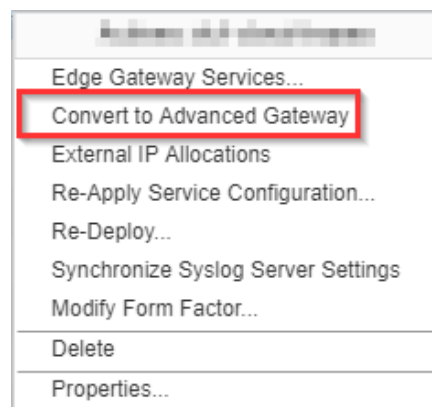


How to Configure a SSL VPN in vCloud Director

Please note before proceeding with this Knowledge Base article, your vCloud Organization must have the Advanced Edge Gateway enabled in vCloud.

You can tell if you have an Advanced Gateway or not, by right clicking on your organization's Edge Gateway and confirming if "Convert to Advanced Gateway" is available. If it is available, please choose "Convert to Advanced Gateway" – this will cause a very short interruption (30 Seconds) in connectivity to the servers.

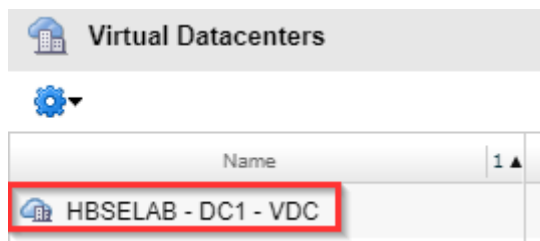


Navigate to the SSL-VPN-Plus Screen

Proceed to the "Administration" tab:



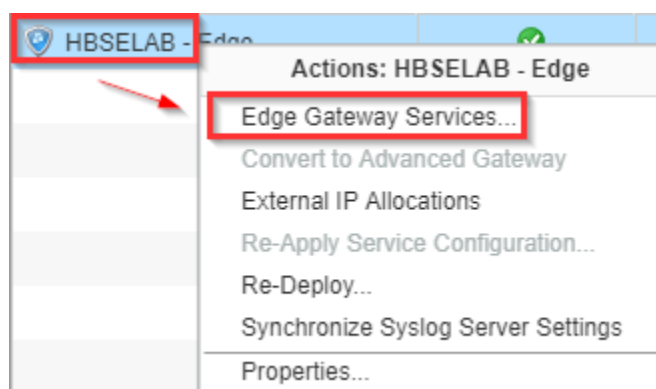
Select (left-click) your Organization's Virtual Datacenter:



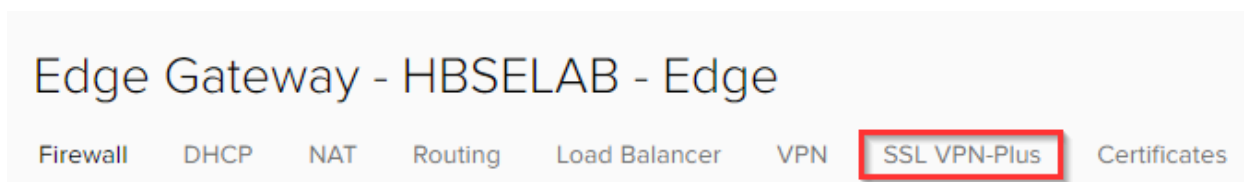
Select the “Edge Gateways” tab:



Right-click on your Edge Gateway and select “Edge Gateway Service...”



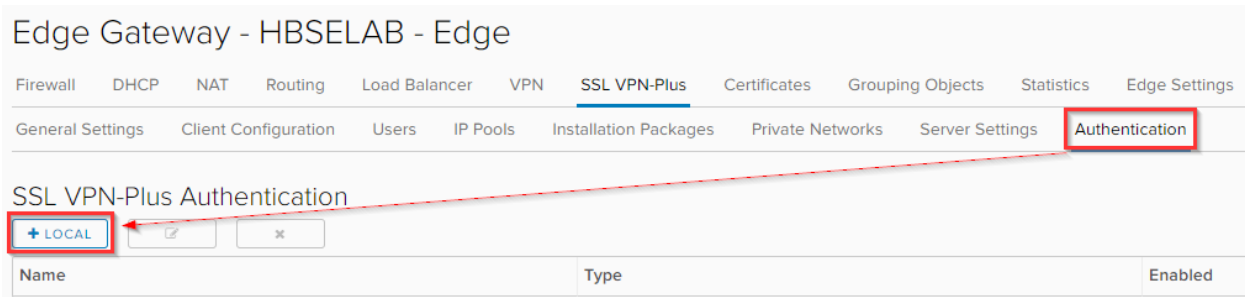
A new tab will open in your browser. You can now select the “SSL VPN-Plus” tab:



Configure an Authentication Server

Before other settings can be configured, an Authentication server must be enabled.

Select the “Authentication” tab, and then select “+ Local”:



The password policy is enabled by default, if you wish to keep one, leave the switch toggled and configure the specific password policies you would like. If you do not wish to have one, toggle the password policy off. Please note, these passwords will be separate from domain or local credentials on the user's machine.

The 'Add Authentication Server' dialog box is shown. It contains the following settings:

- PASSWORD POLICY**
- Enable password policy:** Toggled on (green switch).
- Password Length *:** From 1 to 63.
- Minimum no. of alphabets:** (Empty field)
- Minimum no. of digits:** (Empty field)
- Minimum no. of special characters:** (Empty field)
- Password should not contain user ID:** Toggled off (grey switch).
- Password expires in *:** 30 Day(s).
- Expiry notification in *:** 25 Day(s).

Configure the account lockout policy (if you desire one) as you like. If you do not wish to have a lockout policy, then toggle it off.

The retry duration denotes the number of minutes the retry count will be kept track of. The lockout duration denotes the number of minutes the user will be locked out if they have too many unsuccessful attempts during the duration period.

Finally select the toggle to enable the Authentication Server, and select “KEEP” to save your configuration.

Add Authentication Server

ACCOUNT LOCKOUT POLICY

Enable account lockout policy ☒

Retry Count * 3
User account will get locked after specific number of unsuccessful retries.

Retry Duration * 3

Lockout Duration * 1

STATUS

Enabled ☒

DISCARD KEEP

You will now see you have an authserver, the number denoted is generic. Do ensure that it is enabled.

Edge Gateway - HBSELAB - Edge

Firewall DHCP NAT Routing Load Balancer VPN **SSL VPN-Plus** Certificates Grouping Objects Statistics Edge Settings

General Settings Client Configuration Users IP Pools Installation Packages Private Networks Server Settings **Authentication**

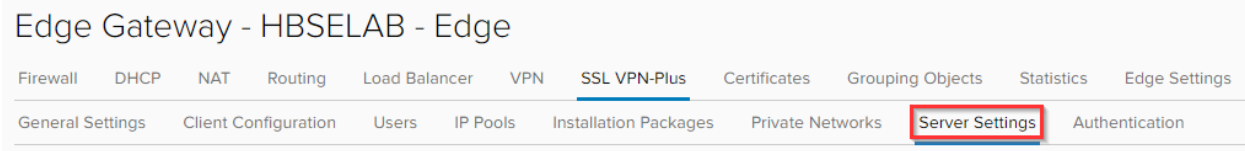
SSL VPN-Plus Authentication

+ LOCAL EDIT X

Name	Type	Enabled
authserver-62	Local	<input checked="" type="checkbox"/>

Configure the SSL VPN Server Settings

On the SSL VPN-Plus tab, select “Server Settings”:



Toggle the button to enable the server.

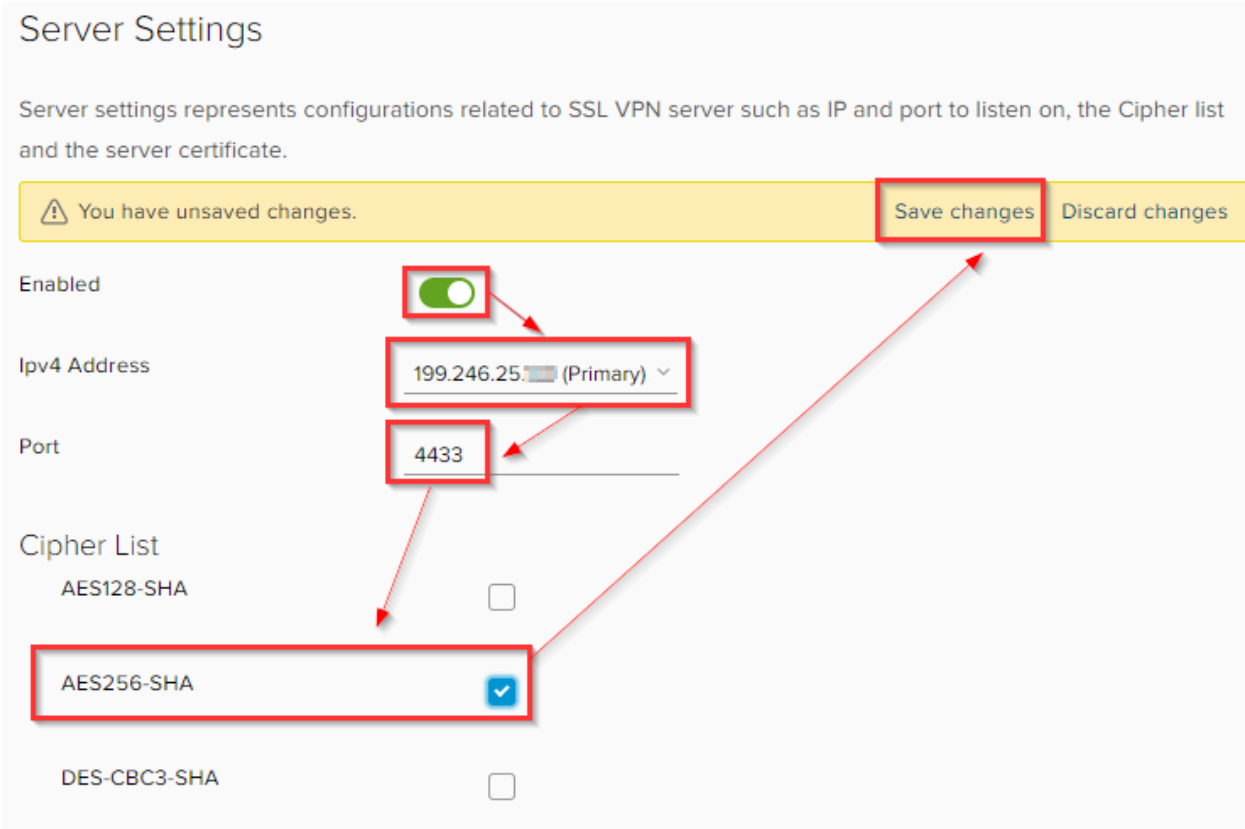
Then use the drop down to select your desired IP address from the drop-down menu.

(Optional) Enter a TCP port number.

Please note – The TCP port number is used by the SSL client installation package. By default, the system uses port 443, which is the default port for HTTPS/SSL traffic. Even though a port number is required, you can set any TCP port for communications. As many of our customers use 443 for other traffic, we recommend setting an alternate port.

Select the encryption method from the Cipher List. (We recommend no less than AES256).

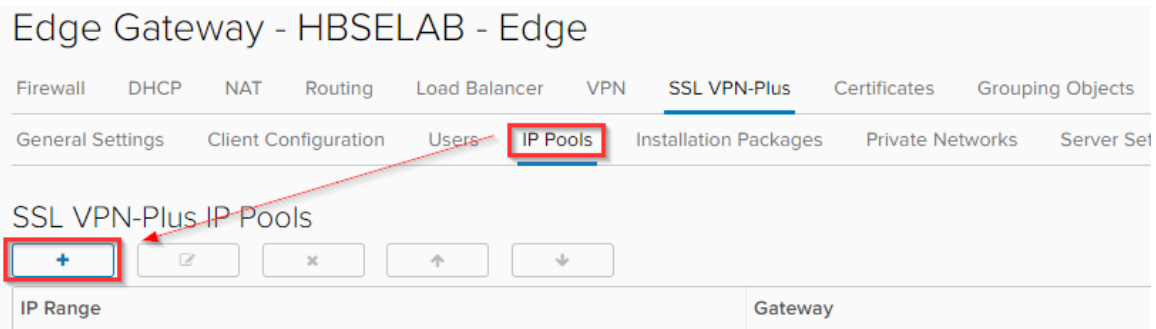
Finally, select “Save Changes”.



Create an IP Pool for Use with SSL VPN-Plus on an Edge Gateway

The SSL VPN assigns an IP address to the remote users from the IP pools based on the pool setup in the following steps.

On the SSL VPN-Plus tab, select “IP Pools” and select the “+” to create a new pool.



Input the range you wish to use for the SSL VPN pool, please note, you cannot use the IP ranges currently in use in vCloud. As an example, if your current Cloud LAN pool is 10.10.1.0/24, you cannot use this, you would use a different range such as 10.10.2.0/24.

Here is the range used in the example: 10.20.30.10-10.20.30.250 – This leaves us with 240 free IPs.

You must also input the netmask, gateway, enable the pool. The DNS entries are optional. Once all fields are filled out, select “Keep”. We will need to make a firewall entry for this pool, this will be done in another step.

Create New IP Pool

IP Range * 10.20.30.10-10.20.30.250

Netmask * 255.255.255.0

Gateway * 10.20.30.1

This will add an IP address in na0 interface

Description

Status ☒

Advanced

Primary DNS 8.8.8.8

Secondary DNS 8.8.4.4

DISCARD KEEP

Add a Private Network for Use with the SSL VPN-Plus

The private networks are the ones that the SSL VPN-Plus users will be accessing. So the Cloud LAN. You can confirm this network under “Org VDC Networks” back on the main vCloud Administration page we left behind after accessing the Edge Gateway.

vApps

vApp Templates

Media & Other

Storage Policies

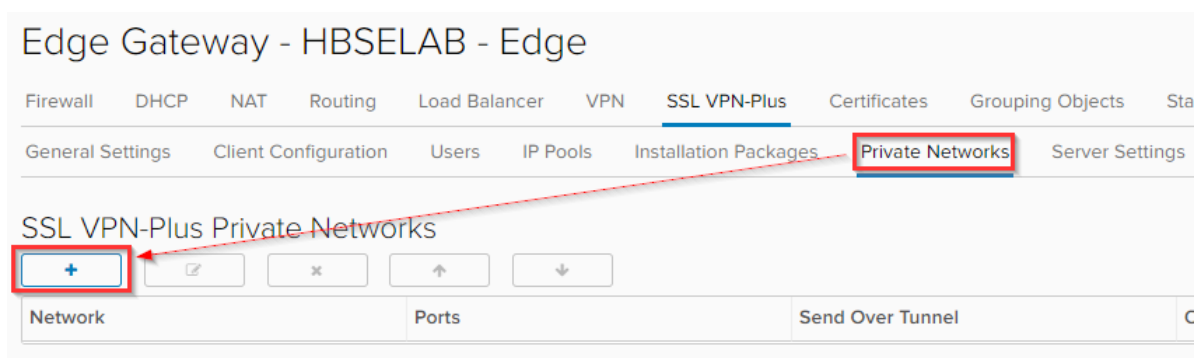
Edge Gateways

Org VDC Networks

Affinity Rules

Name	Status	Gateway Address	Type	Interface Type	Connected To
HBSELAB...		10.10.10.1/24	Routed	Internal	HBSELAB - Edge

In the Edge Gateway, under the SSL VPN-Plus tab, select the “Private Networks” tab:



Edge Gateway - HBSELAB - Edge

Firewall DHCP NAT Routing Load Balancer VPN **SSL VPN-Plus** Certificates Grouping Objects Sta

General Settings Client Configuration Users IP Pools Installation Packages **Private Networks** Server Settings

SSL VPN-Plus Private Networks

+ - x ↕

Network	Ports	Send Over Tunnel	C
---------	-------	------------------	---

Input the IP range desired (per the Org VDC Network). You can optionally specify if traffic should be sent over the tunnel or not (it should be) (this is not where you configure split-tunnel), and what ports can be used in the tunnel. Leaving the ports blank leaves access unrestricted.

Add Private Network

Network * 10.10.10.0/24

Network should be entered in CIDR format e.g. 192.169.1.0/24

Description

Send Traffic Over Tunnel

☒ Enable TCP Optimization

Ports

Status ☒

[DISCARD](#) [KEEP](#)

After you have select “Keep”, select “Save changes”:

Edge Gateway - HBSELAB - Edge

Firewall DHCP NAT Routing Load Balancer VPN **SSL VPN-Plus** Certificates Grouping Objects Statistics Edge Settings

General Settings Client Configuration Users IP Pools Installation Packages **Private Networks** Server Settings Authentication

SSL VPN-Plus Private Networks

You have unsaved changes. [Save changes](#) [Discard changes](#)

[+](#) [✎](#) [✕](#) [↑](#) [↓](#)

Network	Ports	Send Over Tunnel	Optimize Traffic	Status
10.10.10.0/24	-	Enabled	Enabled	Enabled

Configure the SSL VPN-Plus Client

Proceed to “Client Configuration” and ensure you are happy with the settings. The main setting here is if it’s a “Split” or “Full” tunnel. In split tunnel mode, only the VPN traffic flows through the edge gateway. In full tunnel mode, the edge gateway becomes the default gateway for the remote user and all traffic, such as VPN, local, and Internet, flows through the edge gateway.

If you select full tunnel mode, enter the IP address for the default gateway used by the clients of the remote users and, optionally, select whether to exclude local subnet traffic from flowing through the VPN tunnel.

By default “auto reconnect” is already enabled.

In most use cases we see customers use “Split” as the SSL VPN is typically just to access the cloud servers.

Edge Gateway - HBSELAB - Edge

Firewall DHCP NAT Routing Load Balancer VPN **SSL VPN-Plus** Certificates Grouping Objects Statistics Edge Settings

General Settings **Client Configuration** Users IP Pools Installation Packages Private Networks Server Settings Authentication

SSL VPN-Plus Client Configuration

Tunneling mode: ☐ Full ☒ Split

Exclude local subnets ☐

Default gateway:

Enable auto reconnect ☒

Client upgrade notification ☐

If you do make a change you must save it:

Edge Gateway - HBSELAB - Edge

Firewall DHCP NAT Routing Load Balancer VPN **SSL VPN-Plus** Certificates Grouping Objects Statistics Edge Settings

General Settings **Client Configuration** Users IP Pools Installation Packages Private Networks Server Settings Authentication

SSL VPN-Plus Client Configuration

You have unsaved changes. **Save changes** Discard changes

Tunneling mode: ☐ Full ☒ Split

Exclude local subnets ☐

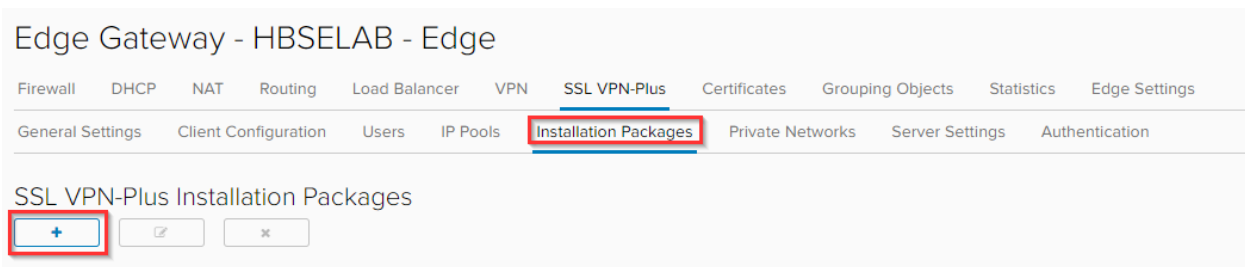
Default gateway:

Enable auto reconnect ☒

Client upgrade notification ☐

Configure Installation Packages

Proceed to the “Installation Packages” tab to setup the SSL VPN-Plus client. Select “+” to configure the package.

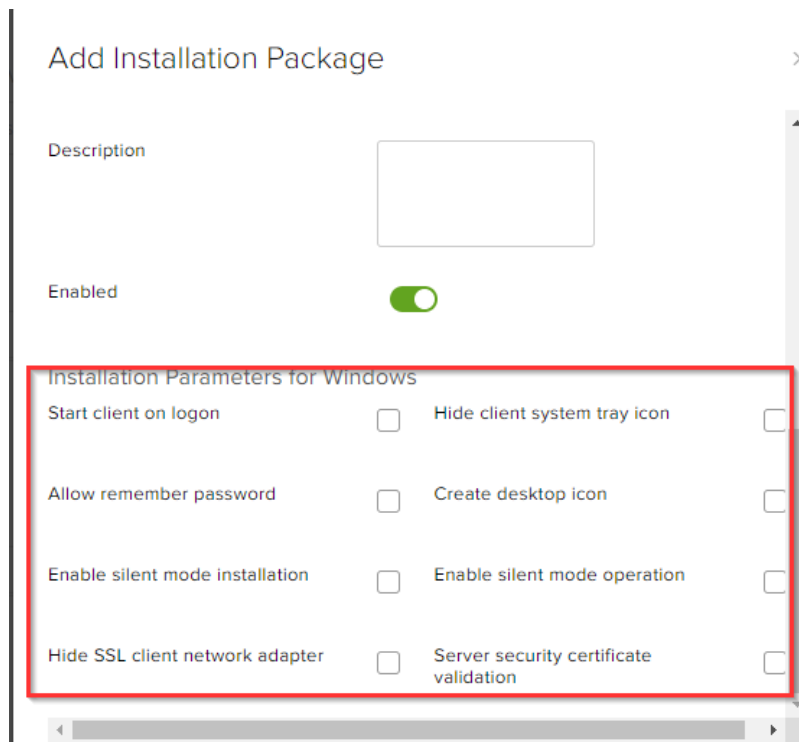


You will need to input a profile name, input your Gateway IP, and Port (this was seen under “Configure the SSL VPN Server Settings”).

Additionally you can configure if the client is available for Mac or Linux users:

The screenshot shows a dialog box titled "Add Installation Package" with a close button (X) in the top right corner. Inside the dialog, there is a text input field for "Profile Name *" containing the text "HB-SE-SSLVPN". Below this field are two buttons: a blue button with a "+" sign and a button with an "x" icon. Below the buttons is a table with two columns: "Gateway" and "Port". The "Gateway" column contains the value "199.246.25." (highlighted with a red box). The "Port" column contains the value "4433" (highlighted with a red box). Below the table, there is a section titled "Create installation packages for". Under this section, there are three rows: "Windows" with a checked checkbox, "Linux" with an unchecked checkbox, and "Mac" with an unchecked checkbox.

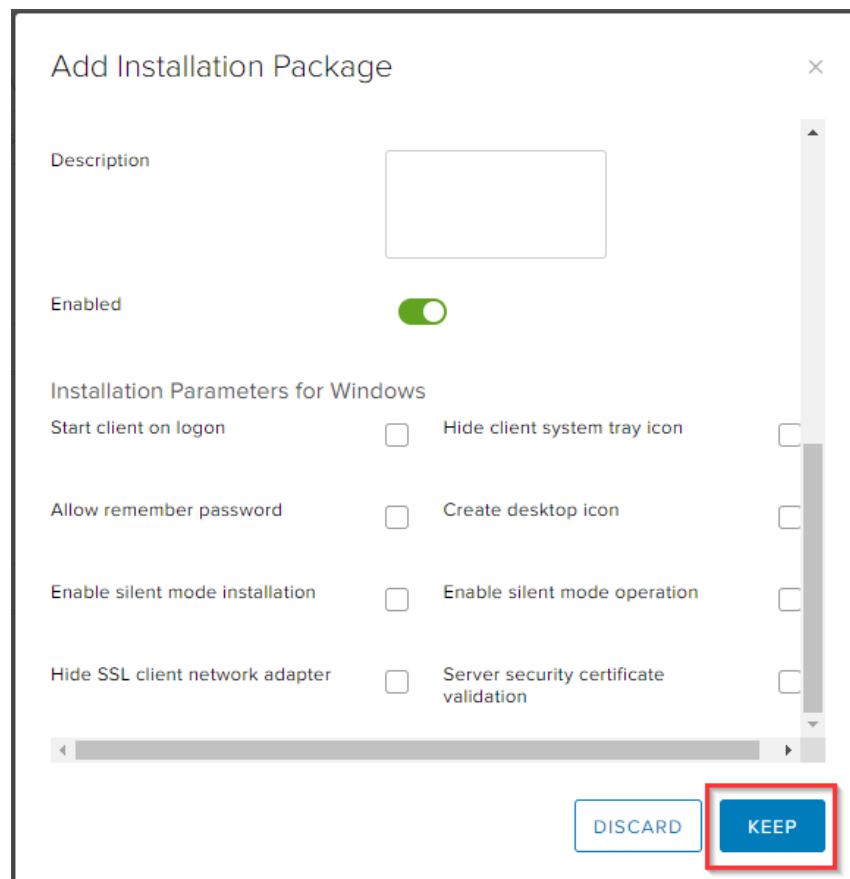
Further down there are also a number of settings that control how the client behaves on the user's machine.



The screenshot shows a dialog box titled "Add Installation Package" with a close button (X) in the top right corner. It contains a "Description" text area, an "Enabled" toggle switch (which is turned on), and a section titled "Installation Parameters for Windows" enclosed in a red rectangular box. This section contains eight checkboxes arranged in two columns:

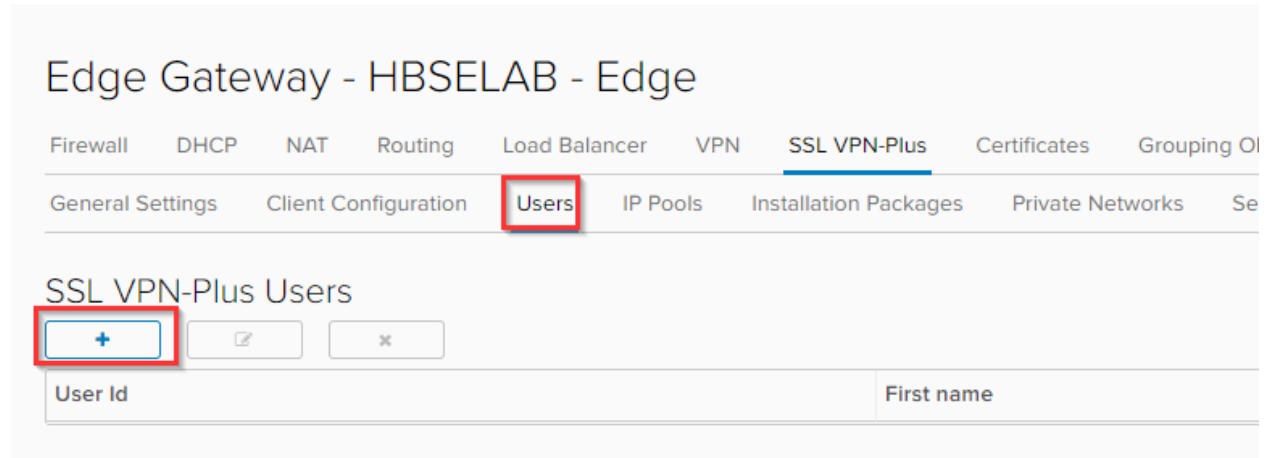
Parameter	Checkbox
Start client on logon	<input type="checkbox"/>
Hide client system tray icon	<input type="checkbox"/>
Allow remember password	<input type="checkbox"/>
Create desktop icon	<input type="checkbox"/>
Enable silent mode installation	<input type="checkbox"/>
Enable silent mode operation	<input type="checkbox"/>
Hide SSL client network adapter	<input type="checkbox"/>
Server security certificate validation	<input type="checkbox"/>

Once you have chosen your settings, you will select "Keep" to save them:



This screenshot shows the same "Add Installation Package" dialog box as the previous one, but with the "KEEP" button highlighted by a red rectangular box. The "KEEP" button is located at the bottom right of the dialog, next to a "DISCARD" button. The "Installation Parameters for Windows" section is still visible and contains the same eight checkboxes as in the previous image.

Proceed to the “Users” tab and select “+” to add a user.





The screenshot shows the configuration interface for an Edge Gateway, specifically the 'SSL VPN-Plus' section. The 'Users' tab is selected and highlighted with a red box. Below the tab, there is a section titled 'SSL VPN-Plus Users' with a red box around the '+' button to add a new user. The interface also shows other tabs like Firewall, DHCP, NAT, Routing, Load Balancer, VPN, Certificates, and Grouping. Below the 'Users' tab, there are buttons for 'General Settings', 'Client Configuration', 'IP Pools', 'Installation Packages', 'Private Networks', and 'Se'.

Edge Gateway - HBSELAB - Edge

Firewall DHCP NAT Routing Load Balancer VPN **SSL VPN-Plus** Certificates Grouping OI

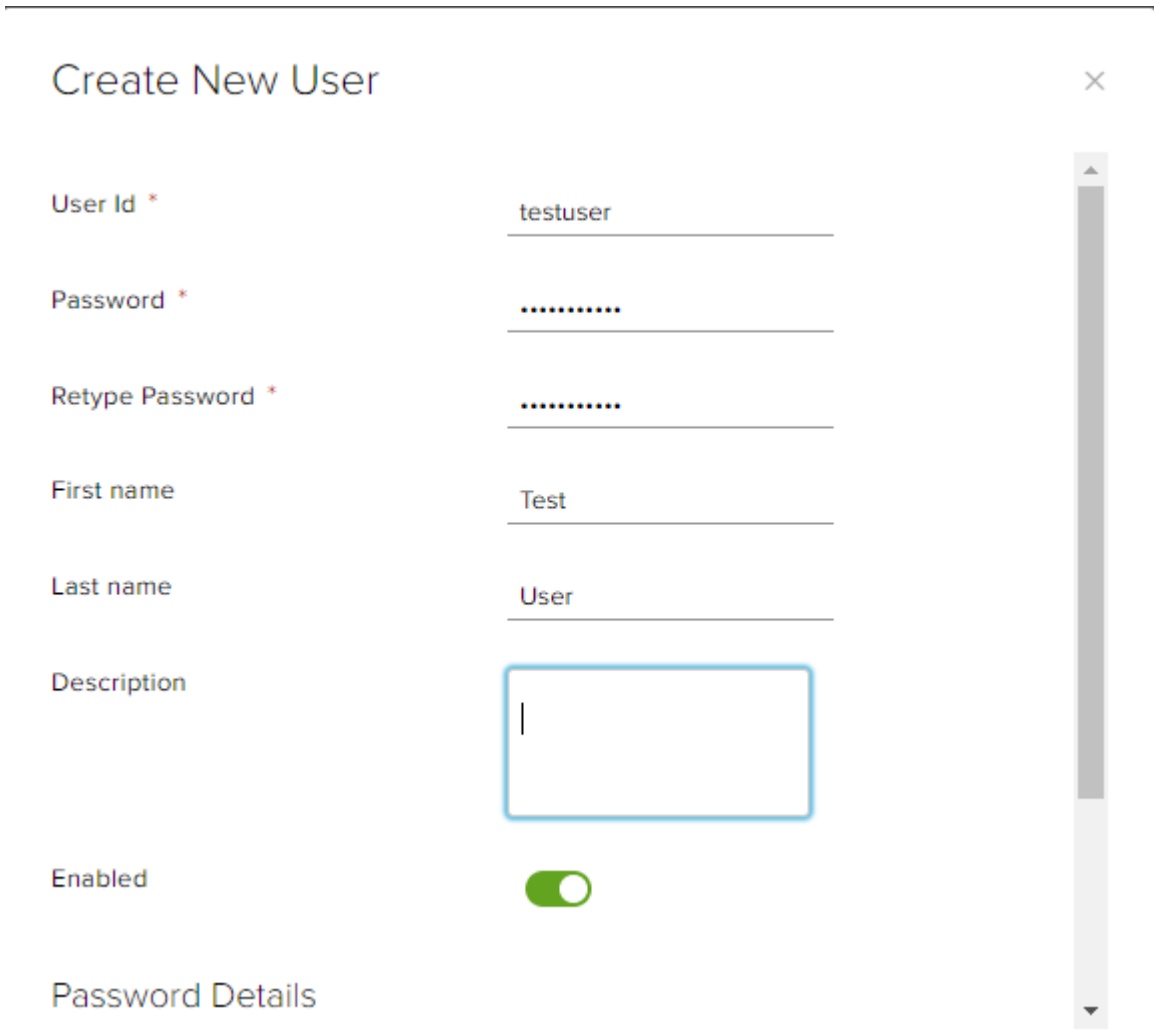
General Settings Client Configuration **Users** IP Pools Installation Packages Private Networks Se

SSL VPN-Plus Users

+  

User Id	First name
---------	------------

Input the user information, including their first password. Depending how you configure settings here they may need to change their password after first login.



The screenshot shows the 'Create New User' dialog box. It contains fields for 'User Id *' (testuser), 'Password *' (masked with dots), 'Retype Password *' (masked with dots), 'First name' (Test), 'Last name' (User), 'Description' (empty), and 'Enabled' (toggle switch). The 'Password Details' section is also visible at the bottom.

Create New User

User Id * testuser

Password *

Retype Password *

First name Test

Last name User

Description

Enabled ☒

Password Details

You can chose at this step to force them to change the password at next login. Select “Keep” to keep the user settings.

Create New User

First name

Test

Last name

User

Description

Enabled

☒

Password Details

Password never expires

☐

Allow change password

☒

Change password on next login

☐

DISCARD

KEEP

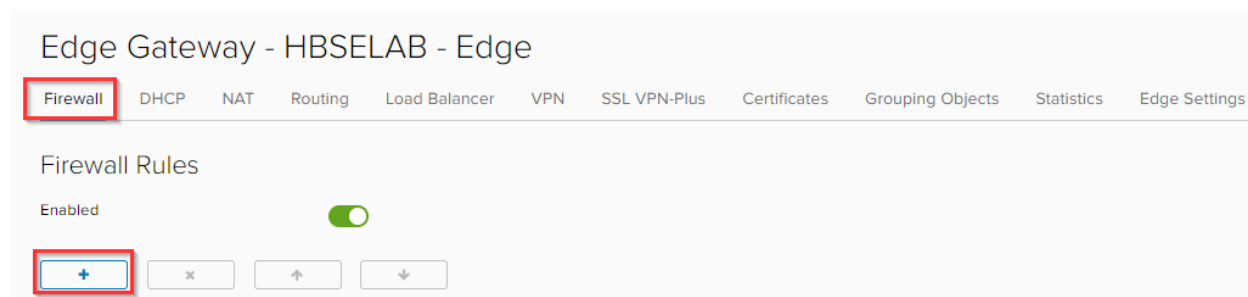
Repeat the above step until all your users are created.

Modify the Firewall to Allow Traffic to Traverse

Finally, all the SSL VPN-Plus settings are configured. The firewall rules will need to be modified to allow traffic to traverse between the IP Pool of the SSL VPN and the Private Network.

Other rules would have been created by default and you will see them in the firewall at this time.

Select “+” to create a new rule.



Name the rule, and under “Source” select “IP”

No.	Name	Type	Source	Destination
2 ✓	SSL VPN to Any	User	Any IP +	Any

Input your IP Pool range here, and select “Keep”:

Source IP Address

Value:

10.20.30.0/24

Valid values can be IP address, CIDR, IP range or the keyword any.

DISCARD

KEEP

Repeat this step and add the Private IP pool (Cloud LAN). It should look like the below (except for your IPs of course). Next do the same for “Destination”:

No.	Name	Type	Source	Destination
2 ✓	SSL VPN to Any	User	10.20.30.0/24 10.10.10.0/24	Any



You can restrict the port to those on your cloud server, or leave it open so any port can be accesses by an SSL VPN user. In the below example, we’ve left it as “Any”. “Save changes” once your rule is complete.

Firewall Rules

⚠ This rule set has unsaved changes. Save to start deploying.

Save changes Discard changes

Enabled ☒

+ × ↑ ↓

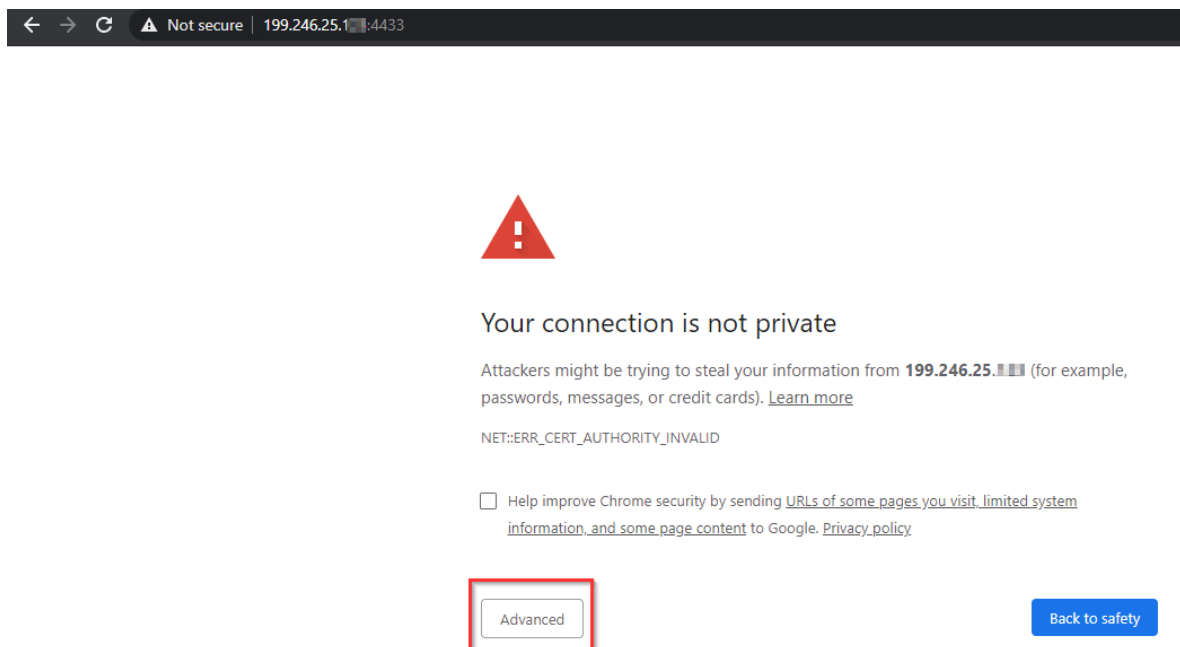
Show only user-defined rules ☐

No.	Name	Type	Source	Destination	Service	Action
2 ✓	SSL VPN to Any	User	10.20.30.0/24 10.10.10.0/24	10.10.10.0/24 10.20.30.0/24	Any	Accept

Have Users Download and Use the Client

Finally, users can now download and use the client. You will need the download URL for them. This will be `https://<gatewayIP>:<gatewayport>` that was set during the installation package setup. (See below).

The webpage will look like the below. Have the user select “Advanced”



And then select “Proceed to IP”:



Your connection is not private

Attackers might be trying to steal your information from **199.246.25.100** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

☐ Help improve Chrome security by sending [URLs of some pages you visit, limited system information, and some page content](#) to Google. [Privacy policy](#)

Hide advanced

Back to safety

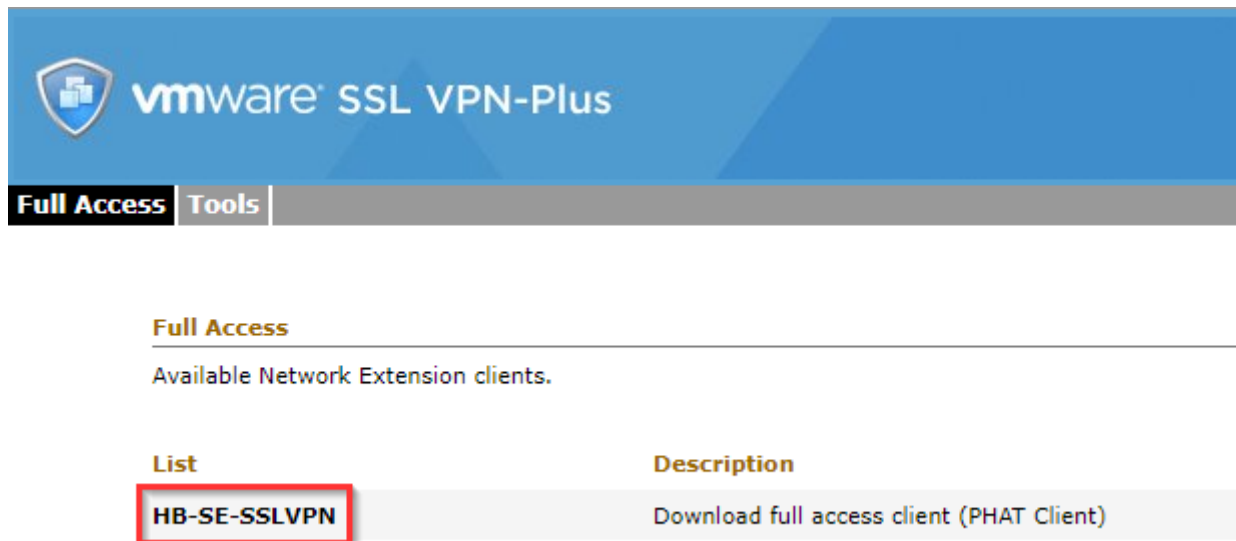
This server could not prove that it is **199.246.25.100**, its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to 199.246.25.100 \(unsafe\)](#)

They can then login with the credentials you provide them:



They can then click to download the client:

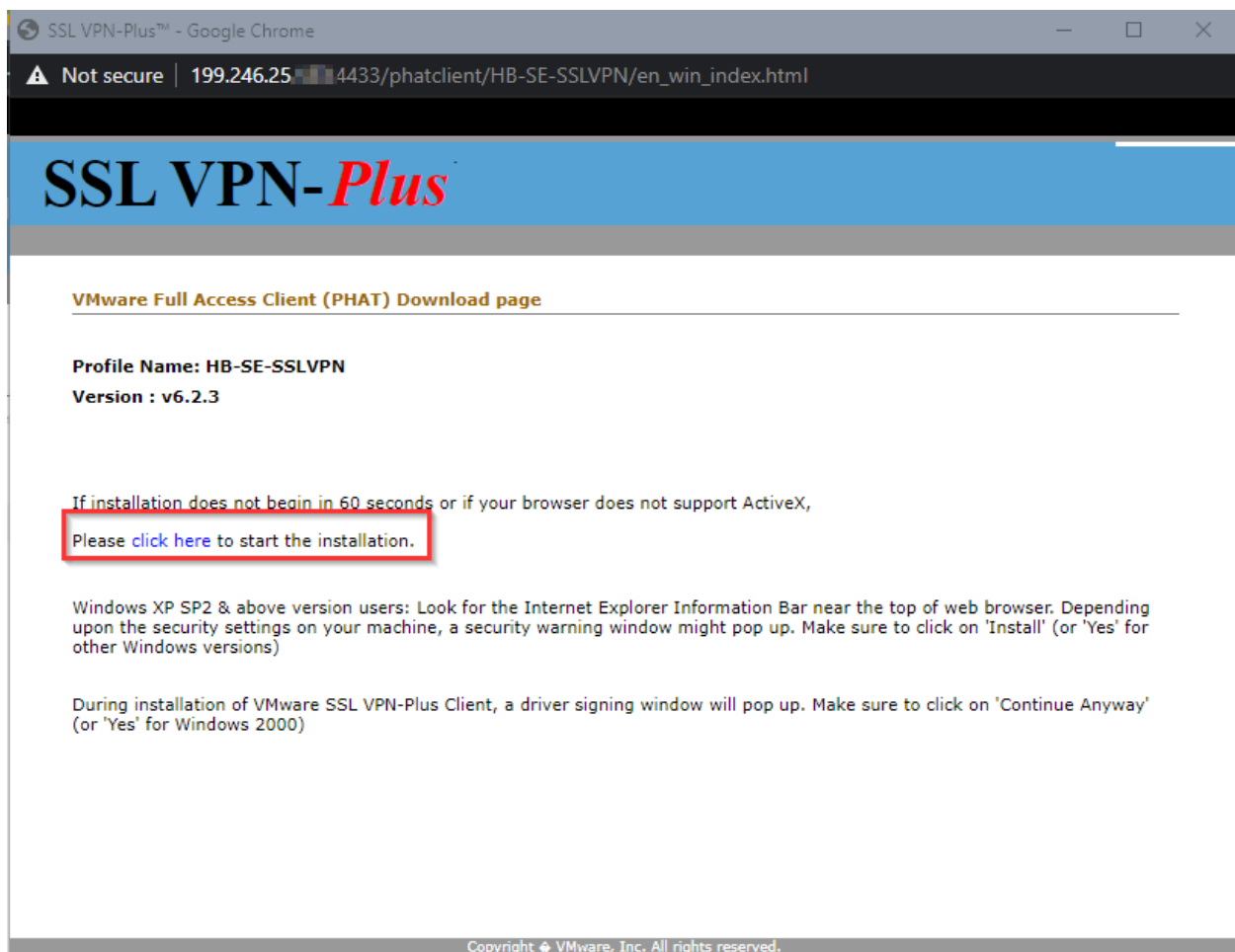


Full Access

Available Network Extension clients.

List	Description
HB-SE-SSLVPN	Download full access client (PHAT Client)

This will open a pop up window, where the download will either begin, or they can select to start it manually:



SSL VPN-Plus™ - Google Chrome

Not secure | 199.246.25.4433/phatclient/HB-SE-SSLVPN/en_win_index.html

SSL VPN-Plus

VMware Full Access Client (PHAT) Download page

Profile Name: HB-SE-SSLVPN
Version : v6.2.3

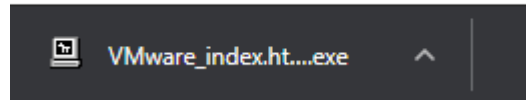
If installation does not begin in 60 seconds or if your browser does not support ActiveX,
Please [click here](#) to start the installation.

Windows XP SP2 & above version users: Look for the Internet Explorer Information Bar near the top of web browser. Depending upon the security settings on your machine, a security warning window might pop up. Make sure to click on 'Install' (or 'Yes' for other Windows versions)

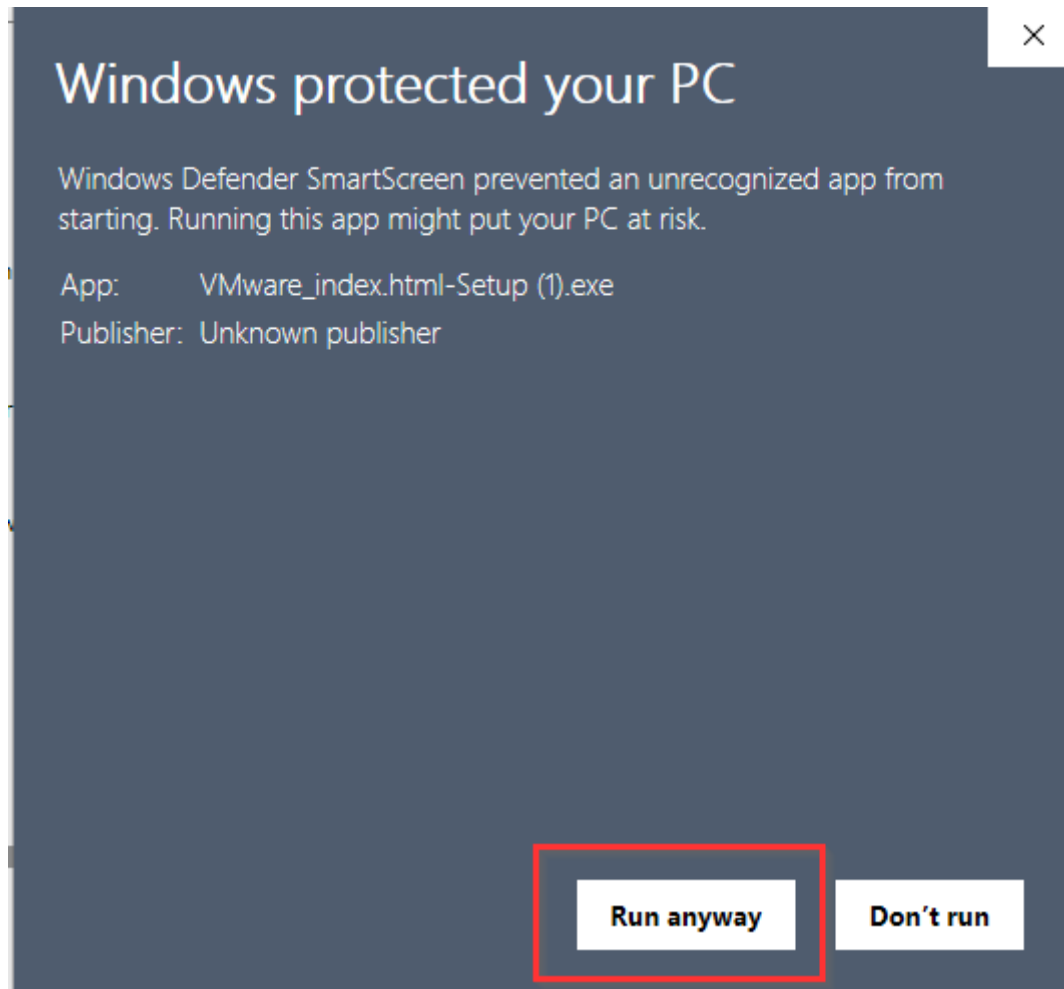
During installation of VMware SSL VPN-Plus Client, a driver signing window will pop up. Make sure to click on 'Continue Anyway' (or 'Yes' for Windows 2000)

Copyright © VMware, Inc. All rights reserved.

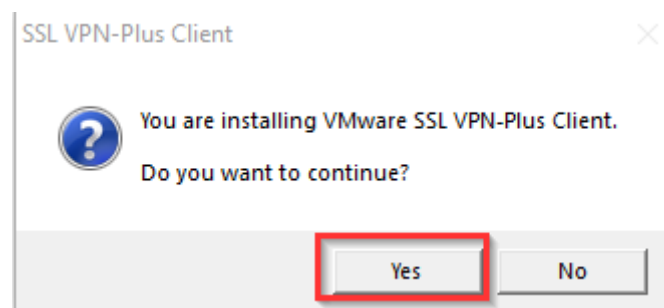
Once the client has downloaded, have them run it.



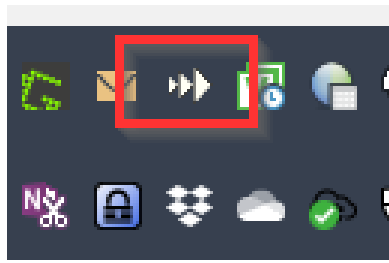
If they get a Windows Defender pop up, they will need to select “More info” and “Run anyway”:



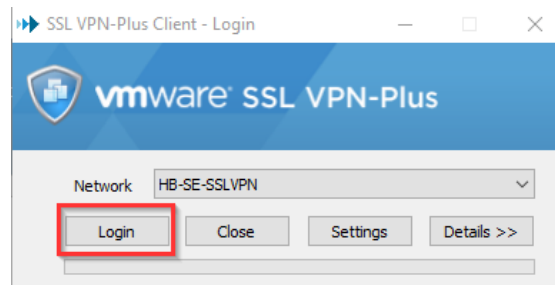
There will then be a pop up confirming they want to install it, have them select “Yes”.



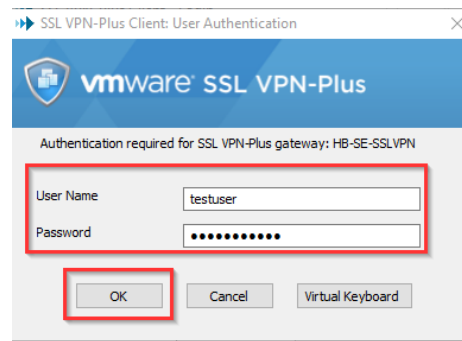
It will install and then it will likely appear in their task tray, have them double click the icon:



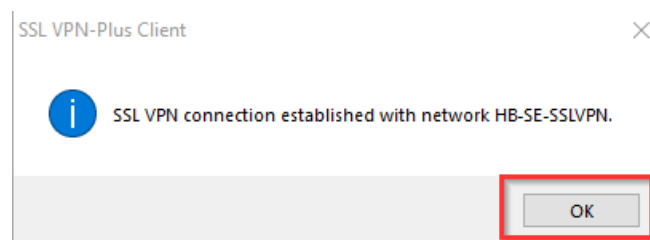
They can then select “Login”:



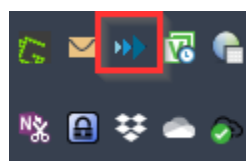
They will then need to enter their credentials you have provided and select “OK”.



They will then receive a pop up notifying them they have successfully connected (or not) they can acknowledge it:



And finally, their SSL VPN icon will have colour:



End Notes

This setup while a walk through is also meant to provide a medium level overview of the setup of the SSL VPN-Plus within vCloud Director. There are additional settings and setup methods that have not been covered. It is possible to have the SSL VPN-Plus leverage LDAP, as well as have it use a certificate.

For additional setup assistance, please contact support@hostedbizz.com and one of our support staff will reach out to assist further.