMs in Microsoft Azure, you must deploy the network hub in Microsoft Azure.

To deploy the network hub:

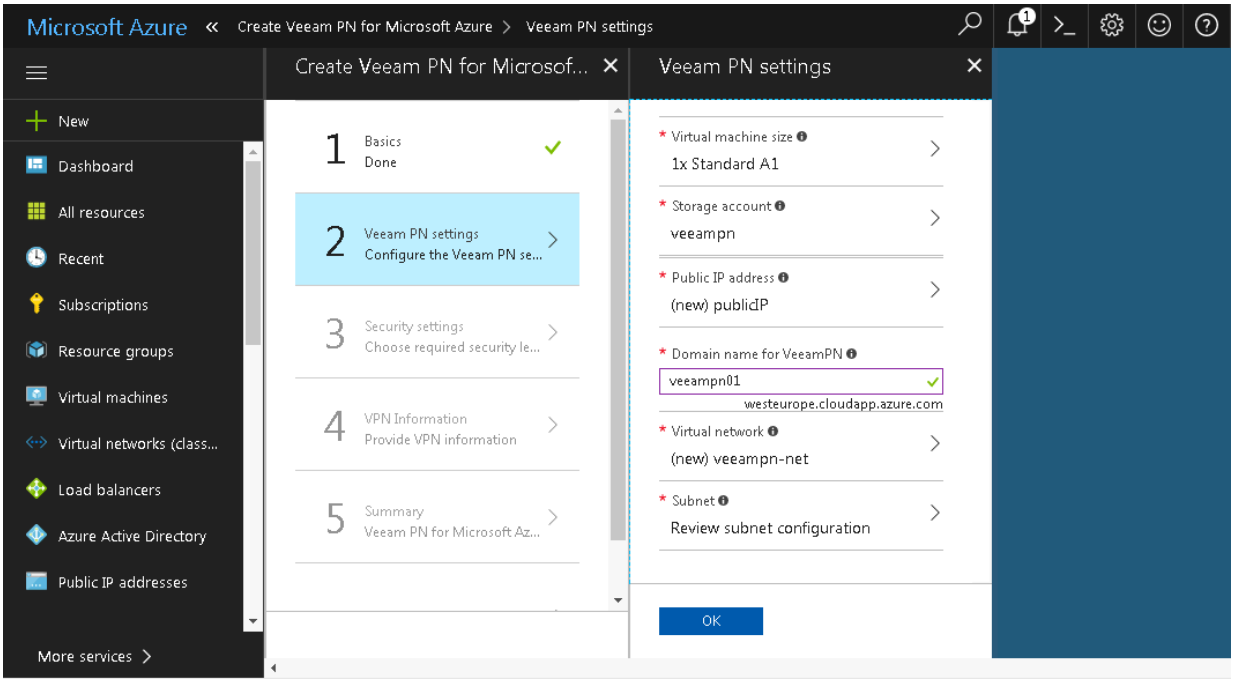
1. Sign in to the Microsoft Azure portal at https://portal.azure.com.
2. In the menu on the left, click **New**.
3. In the marketplace, search for the '*Veeam PN for Microsoft Azure*' template.
4. Select the template and click **Create**.



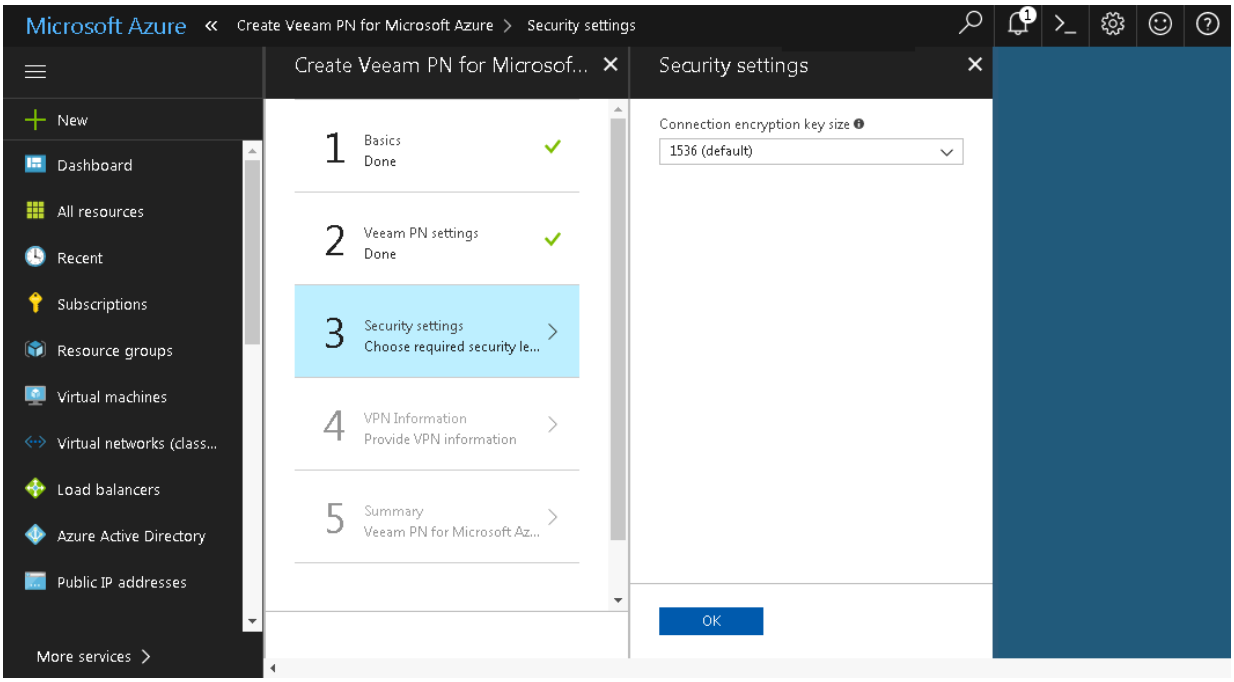
5. On the **Basics** blade, specify basic VM settings: VM name, user credentials for the network hub administrator account, subscription, resource group and location.



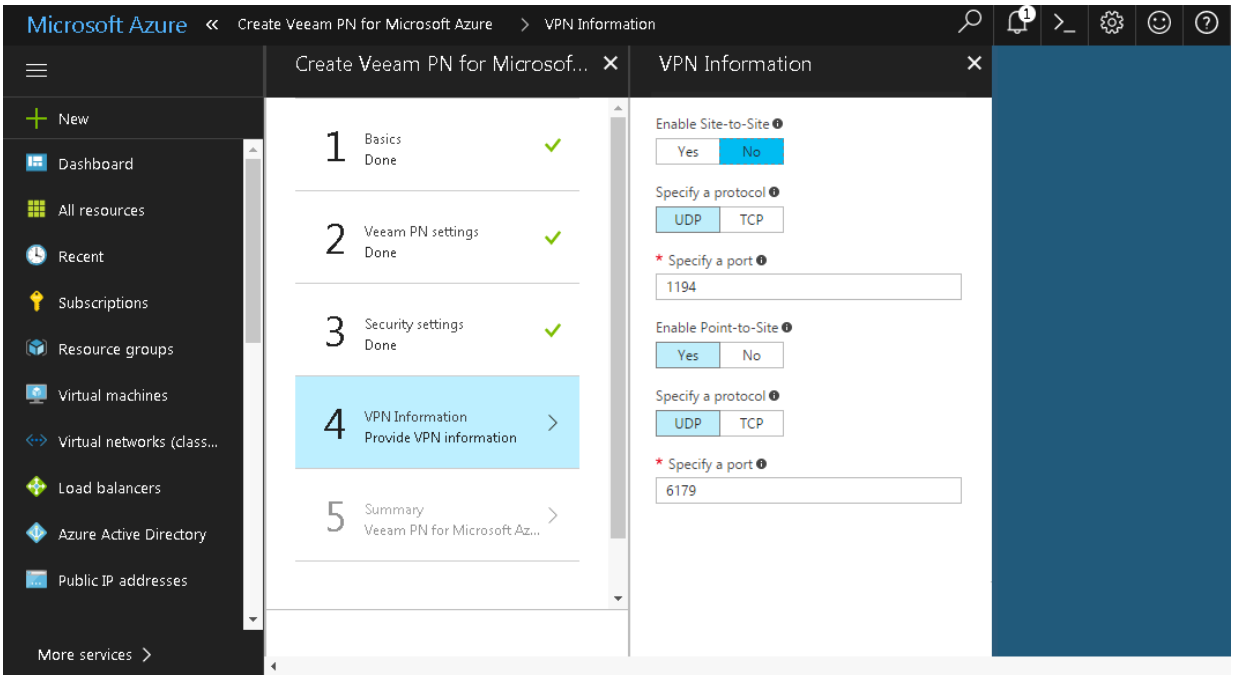
6. On the **Veeam PN settings** blade, specify basic settings for the network hub appliance: VM size (A1 size is minimum), storage account, public IP address, domain name, virtual network and subnet.



7. On the **Security settings** blade, specify parameters for the self-signed SSL certificate that Veeam PN will use to secure connection in the VPN: the certificate key length.



8. On the **VPN Information** blade, make sure that **Yes** is enabled in the **Enable Point-to-Site** field. In the **Specify a protocol** and **Specify a port** fields, leave default settings.



9. On the **Summary** blade, click **OK**.

10. On the **Buy** blade, click **Purchase**.

    Veeam PN will deploy the network hub from the Microsoft Azure template. The deployment process typically takes several minutes. Wait for this process to complete.

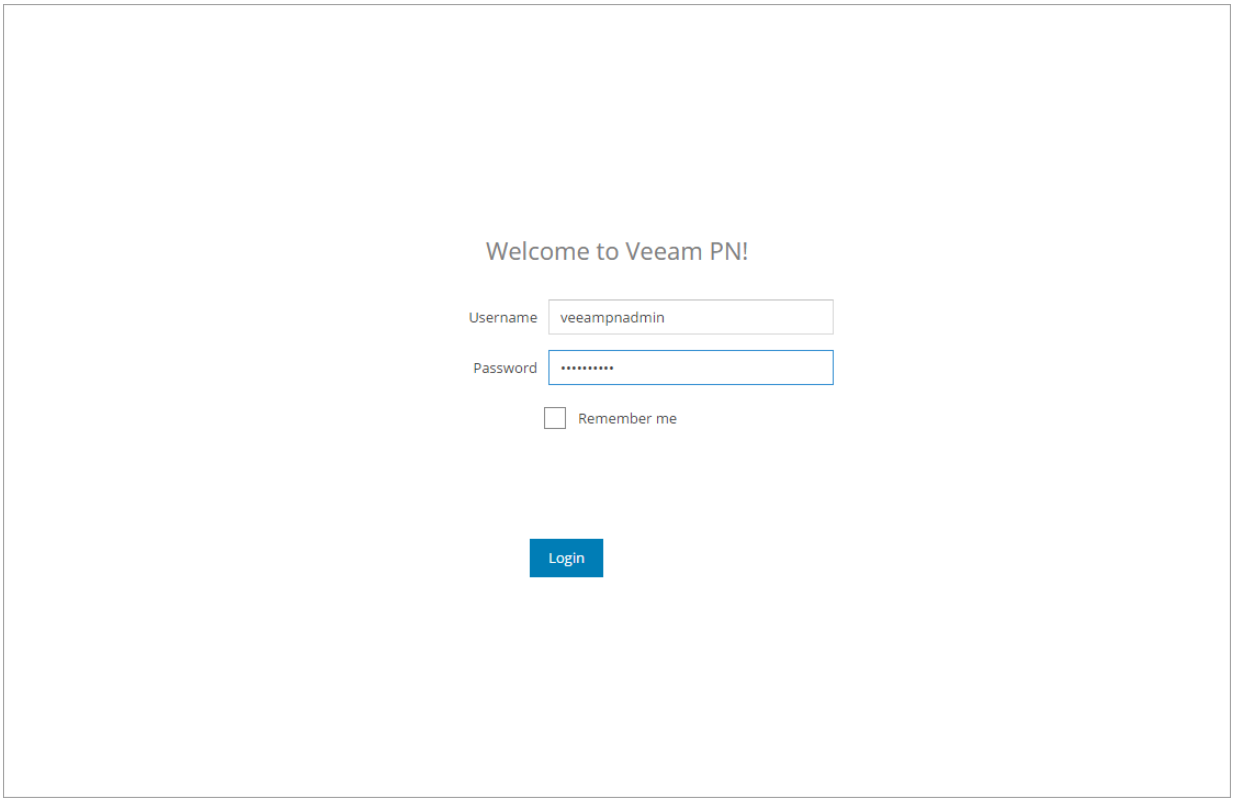
11. In the Microsoft Azure portal, open properties of the deployed VM and get its IP address.

12. In a web browser, access the Veeam PN portal by the following address: `https://<networkhubIP>`.

The browser will display a warning notifying that the connection is untrusted. Ignore the warning and agree to proceed to the portal.

13. At the **Welcome** screen, log in to the portal under the network hub administrator account. You specified credentials for the network hub administrator account on the **Basic** blade.

14. Click **Login**.



15. On the welcome screen of the **Azure Setup** wizard, click **Next**.

16. The **Azure Setup** wizard will display the https://aka.ms/devicelogin link and an authentication code. Copy the code to the Clipboard, open the https://aka.ms/devicelogin link in a web browser and enter the code in the code field.

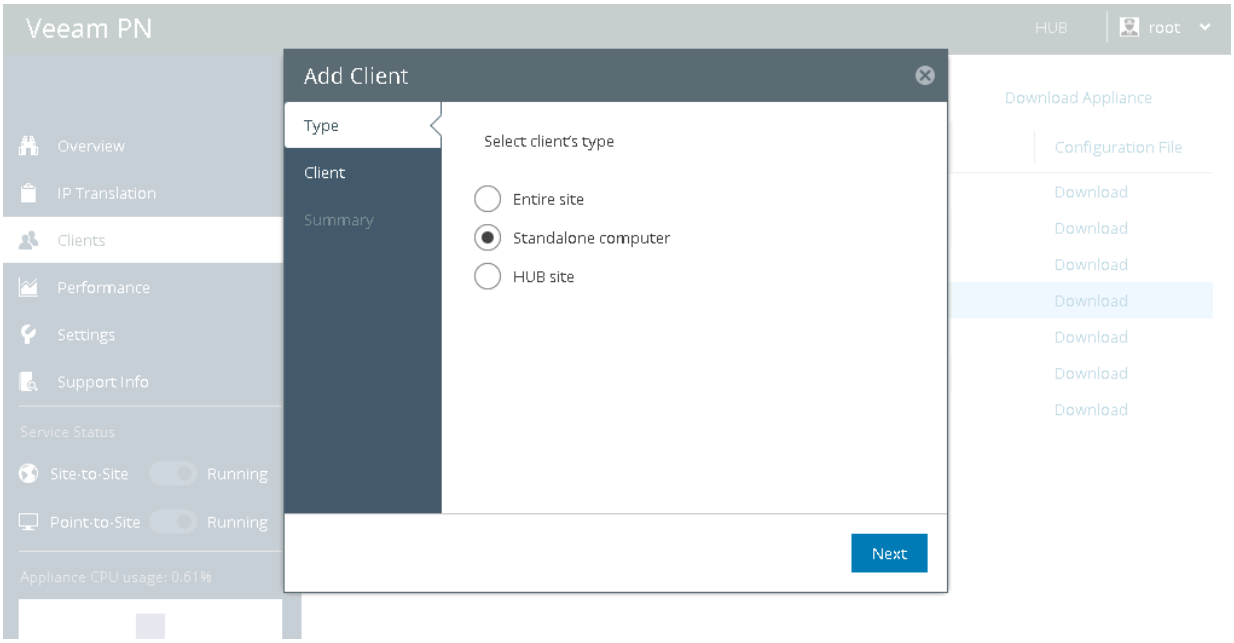
17. Click **Next**. Veeam PN will assign the Network Contributor role on the routing table in the Microsoft Azure network to the network hub administrator account. Wait for the process to complete and click **Finish**.

Step 2. Register Clients for User Machines

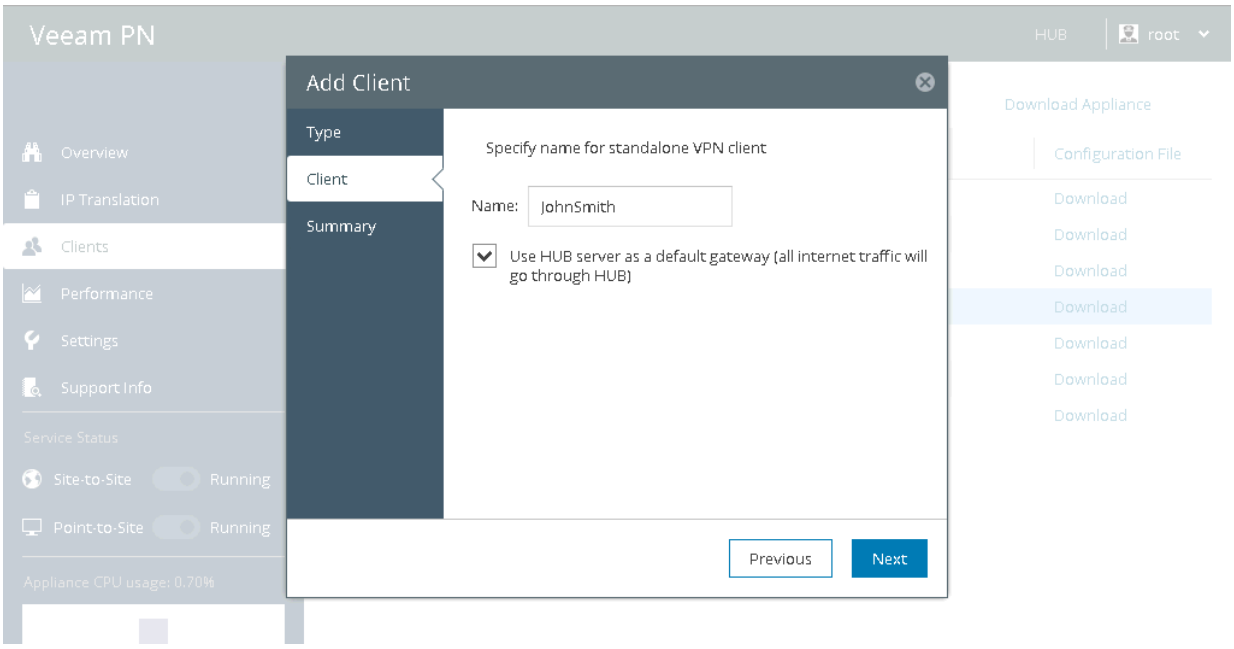
To provide remote users with access to VMs in Microsoft Azure, you must register clients for these users in the Veeam PN portal. Veeam PN will generate configuration files for users. You will use these configuration files to set up a VPN connection on user machines.

To register a client for user machines:

1. In the Veeam PN portal, in the configuration menu on the left click **Clients**.
2. At the top of the clients list, click **Add**.
3. At the **Type** step of the wizard, select **Standalone computer**.



4. At the **Client** step of the wizard, enter a name for the user machine.
5. Select the **Use HUB server as a default gateway** check box.



6. At the **Summary** step of the wizard, click **Finish**.

   Veeam PN will generate an XML file with VPN settings for the user. The XML file will be automatically downloaded to the default downloads folder. Save the downloaded file in a network shared folder accessible from the user machine.

7. Repeat steps 1-5 for all users to whom you want to provide access.

Step 3. Configure OpenVPN on User Machines

To let a user access VMs in Microsoft Azure over the VPN, you must configure VPN settings on the user machine. To do this, you must use OpenVPN software and a configuration file generated by Veeam PN.

To configure OpenVPN on user machines:

1. Download the OpenVPN setup file for the user machine OS from: https://openvpn.net/index.php/open-source/downloads.html.

2. Run the OpenVPN setup file and install the product with default installation settings.

3. Place the configuration file generated by Veeam PN in a folder where OpenVPN configuration files are stored: `C:\Program Files\OpenVPN\config`.

4. Repeat steps 1-3 for all users to whom you want to provide access.

Step 4. Establish VPN connection from User Machines to Microsoft Azure

To establish a VPN connection from user machines to Microsoft Azure:

1. On a user machine, create a batch file with the following command:

   ```
   "openvpn-gui.exe" -- connect "C:\Program Files\OpenVPN\config\client.ovpn"
   ```

   where `C:\Program Files\OpenVPN\bin\openvpn-gui.exe` is a path to the OpenVPN product folder and `C:\Program Files\OpenVPN\config\client.ovpn` is a path to the user machine configuration file.

2. Run the batch file. Veeam PN will establish a connection from the user machine to the network hub.

3. Repeat steps 1-2 for all users to whom you want to provide access.

Result

You have set up a VPN connection from user machines to VMs to Microsoft Azure. VMs running in Microsoft Azure are now accessible to users working remotely.

Set Up VPN Between Remote Sites

You can use Veeam PN to set up a VPN connection between remote company offices and sites. This scenario can be helpful if company services and applications are distributed between two or more sites, for example, a headquarters site and branch office. In this case, you can join several remote networks over the VPN and enable secure communication between them.

Reference Environment

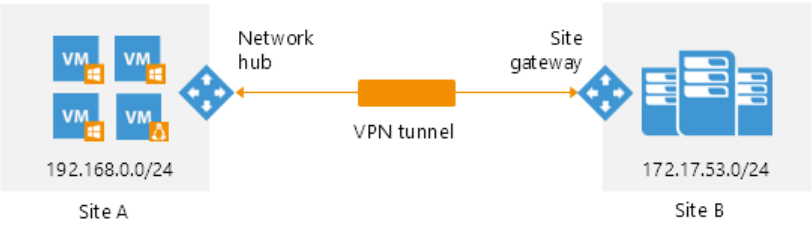
This how-to assumes that your company environment is distributed between two remote sites:

- Site A: part of your applications and services are hosted on Site A.
- Site B: part of your applications and services are hosted on Site B.

In this scenario, you will deploy Veeam PN components in the following way:

- The network hub will be deployed on Site A.
- A site gateway will be deployed on Site B.

The network hub and site gateway will produce the two terminal points of a VPN tunnel. Application and services on Site A and Site B will be able to communicate securely with each other over the VPN. Users on one remote site will be able to access resources on the other site.



Prerequisites

To follow instructions of this how-to, check the following prerequisite:

You must have a VMware vSphere host in each site. The network hub and site gateway are deployed as virtual appliances and placed on VMware vSphere hosts.

Step-By-Step Walkthrough

To set up a VPN connection between remote sites, you will:

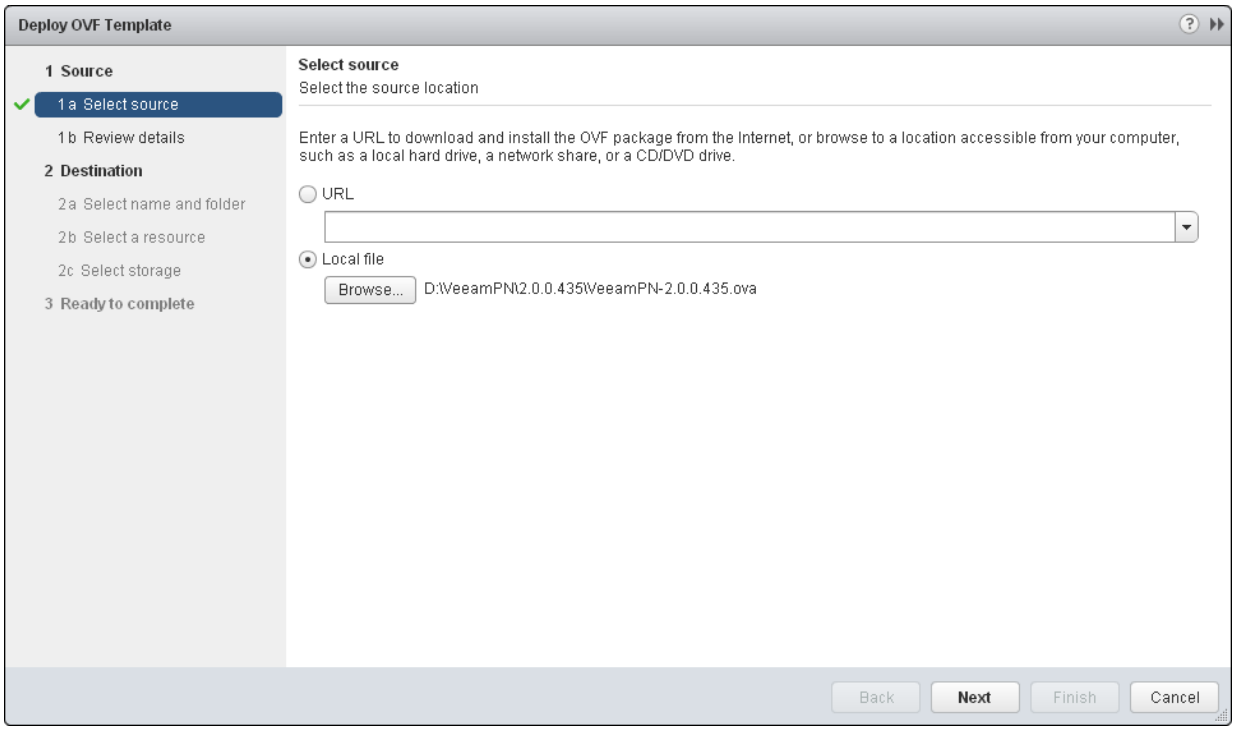
1. Deploy the network hub in a local site network.
2. Register a client for a remote network.
3. Deploy a site gateway in the remote network.
4. Add static routes for outgoing traffic on default gateways.

Step 1. Deploy Network Hub in Local Site Network

The network hub is the core of the VPN infrastructure. If you want to join several remote networks, you must deploy the network hub in one of them.

To deploy the network hub:

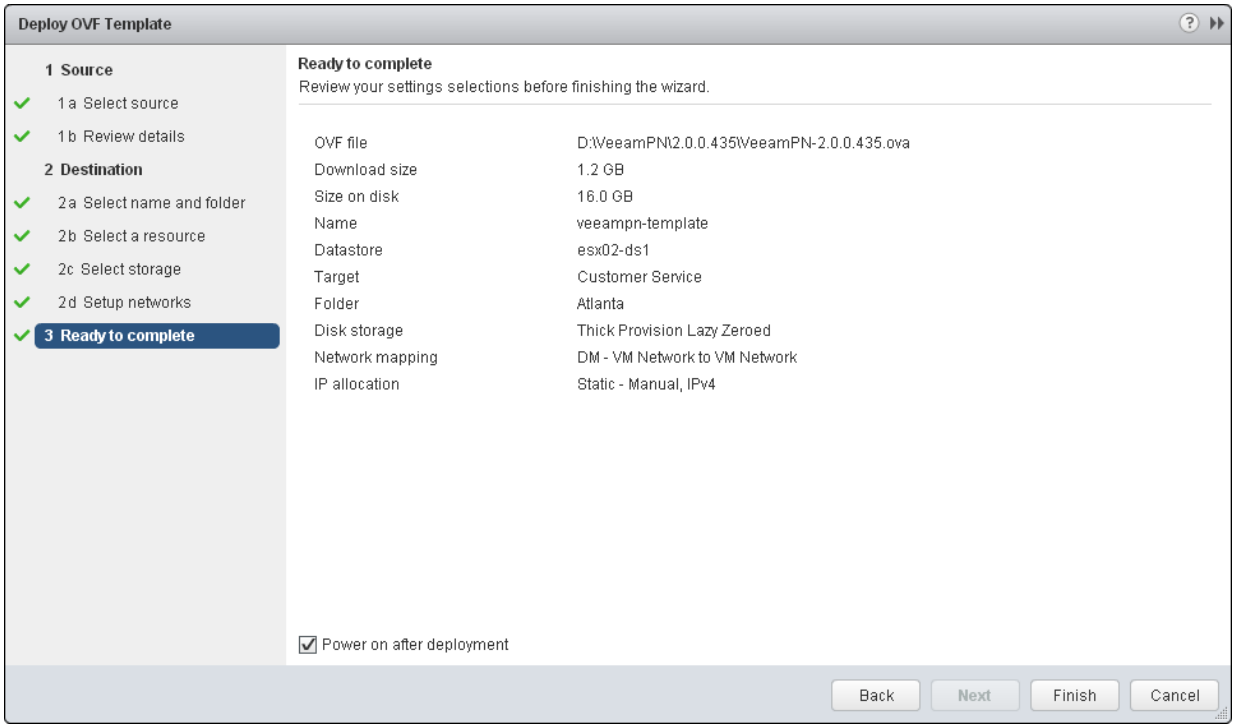
1. Download the Veeam PN OVA package from: https://www.veeam.com/downloads.html and save it in a network shared folder accessible from the site where you plan to deploy the network hub.
2. In VMware vSphere Web Client, open the hosts and clusters inventory list and select a host on which you want to place the network hub.
3. From the menu at the top of the working area, select **Actions** > **Deploy OVF Template**.
4. At the **Select source** step of the wizard, select **Local file**, click **Browse** and browse to the Veeam PN OVA package.



5. Follow the next steps of the wizard and specify network hub deployment settings: datastore on which the network hub disk must be placed, disk format, network to which the network hub must be connected and so on.

6. At the last step of the wizard, select the **Power on after deployment** check box and click **Finish**.

   VMware vSphere will deploy the network hub on the selected host. The deployment process typically takes several minutes. Wait for this process to complete and proceed to network hub configuration.

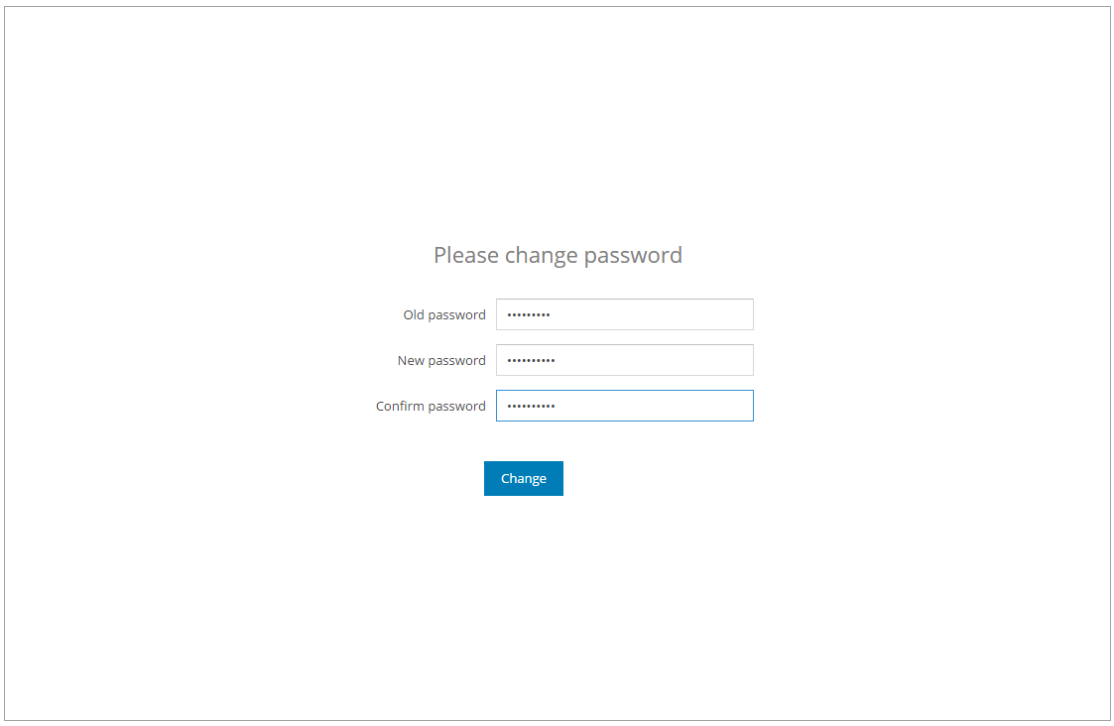


7. In VMware vSphere Web Client, navigate to the **Summary** tab and get an IP address of the network hub.

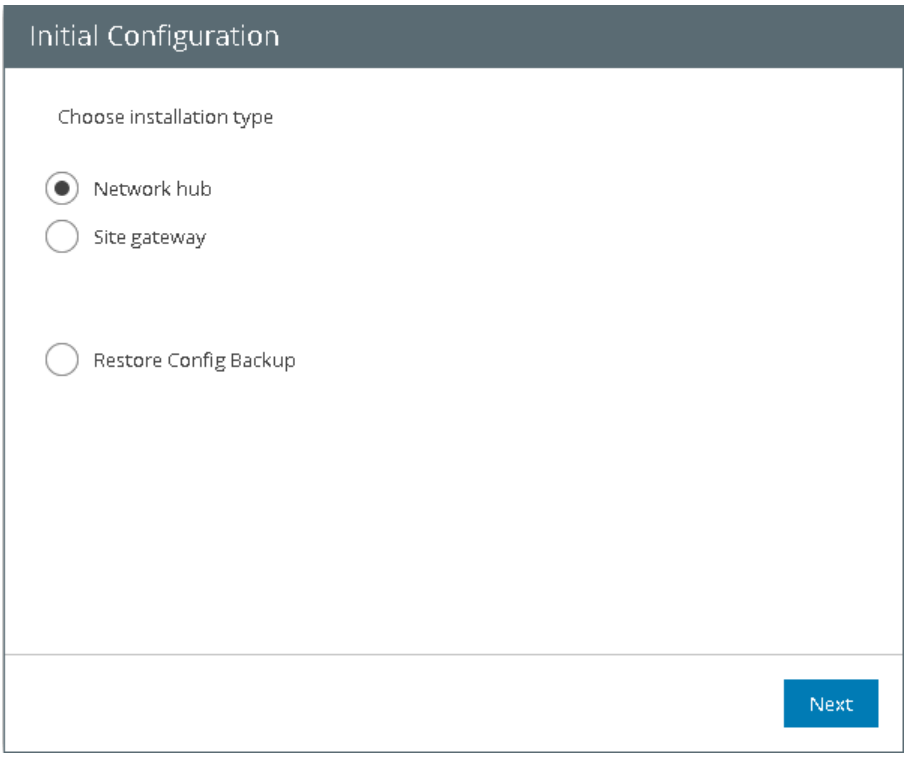
8. In a web browser, access the network hub portal by the following address: `https://<applianceIP>`.

   The browser will display a warning notifying that the connection is untrusted. Ignore the warning and agree to proceed to the portal.

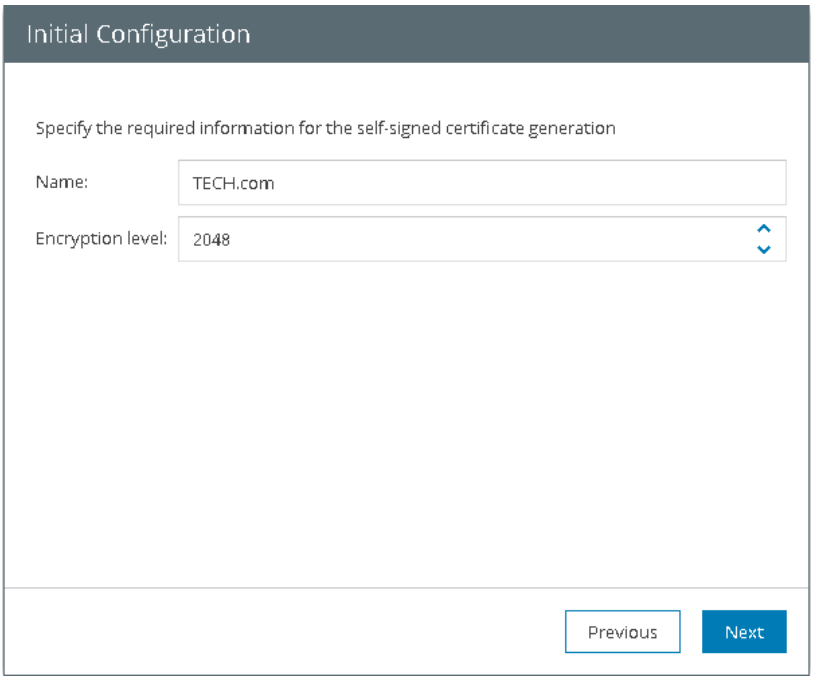
9. At the **Welcome to Veeam PN** screen of the portal, log in to the network hub portal using the credentials of the built-in account:
    - Username: *root*
    - Password: *VeeamPN*
10. Click **Login**.
11. When prompted, change the password for the built-in account.



12. At the first step of the **Initial Configuration** wizard, select **Network hub** and click **Next**.



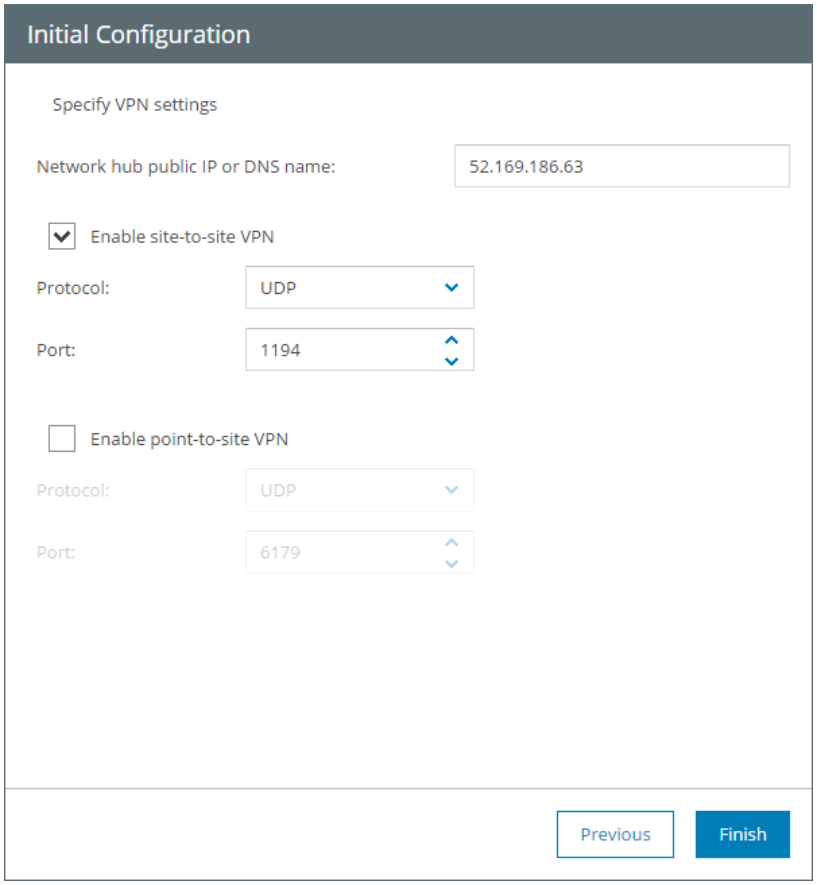
13. Specify parameters for a self-signed certificate that Veeam PN will use to secure communication in the VPN: the certificate key length and click **Next**.



14. After the certificate is generated, click **OK**, then click **Next** to proceed to the network hub configuration.

15. In the **Network hub public IP or DNS** name field, specify an IP address or full DNS name for the network hub. The IP address or DNS name must be public and accessible from remote user machines.

16. Select the **Enable site-to-site VPN** check box. In the **Protocol** and **Port** fields, leave default settings.



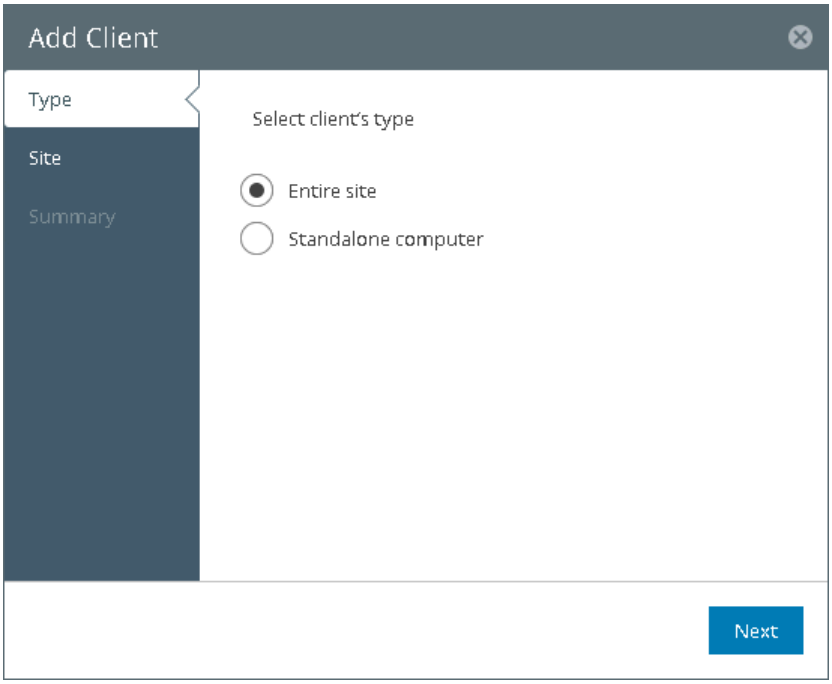
17. Click **Finish**.

Step 2. Register Client for Remote Network

To add a remote network to the VPN, you must register a client for this network in the Veeam PN portal. Veeam PN will generate a configuration file for the remote network. You will use the configuration file to set up a site gateway in the network.

To register a client for the remote network:

1. In the Veeam PN portal, in the configuration menu on the left click **Clients**.
2. At the top of the clients list, click **Add**.
3. At the **Type** step of the wizard, select **Entire site**.

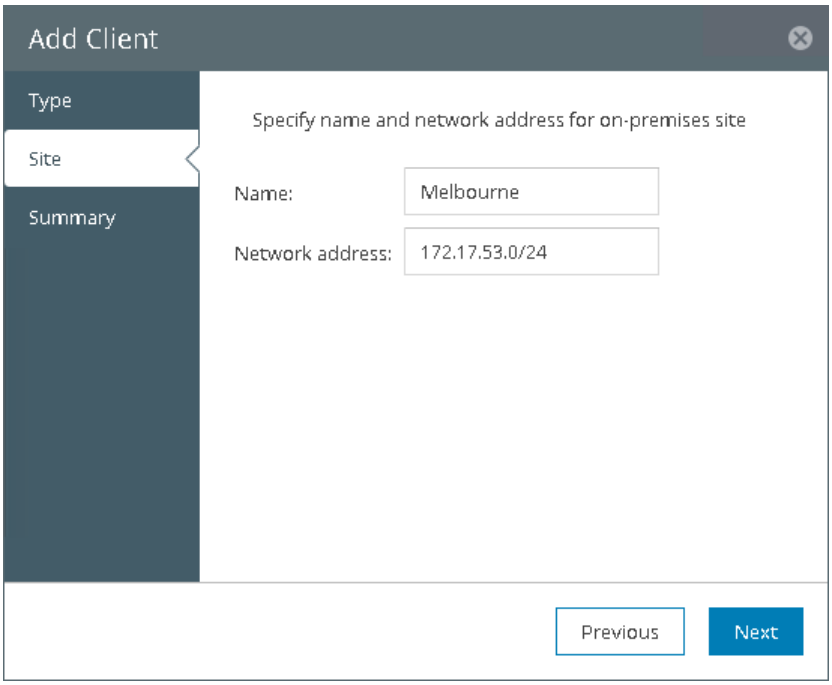


NOTE:

If you add a client for the Hub site, it will make machines on the Hub site accessible over the VPN. To see how to add a client for the Hub site, see Registering Hub Site.

4.

5. At the **Site** step of the wizard, enter a name and address of the remote network using the CIDR notation.



6. At the **Summary** step of the wizard, click **Finish**.

   Veeam PN will generate an XML file with VPN settings for the remote network. The XML file will be automatically downloaded to the default downloads folder. Save the downloaded file in a network shared folder accessible from the remote network.

Step 3. Deploy Site Gateway in Remote Network

When you deploy the network hub in Site A, you configure one point of the VPN tunnel. To configure the other point of the VPN tunnel, you must deploy a site gateway in Site B. The network hub will establish a connection with the site gateway, which lets data to travel securely between remote sites over a public connection.

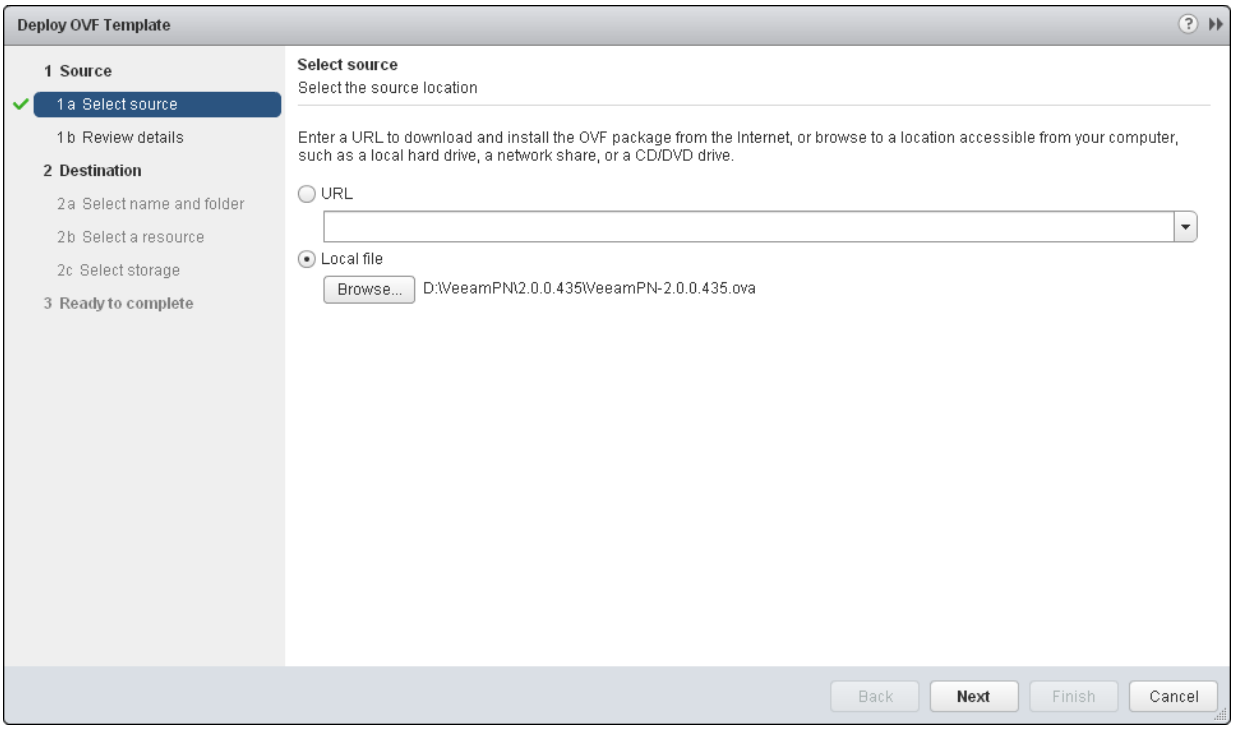
To deploy a site gateway in the remote network:

1. Download the Veeam PN OVA package from: https://www.veeam.com/downloads.html and save it in a network shared folder accessible from the remote network.

2. In VMware vSphere Web Client, open the hosts and clusters inventory list and select a host on which you want to deploy the site gateway.

3. From the menu at the top of the working area, select **Actions** > **Deploy OVF Template**.

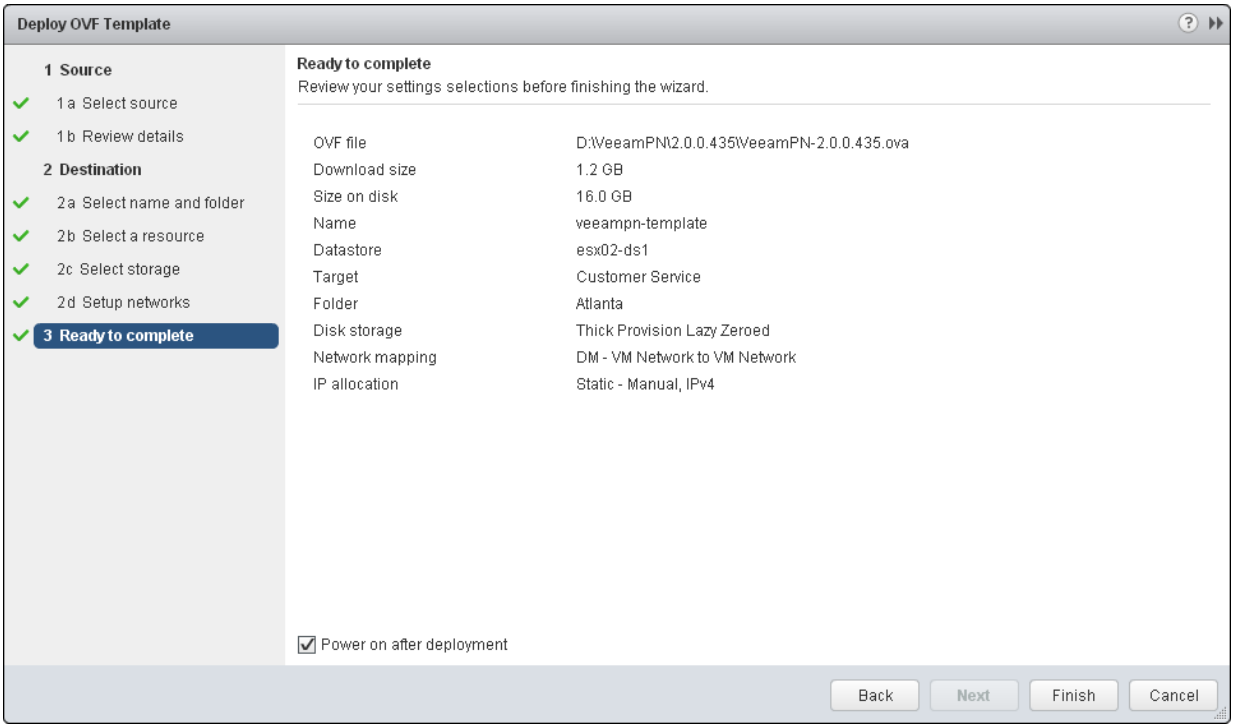
4. At the **Select source** step of the wizard, select **Local file**, click **Browse** and browse to the Veeam PN OVA package.



5. Follow the next steps of the wizard and specify site gateway settings: datastore on which the site gateway VM disk must be placed, disk format, network to which the site gateway must be connected and so on.

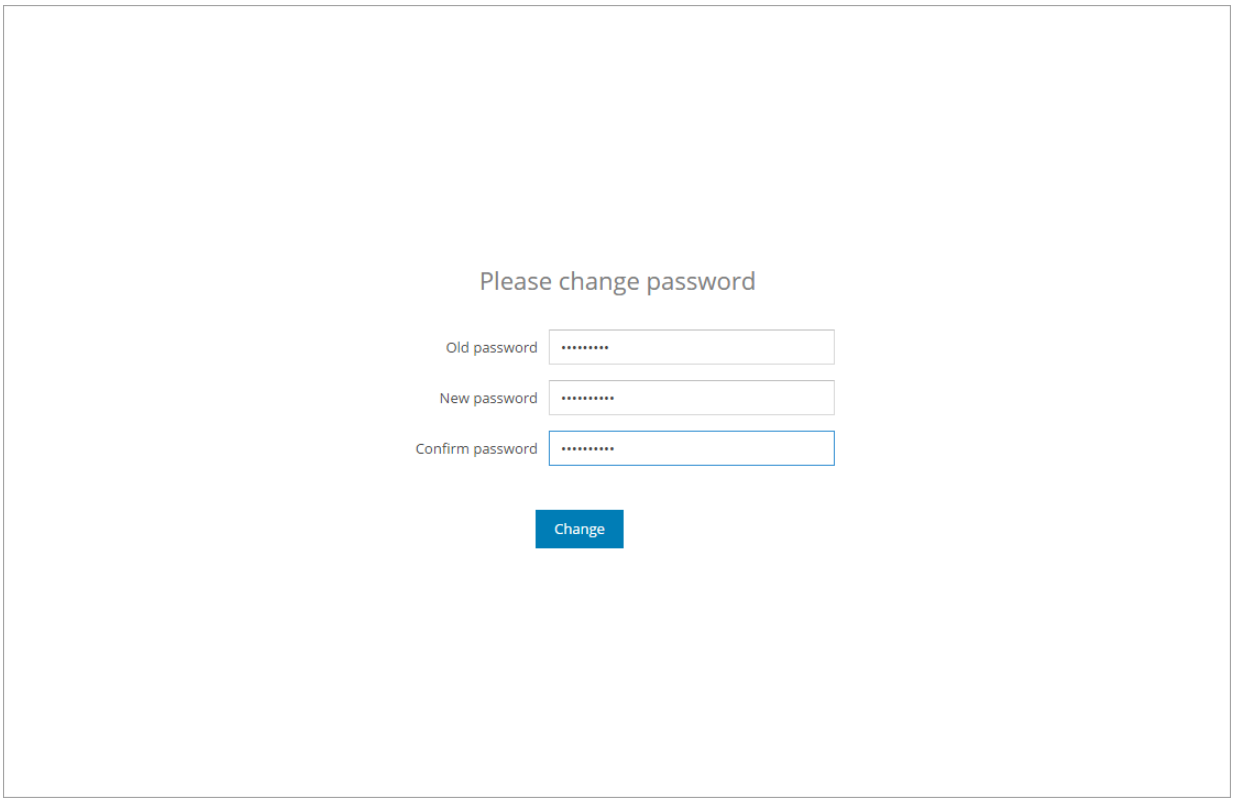
6. At the last step of the wizard, select the **Power on after deployment** check box and click **Finish**.

   The deployment process typically takes several minutes. Wait for the process to complete and proceed to site gateway configuration.

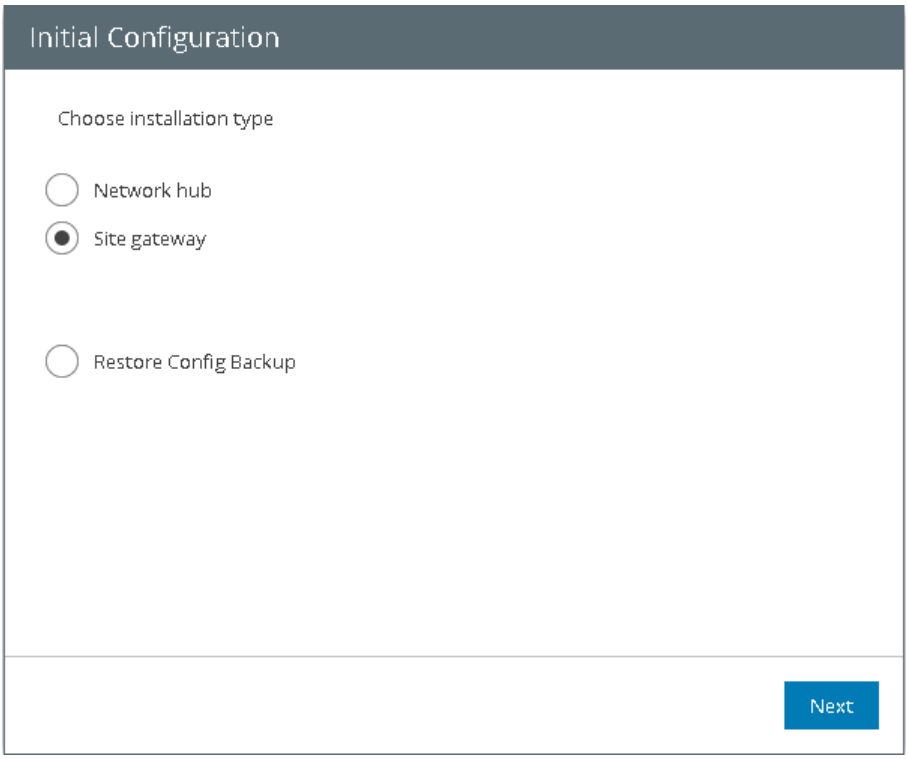


7. In VMware vSphere Web Client, navigate to the **Summary** tab and get an IP address of the deployed site gateway.
8. In a web browser, access the site gateway portal by the following address: `https://<sitegatewayIPaddress>`.

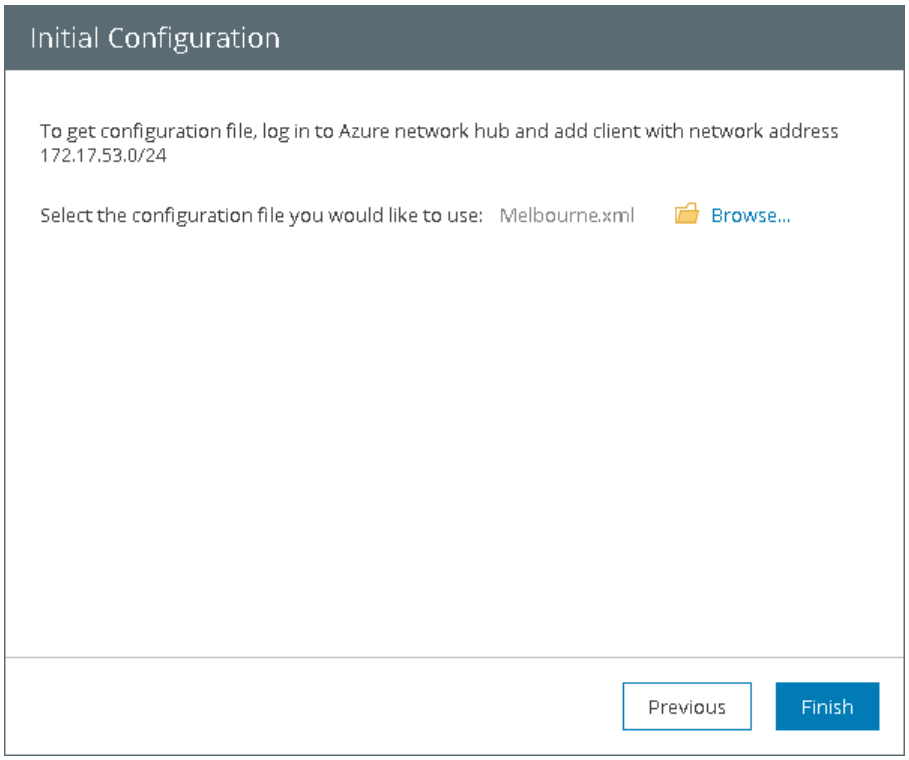
   The browser will display a warning notifying that the connection is untrusted. Ignore the warning and agree to proceed to the portal.
9. At the **Welcome to Veeam PN** screen of the portal, enter credentials for the built-in account:
   - Username: *root*
   - Password: *VeeamPN*
10. Click **Login**. When prompted, change the password for the built-in account.



11. At the first step of the **Initial Setup** wizard, select **Site gateway**.



12. Click **Browse** and browse to the configuration file generated by Veeam PN.



13. Click **Finish**.

Step 4. Add Static Routes for Outgoing Traffic on Default Gateways

By default, when a machine in one remote site needs to communicate with a machine in another remote site, it sends a request over the default site gateway. To route traffic going between sites over the VPN tunnel, you need to add static routes on default gateways on both sites. These static routes will destine the traffic from the default gateway to the Veeam PN appliance — network hub or site gateway, which, in its turn, will route traffic through the VPN tunnel between the two sites.

For example, Site A and Site B have the following configuration:

Site A: 192.168.0.0/24

- Network mask: 255.255.255.0
- Site gateway IP address: 192.168.0.2
- Default gateway IP address: 192.168.0.1
- Client machine IP address: 192.168.0.14

Site B: 172.17.53.0/24

- Network mask: 255.255.255.0
- Site gateway IP address: 172.17.53.2
- Default gateway IP address: 172.17.53.1
- Client machine IP address: 172.17.53.12

If a machine in Site A needs to communicate with a machine in Site B, the traffic will first be sent to the default gateway 192.168.0.1. The default gateway must then route the traffic to the site gateway that, in its turn, will route the traffic through the VPN tunnel. For this reason, you must add the following route on the default gateway 192.168.0.1:

```
route add 172.17.53.0 mask 255.255.255.0 192.168.0.2
```

In a similar manner, you must add a route on the default gateway 172.17.53.1 in Site B:

```
route add 192.168.0.0 mask 255.255.255.0 172.17.53.2
```

Result

You have set up a VPN connection between two remote sites. VMs running on one site are now accessible for machines running on the other site.

Set Up VPN from Endpoints to Local Site

You can use Veeam PN to set up a VPN connection from remote user machines to application and services on a local company site. This scenario can be helpful if some of your users are working remotely, for example, travelling, and still need to use company resources. In this case, you can provide separate users with remote access to the company site over the VPN.

Reference Environment

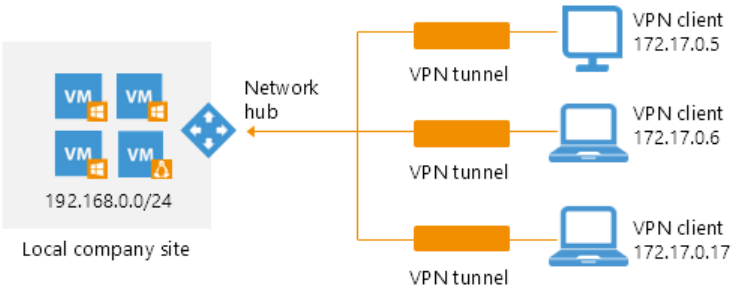
This how-to assumes that your company environment is configured in the following way:

- Local company site: your applications and services are hosted on a local company site.
- Remote users: users who need to gain access to the local company site are working remotely.

In this scenario, you will deploy Veeam PN components in the following way:

- The network hub will be deployed on the local company site.
- You will configure VPN settings on user machines with the help of OpenVPN.

Whenever users need to access resources on the local company site, they will establish a VPN connection to the network hub, that, in its turn, will route requests to machines on the local company site.



Prerequisites

To follow instructions of this how-to, check the following prerequisite:

You must have a VMware vSphere host on the local company site. The network hub is deployed as a virtual appliance and placed on a VMware vSphere host.

Step-By-Step Walkthrough

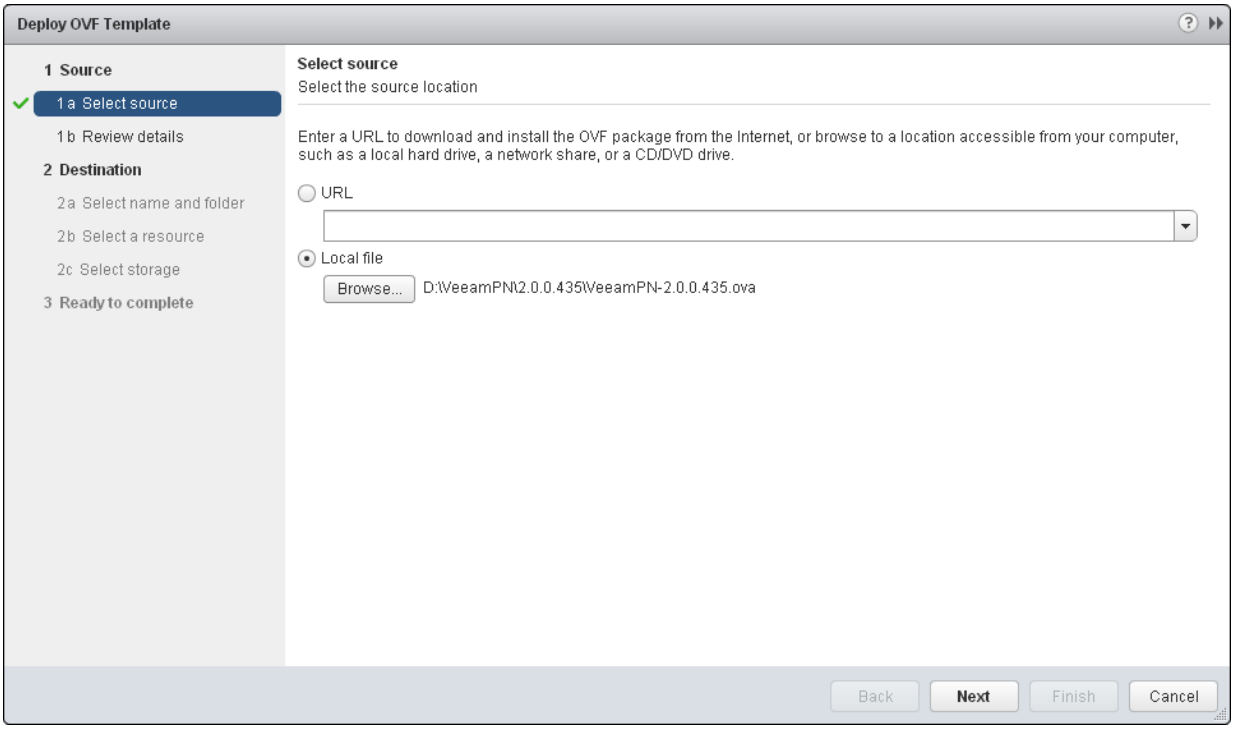
To set up a VPN connection from user machines to the local company site, you will:

1. Deploy the network hub on the local company site.
2. Register clients for user machines in the Veeam PN portal.
3. Configure OpenVPN on user machines.
4. Establish a VPN connection from user machines to the network hub on the local company site.

Step 1. Deploy Network Hub in Local Company Site

The network hub is the core of the VPN infrastructure. If you want to set up a VPN connection from user machines to company resources, you must deploy the network hub on the local company site.

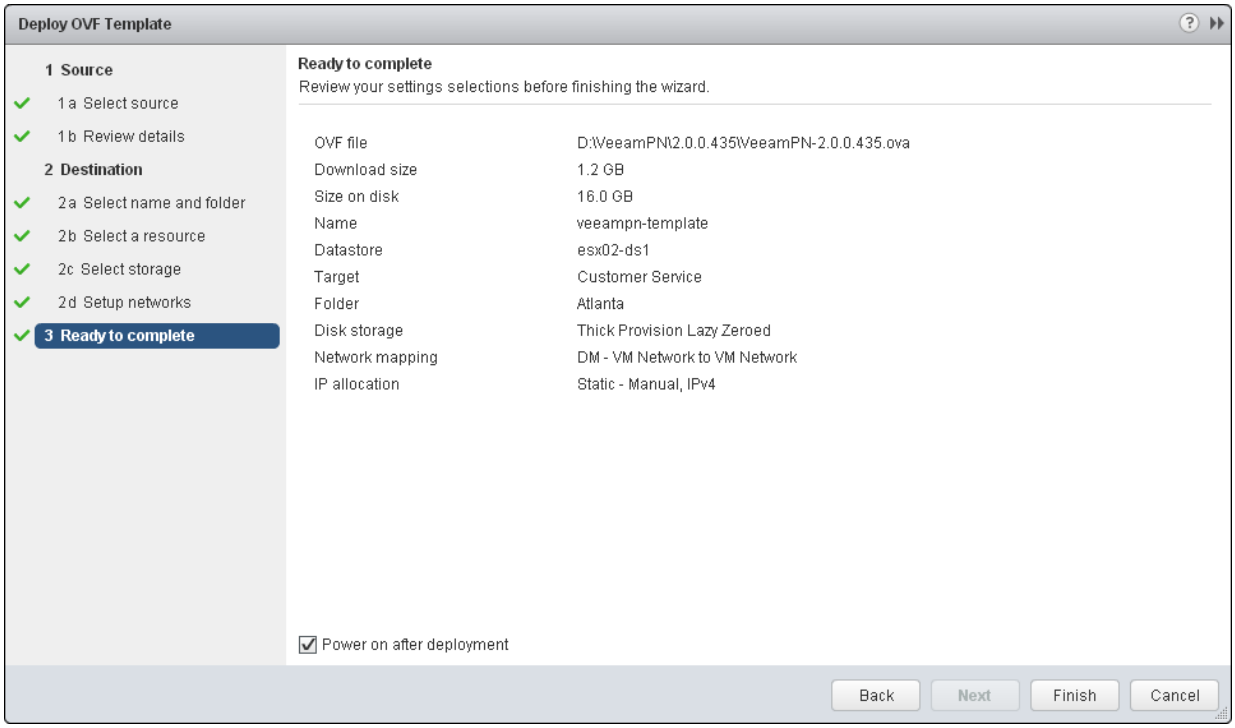
1. Download the Veeam PN OVA package from: https://www.veeam.com/downloads.html and save it in a network shared folder.
2. In VMware vSphere Web Client, open the hosts and clusters inventory list and select a host on which you want to place the network hub.
3. From the menu at the top of the working area, select **Actions** > **Deploy OVF Template**.
4. At the **Select source** step of the wizard, select **Local file**, click **Browse** and browse to the Veeam PN OVA package.



5. Follow the next steps of the wizard and specify network hub deployment settings: datastore on which the network hub disk must be placed, disk format, network to which the network hub must be connected and so on.

6. At the last step of the wizard, select the **Power on after deployment** check box and click **Finish**.

   VMware vSphere will deploy the network hub on the selected host. The deployment process typically takes several minutes. Wait for this process to complete and proceed to network hub configuration.

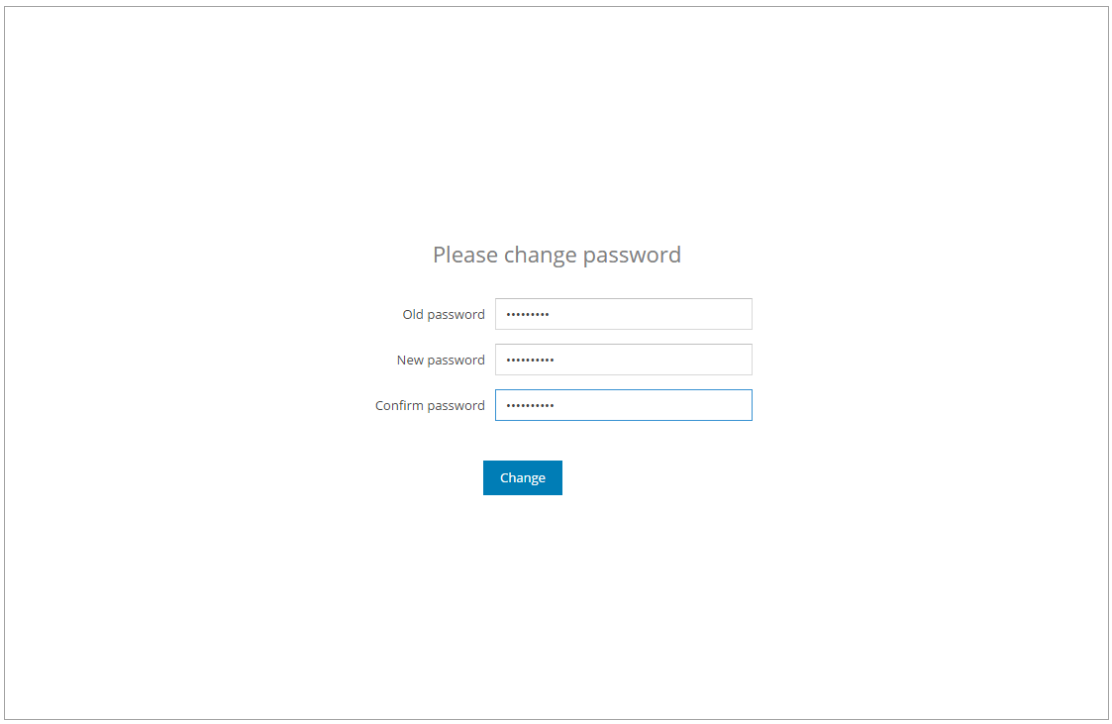


7. In VMware vSphere Web Client, navigate to the **Summary** tab and get an IP address of the network hub.

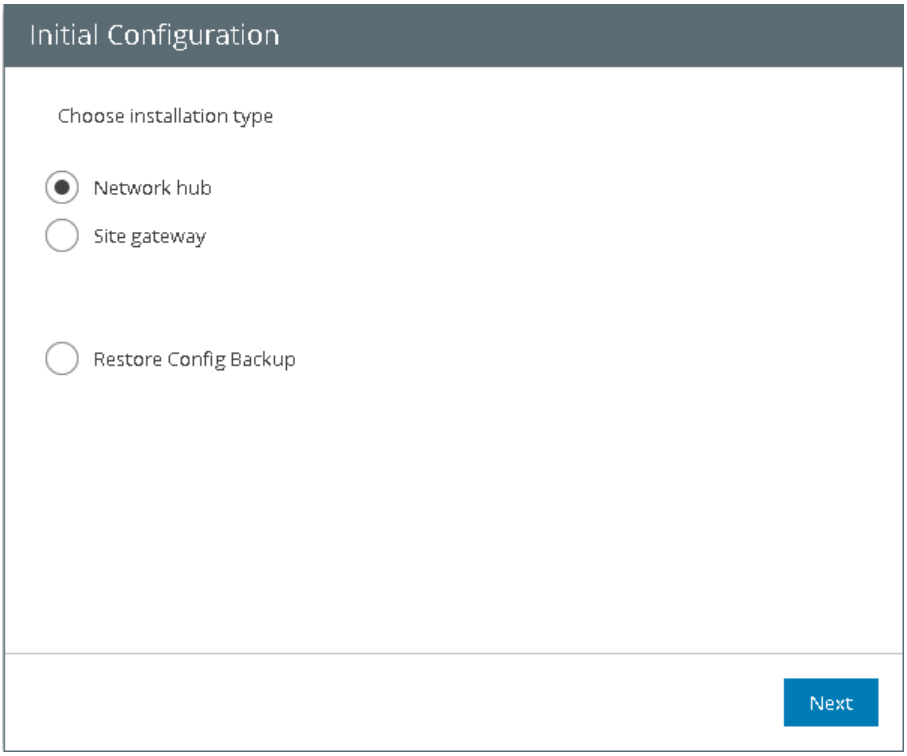
8. In a web browser, access the network hub portal by the following address: `https://<networkhubIP>`.

   The browser will display a warning notifying that the connection is untrusted. Ignore the warning and agree to proceed to the portal.

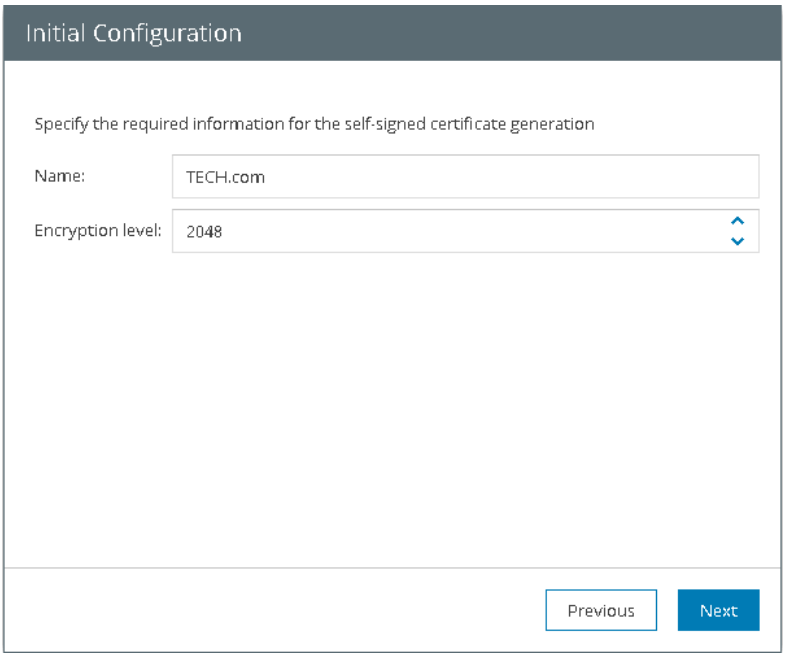
9. At the **Welcome to Veeam PN** screen of the portal, log in to the network hub portal using credentials of the built-in account:
    - Username: *root*
    - Password: *VeeamPN*
10. Click **Login**.
11. When prompted, change the password for the built-in account.



12. At the first step of the **Initial Configuration** wizard, select **Network hub** and click **Next**.



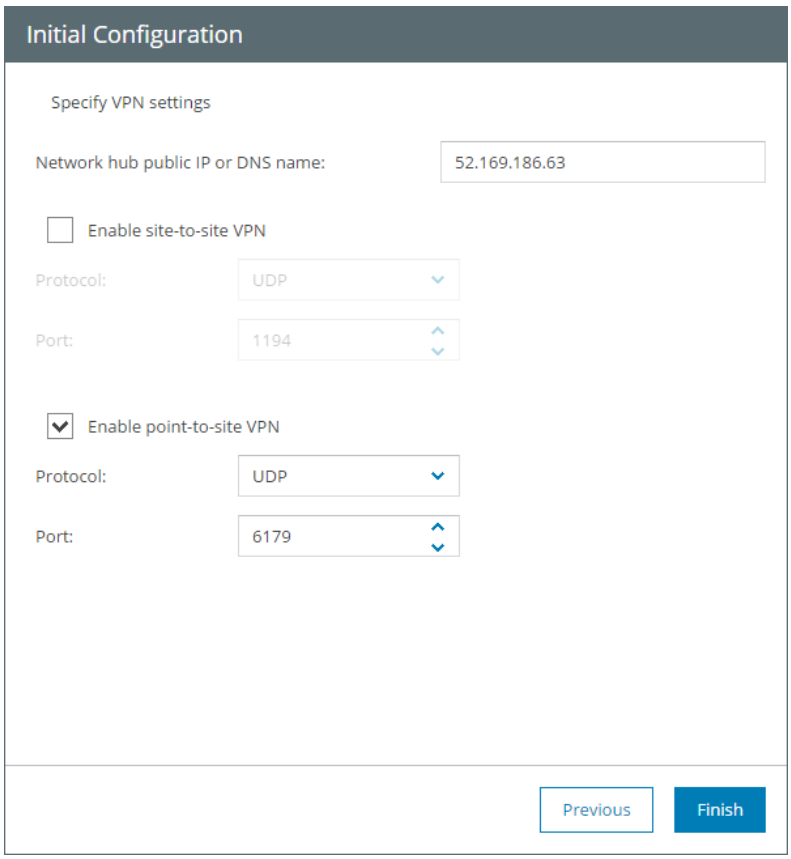
13. Specify parameters for a self-signed certificate that Veeam PN will use to secure communication in the VPN: the certificate key length and click **Next**.



14. After the certificate is generated, click **OK**, then click **Next** to proceed to network hub configuration.

15. In the **Network hub public IP or DNS** name field, specify an IP address or full DNS name for the network hub. The IP address or DNS name must be public and accessible from remote user machines.

16. Select the **Enable point-to-site VPN** check box. In the **Protocol** and **Port** fields, leave default settings.

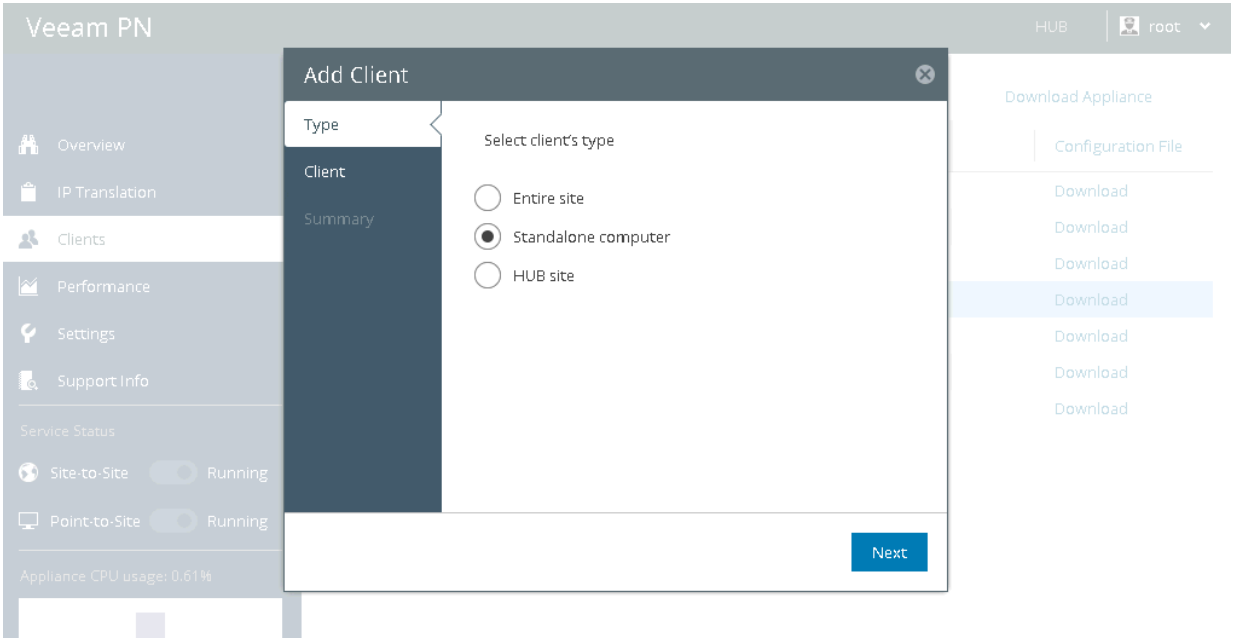


17. Click **Finish**.

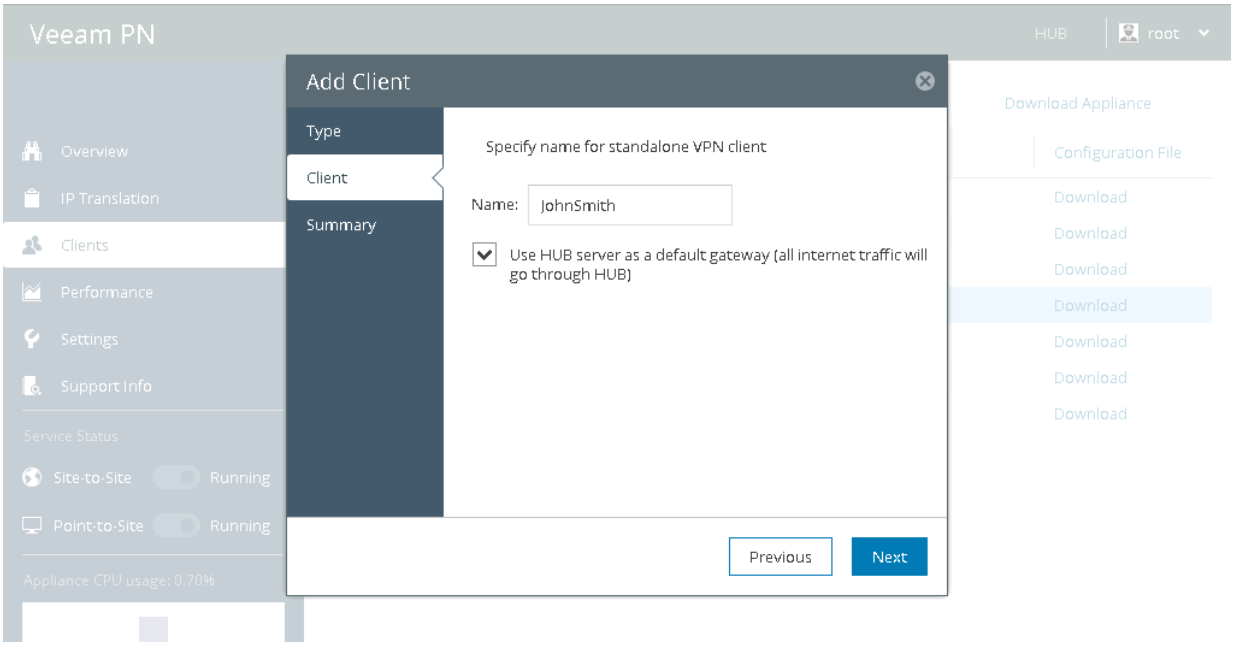
Step 2. Register Clients for User Machines

To provide users with access to company resources, you must register clients for these users in the Veeam PN portal. Veeam PN will generate configuration files for users. You will use these configuration files to set up a VPN connection on user machines.

1. In the Veeam PN portal, in the configuration menu on the left click **Clients**.
2. At the top of the clients list, click **Add**.
3. At the **Type** step of the wizard, select **Standalone computer**.



4. At the **Client** step of the wizard, enter a name for the user machine.
5. Select the **Use HUB server as a default gateway** check box.



6. At the **Summary** step of the wizard, click **Finish**.

Veeam PN will generate an XML file with VPN settings for the user. The XML file will be automatically downloaded to the default downloads folder. Save the downloaded file in a network shared folder accessible from the user machine.

7. Repeat steps 1-5 for all users to whom you want to provide access.

Step 3. Configure OpenVPN on User Machines

To let a user access company resources, you must configure VPN settings on the user machine. To do this, you must use OpenVPN software and configuration file generated by Veeam PN.

To configure OpenVPN on user machines:

1. Download the OpenVPN setup file for the user machine OS from: https://openvpn.net/index.php/open-source/downloads.html.
2. Run the OpenVPN setup file and install the product with default installation settings.
3. Place the client configuration file generated by Veeam PN in a folder where OpenVPN configuration files are stored: `C:\Program Files\OpenVPN\config`.
4. Repeat steps 1-3 for all users to whom you want to provide access.

Step 4. Establish VPN connection from User Machines to Microsoft Azure

To establish a VPN connection from user machines to the local company site:

1. On a user machine, create a batch file with the following command:

   ```
   "openvpn-gui.exe" -- connect "C:\Program Files\OpenVPN\config\client.ovpn"
   ```

   where `C:\Program Files\OpenVPN\bin\openvpn-gui.exe` is a path to the OpenVPN product folder and `C:\Program Files\OpenVPN\config\client.ovpn` is a path to the user machine configuration file.
2. Run the batch file. Veeam PN will establish a connection from the user machine to the network hub.
3. Repeat steps 1-2 for all users to whom you want to provide access.

Result

You have set up a VPN connection from user machines to the local company site. Machines running on the local company site are now accessible to users working remotely.

Install Veeam PN on Ubuntu

You can deploy the Veeam PN appliance in the Microsoft Azure and Amazon AWS marketplaces or download an OVA template from https://www.veeam.com/cloud-disaster-recovery-azure-download.html and deploy it on premises. You can also deploy your own Ubuntu server and install Veeam PN directly from the Veeam Linux Repositories.

> **TIP:**
>
> You can also deploy Veeam PN using an installer script. For details, see Install Veeam PN with Script.

System Requirements

- Ubuntu 18.04
- 1 vCPU (Minimum)
- 1 GB vRAM (Minimum)
- 16 GB of Hard Drive space
- External Network Connectivity

Installing Veeam PN on Ubuntu

To install Veeam PN on an Ubuntu machine, do the following. Note that you must have superuser rights.

1. Download and add the Veeam Software Repository Key to your system:

```
curl -k http://repository.veeam.com/keys/veeam.gpg | apt-key add -
```

2. Add Veeam PN to the list of sources in APT and run an APT update.

```
echo "deb [arch=amd64] http://repository.veeam.com/pn/public pn stable" >
/etc/apt/sources.list.d/veeampn.list
apt-get update
```

3. Add an apt repository for WireGuard.

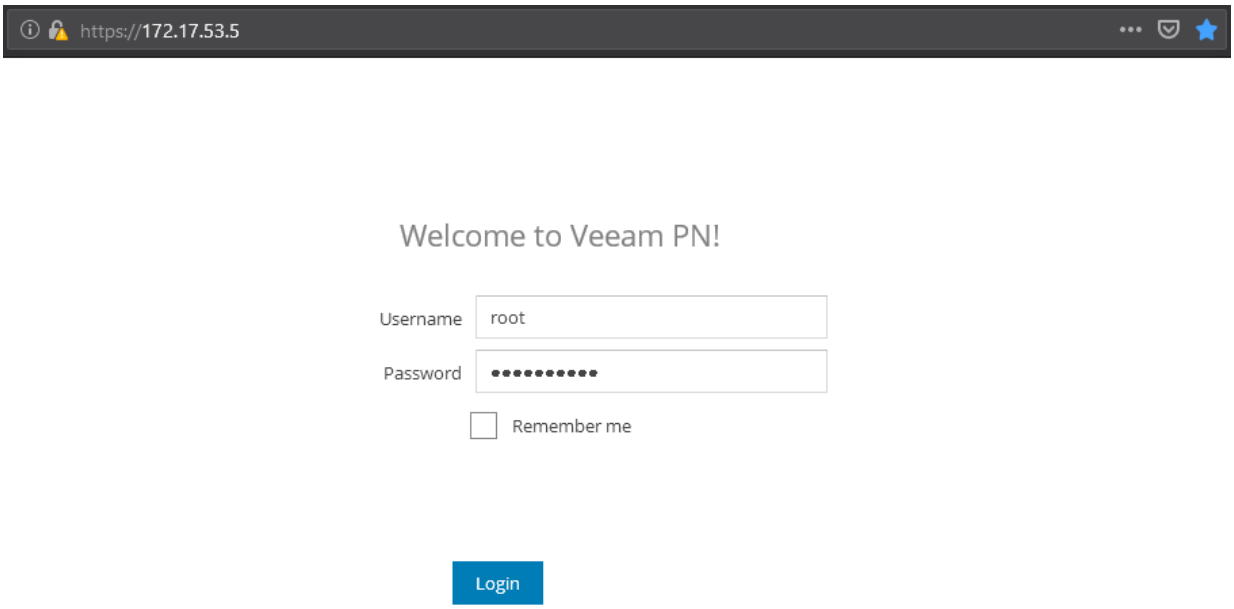
```
apt-add-repository ppa:wireguard/wireguard
```

4. Install two packages: the Server and UI components.

```
apt-get -y install veeam-vpn-ui veeam-vpn-svc
```

   Apt-get will list a significant amount of dependencies that must be installed as well. During the installation of packages, you may be asked to overwrite existing IPTables rules.

5. After the installation of packages is complete, you can log in to the Veeam PN web portal. To open Veeam PN web portal, open `https://<Veeam_PN_server_IP_address>` in a web-browser. Use your root user credentials to log in to the web portal.



Install Veeam PN with Script

On Ubuntu 18.04 machine, you can deploy Veeam PN using the installer script. If you want to deploy Veeam PN using the script, you don't need to download the Veeam PN image. The script will download all required files from Linux repository. You can download the installer script (`VeeamPN-installer.run.sh`) at: https://www.veeam.com/veeampn-download.html.

Before you deploy Veeam PN, see system requirements.

To install Veeam PN, run the installer script with the required parameters.

```
sudo bash ./VeeamPN-installer.run.sh -- -y -c -f
```

Parameter	Description
-c (--configure-system)	Pre-configures the system before installation: configures ssh settings, installs updates.
-f (--force)	Forces the installation: ignores pre-checks of additional tools (Apache, WireGuard, etc.)
-y (--quiet)	Switches to quiet mode (unattended installation): the wizard will not ask you to confirm installation of required tools.
-v (--version)	Shows version information.
-h (--help)	Shows help.

Install Free SSL Certificate on Veeam PN Appliance Host

During the installation, Veeam PN generates a self-signed certificate. To mitigate the risk of MITM attacks, you can obtain and install a free SSL certificate from Let's Encrypt.

To install the certificate, do the following:

1. Open the console of Veeam PN appliance machine.
   - [VMware vSphere] Open the TTY console of the VM where Veeam PN appliance is deployed.
   - [Microsoft Azure] In PuTTY, use the Veeam PN appliance hostname to connect to the console.
2. Add a PPA (Personal Package Archive) to the list of repositories and install Certbot:

   ```
   sudo apt-get update
   sudo apt-get install software-properties-common
   sudo add-apt-repository universe
   sudo add-apt-repository ppa:certbot/certbot
   sudo apt-get update
   sudo apt-get install certbot python-certbot-apache
   ```

3. Certbot has an Apache plugin that automates certificate installation. The plugin will install an SSL certificate and automatically edit the machine configuration to server the installed certificate.

   To install an SSL certificate, run the following command:

   ```
   sudo certbot --apache
   ```

Automated Renewal of SSL Certificate

Let's Encrypt certificates last for 90 days. You can enable the cron job of Certbot that will renew your SSL certificate automatically before it expires.

```
sudo certbot renew --dry-run
```

Reference

For detailed instructions, see: https://certbot.eff.org/lets-encrypt/ubuntuxenial-apache.

Improve Veeam PN Performance

The **txqueuelen** parameter of an interface in the Linux kernel. It limits the number of packets in the transmission queue in the interface's device driver.

The default value of **txqueuelen** is 1000 for Veeam PN appliance server deployed from Azure Marketplace or from OVA template. Values of up to 8000 have been used successfully to further improve performance. If a host is low performance or has slow links, having too big txqueuelen may disturb interactive performance.

To change the value of **txqueuelen**, log in to the Veeam PN appliance TTY console and run the following command:

```
ifconfig ens160 txqueuelen 4000
```

Revision History

Revision #	Date	Description of Changes
REV 3	26 Nov 2019	Updated for Veeam PN 2.1: Added support of Veeam PN deployment in Amazon AWS.
REV 2	14 May 2019	Updated for Veeam PN 2.0: Added support of WireGuard technology and DNS forwarding.
REV 1	13 Dec 2017	Initial version of the document for Veeam PN 1.0.