
Configure Pre-Logon for the Versa SASE Client

 For supported software information, click [here](#).

The pre-logon connection method for a Versa SASE client allows a client device to establish a VPN connection to an organization's network. Pre-logon authenticates a user on the client device and then establishes a secure connection to the organization's network.

Note that in earlier software releases, for releases prior to Release 7.4.3 for Android, Release 7.3.7 for MacOS, and Release 7.4.5 for Windows, the product was called the Versa Secure Access (VSA) client application software.

To use pre-logon authentication, before you ship a laptop device to a new enterprise user, you must install the SASE client with pre-logon enabled, and you must also install the necessary OS updates and security patches to meet the security requirements of your organization. Then, the new user is able to log in to and access the organization's internal resources when they log in for the first time, regardless of where they log in from.

If the organization uses Active Directory (AD) on-premises, connectivity between the user device and AD is required when a user logs in for the first time. Pre-logon authenticates the user and establishes a secure connection to the organization's network. When you enable pre-logon, a new user who has no connectivity to Active Directory can log in to the network the first time, because they can log in using the SASE client and the login credentials provided by the network administrator.

To allow endpoints to access resources in the network, you must create security policies that match the pre-logon user. These policies must allow access only to basic services such as DHCP, DNS, Active Directory, and antivirus.

This article describes how to enable pre-logon on the SASE client. For basic VSA configuration information, see [Configure the Versa Secure Access Service](#).

Before You Begin

Before you begin, ensure that you have the following on the local drive:

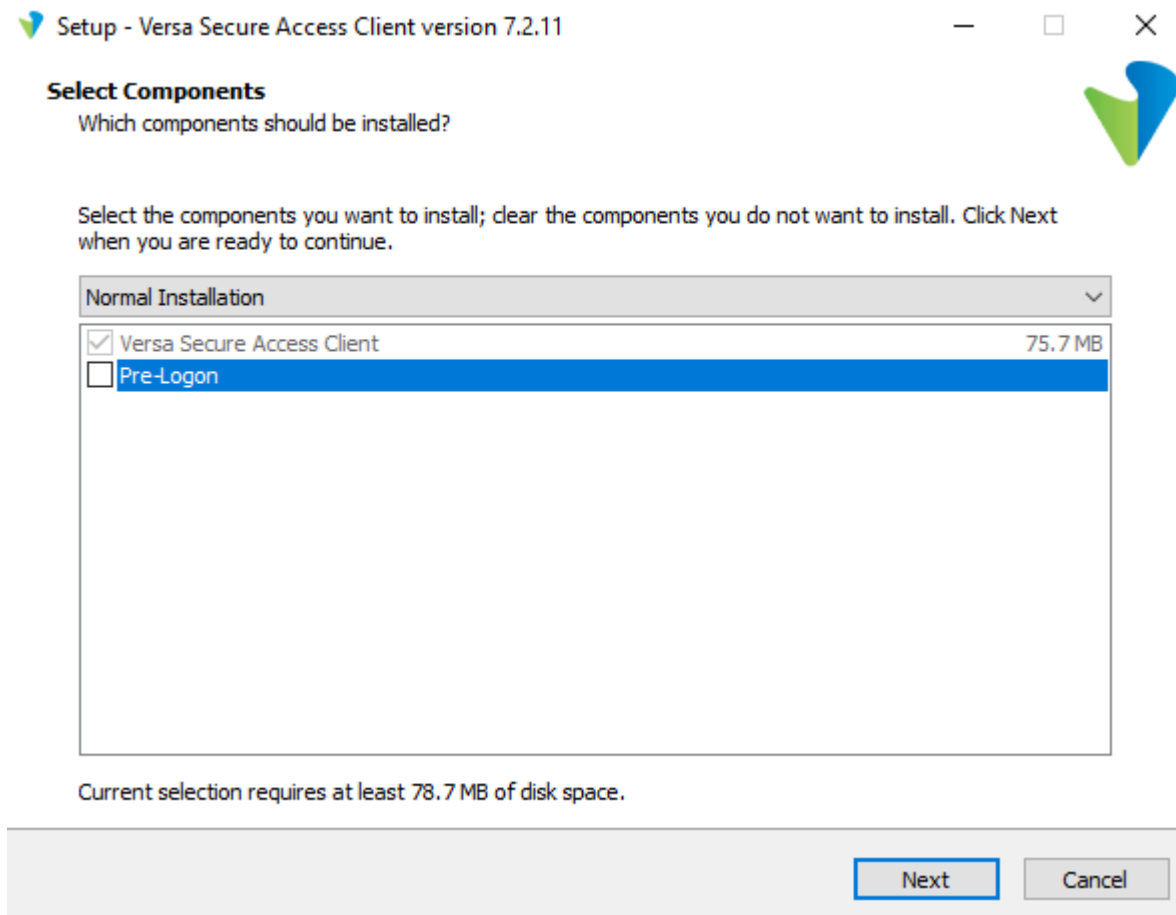
- Pre-logon configuration file, which is a JSON file
- CA certification for the secure access server tunnel authentication

Enable Pre-Logon on the SASE Client

This section describes how to enable pre-logon on a SASE client when the client is a Windows 10 device. To obtain the link from which to download the SASE client, contact Versa Networks Customer Support.

To enable the pre-logon option on the SASE client:

1. Contact Versa Networks to obtain the link for the SASE client application.
2. Download and install the application.
3. Start the application. The setup wizard screen displays.



4. In Select Components, select Pre-Logon. The Normal Installation window then changes to Extended Installation.

Select Components

Which components should be installed?



Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

| Extended Installation | |
|--|---------|
| <input checked="" type="checkbox"/> Versa Secure Access Client | 75.7 MB |
| <input checked="" type="checkbox"/> Pre-Logon | |

Current selection requires at least 78.7 MB of disk space.

Next

Cancel

5. Click Next. The Additional Tasks window displays.

Select Additional Tasks

Which additional tasks should be performed?



Select the additional tasks you would like Setup to perform while installing Versa Secure Access Client, then click Next.

Additional shortcuts:

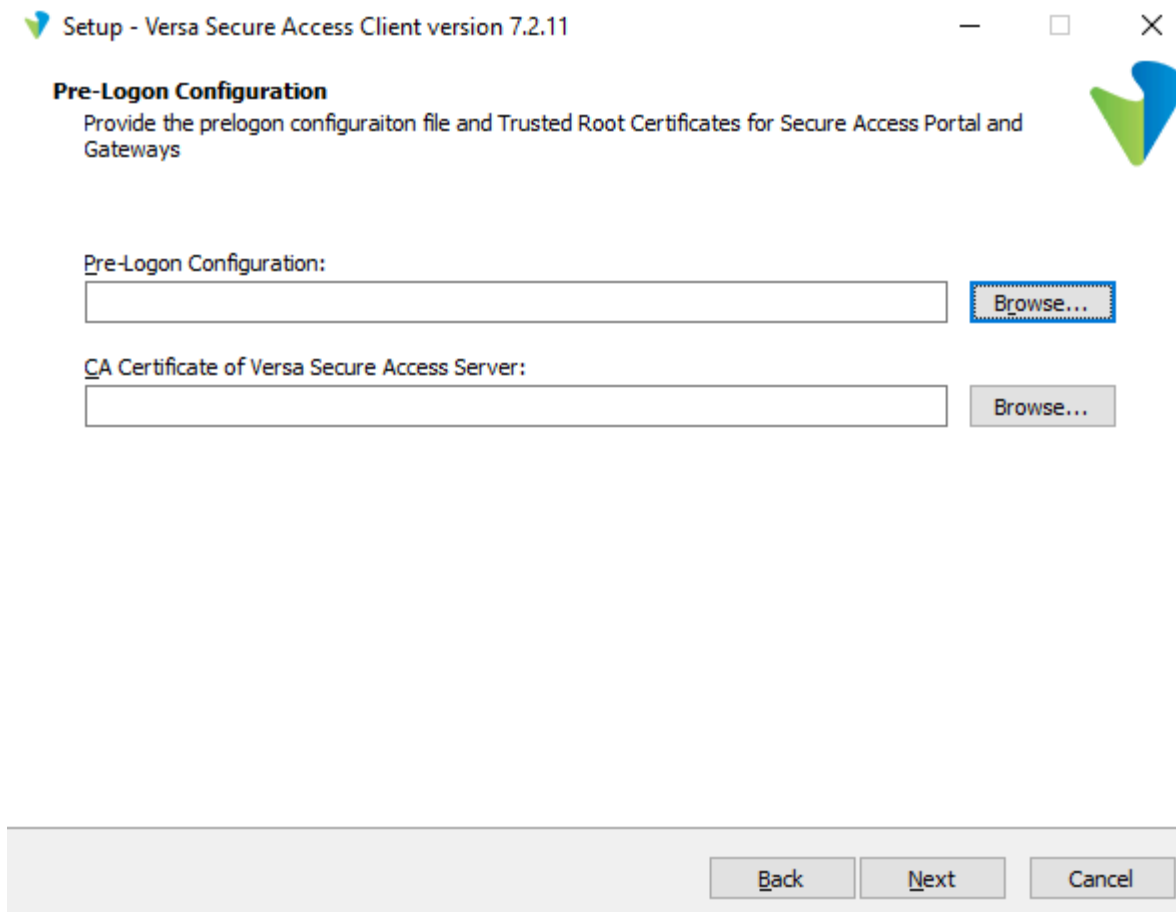
☒ Create a desktop shortcut

Back

Next

Cancel

6. Click Next. The Pre-Logon Configuration window displays.

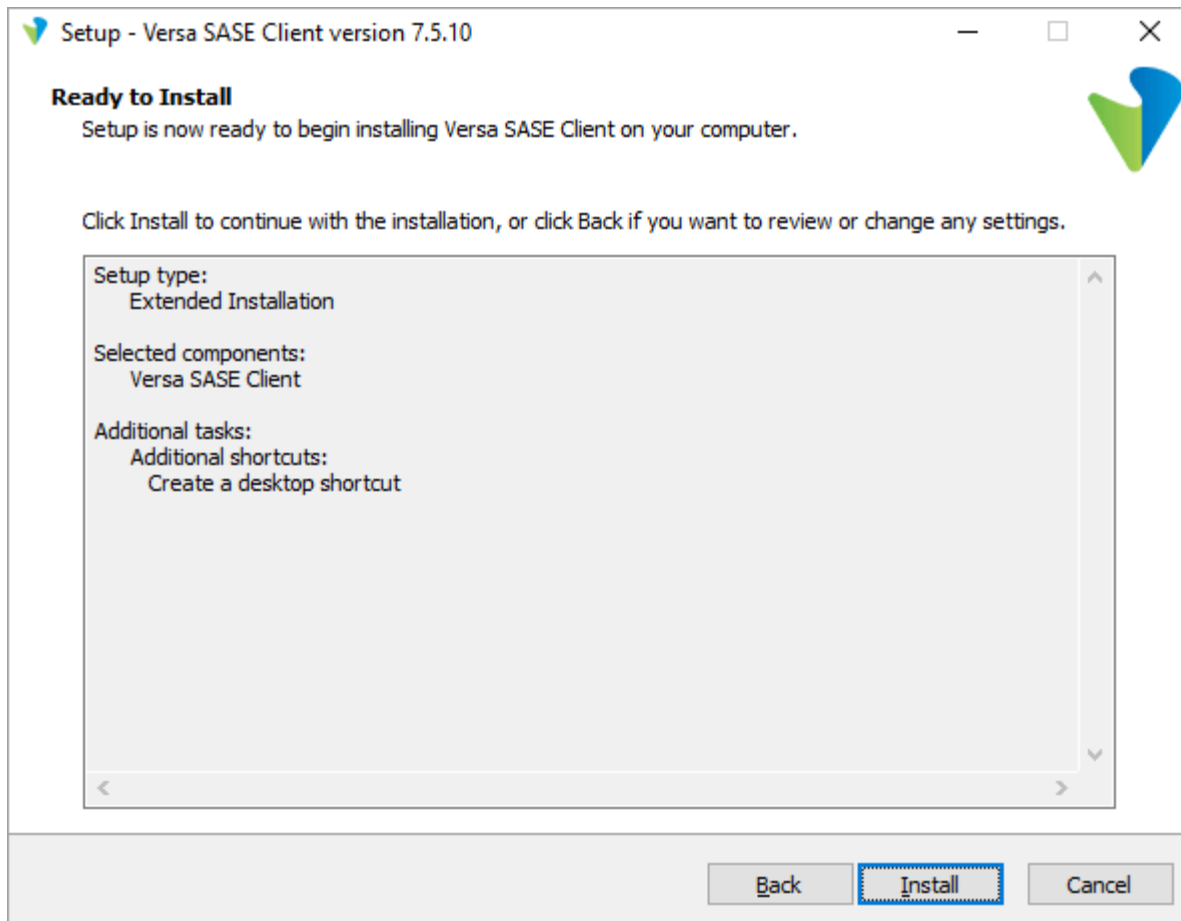


7. If necessary, upload the pre-logon configuration file. In the Pre-Logon Configuration field, click Browse, and then select the configuration file (for example, [PreLogonConfig.json](#)) from your local drive. In Versa Concerto Releases 12.1.1 and later, you can download a sample JSON file from the SASE portal, which includes the prelogon parameters. The default pre-logon JSON file that Versa provides contains the following information.

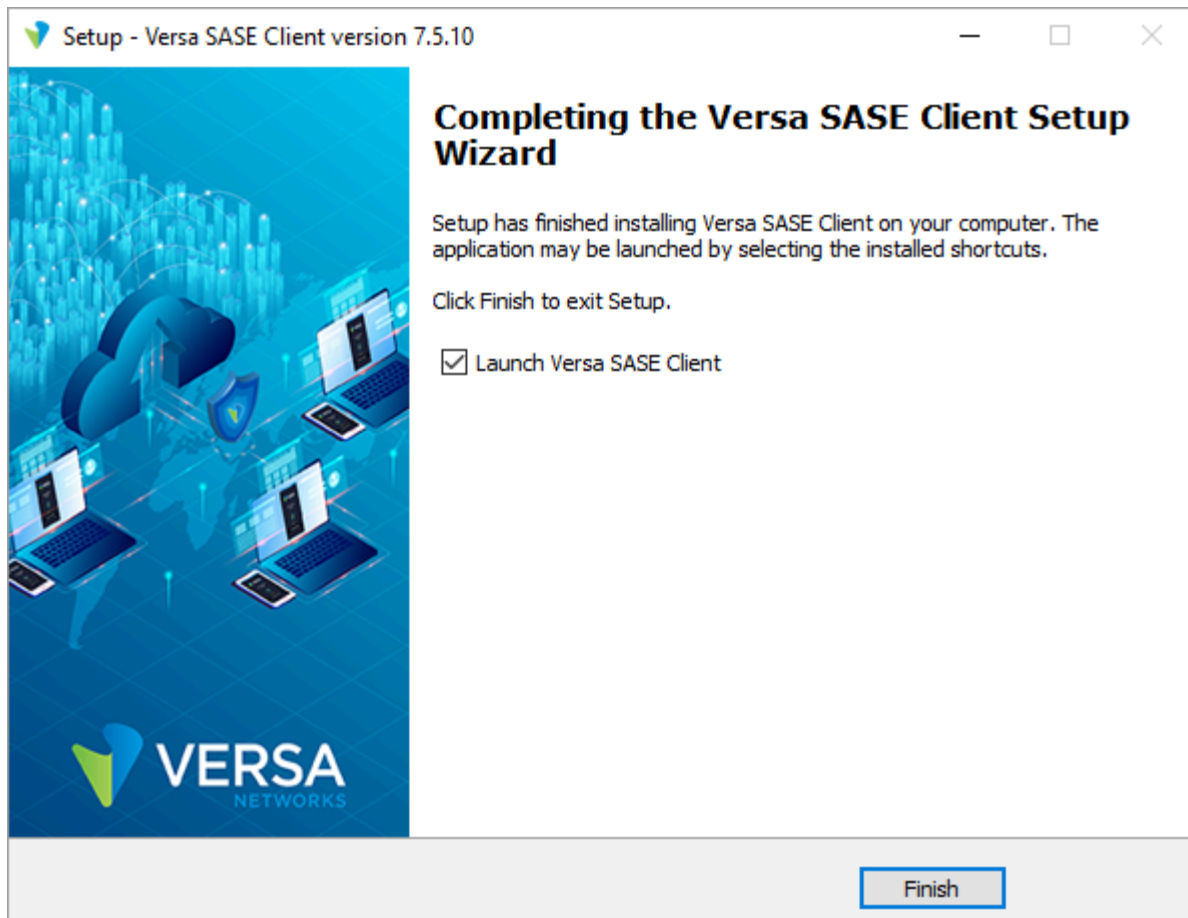
| Field | Description |
|---|--|
| PrelogonControl (Group of Fields) | |
| <ul style="list-style-type: none"> PrelogonDisconnectOnConnect | <p>When enabled (set to true), tunnels that are established in pre-logon mode are disconnected when a user connects to a gateway using the SASE client after logging in to the device.</p> <p><i>Values:</i> Fault, True <i>Default:</i> False</p> |
| <ul style="list-style-type: none"> AutoPrelogonDisconnectTimeoutMins | <p>Duration, in minutes, for which the pre-logon tunnel is available. If you enable PrelogonDisconnectOnConnect, the tunnel is disconnected as soon as the user connects even if the AutoPrelogonDisconnectTimeoutMins time has not elapsed.</p> <p><i>Default:</i> 60 minutes</p> |
| <ul style="list-style-type: none"> PrelogonCertOnlyAuth | <p>When enabled (set to true), pre-logon supports only Device Certificate Method for authentication. You must set this field to true to enable always-on in pre-logon mode.</p> |
| Enterprises (Group of Fields) | |
| <ul style="list-style-type: none"> EnterpriseName | <p>Name of the tenant or enterprise.</p> |
| <ul style="list-style-type: none"> GatewayProfiles (Group of Fields) | <p>List of gateways associated with the enterprise or tenant. To obtain the values for the parameters GatewayProfileName, IPSECProfileID, and FQDN, create a ticket to the Versa Managed Services team.</p> |
| <ul style="list-style-type: none"> GatewayProfileName | <p>Name of the connecting gateway.</p> |
| <ul style="list-style-type: none"> Priority | <p>Gateway priority to use when connecting.</p> |
| <ul style="list-style-type: none"> IPSECProfileID | <p>Profile ID associated with the gateway.</p> |

| | |
|----------------------------------|--|
| ◦ FQDN | FQDN to reach the gateway. |
| ◦ Port | Port on which the gateway listens. |
| ◦ RouteConfig | Specify how to apply routes when establishing a tunnel. |
| • SplitTunnel | Specify how to handle split-tunnel traffic: <ul style="list-style-type: none"> ◦ False—Send all traffic over the tunnel. ◦ True—Send only traffic matching the routes in the configuration over the underlay network. |
| • Routes | Configure the routes for the client to route traffic: <ul style="list-style-type: none"> ◦ Prefix—Details of the route. The client routes destination traffic through the tunnel to this IP address. ◦ Metric—Metric value to use for the route. |
| Domain Servers (Group of Fields) | DNS servers to use for name resolution. |
| ◦ DomainName | Name of the domain. |
| ◦ NameServers | IP addresses of the DNS server. |

8. If necessary, upload the the CA certificate of the VSA server. In the CA Certification of VSA Server field, click Browse, and then select the certificate. You can also associate these files after the client installation. For more information, see [Configure Pre-Logon Settings](#), below.
9. Click Next. The Ready to Install screen displays.



10. Click Install. The installation begins, and an installation status screen displays. To stop the installation, click Cancel.
11. After the installation completes, the Completing the Versa Secure Access Client Setup Wizard screen displays.



12. By default, Launch Versa SASE Client is selected. Click to deselect the option.
13. Click Finish to complete the installation. The Register screen displays, unless you deselected Launch Versa Secure Access Client. For more information, see [Register and Connect a Versa SASE Client](#).
14. Reboot the device to display the network sign-in option on the locked screen. For more information, see [Example of Pre-Logon using SASE Client](#), below.

Install Pre-Logon Using CLI

If you are using tools such as the Microsoft System Center Configuration Manager (SCCM), you can install and configure pre-logon on SASE clients from the CLI.

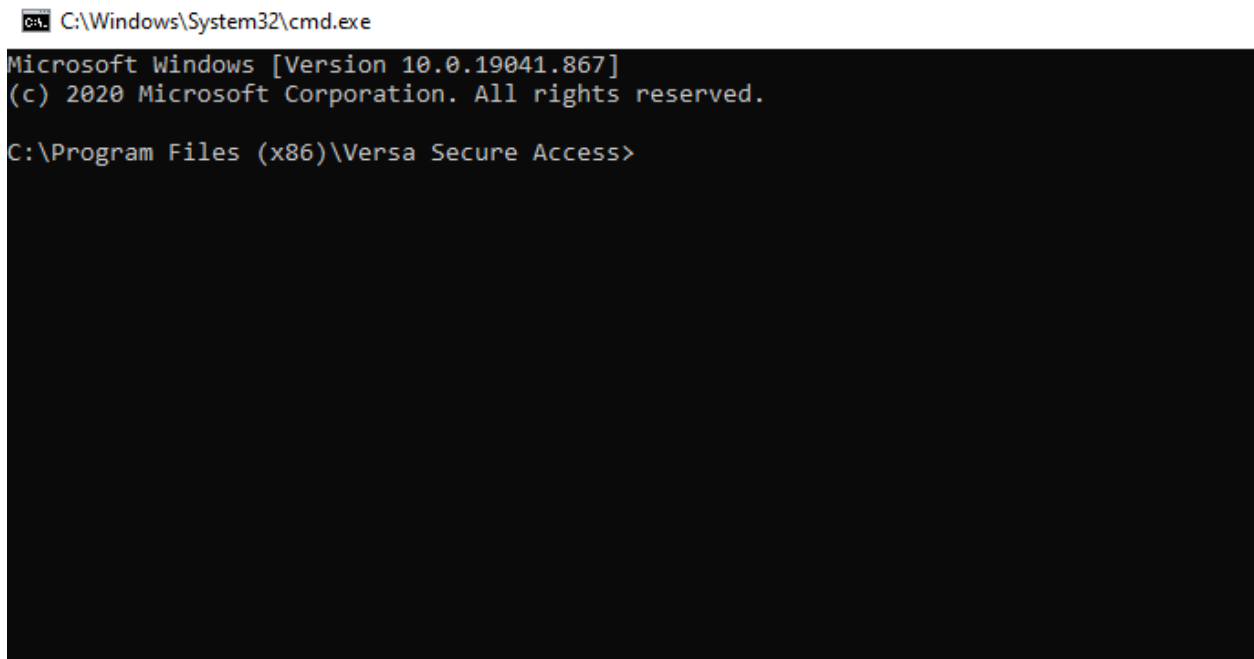
To silently install the SASE client with pre-logon enabled from the CLI, issue the following CLI command. For *version-number*, enter the version of client that you are installing.

```
VersaSecureAccessClient_<version-number>.exe /SP- /silent /components=base,prelogon  
/SUPPRESSMGSBOXES /LOG="log-file-path" /NOICONS /ALLUSERS
```

Configure Pre-Logon Settings

This section describes how to configure the pre-logon configuration file. You can also perform this step if you do not upload a pre-logon configuration file during the SASE client installation.

1. Select the folder in which the SASE client application is installed, for example, C:\Program Files (x86)\Versa Secure Access>.
2. In the file explorer path of this location, type **cmd** and then press Enter. The following command prompt displays.



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19041.867]
(c) 2020 Microsoft Corporation. All rights reserved.
C:\Program Files (x86)\Versa Secure Access>
```

3. To apply the pre-logon configuration, issue the following CLI commands. Note that you must run these commands from administrator mode.

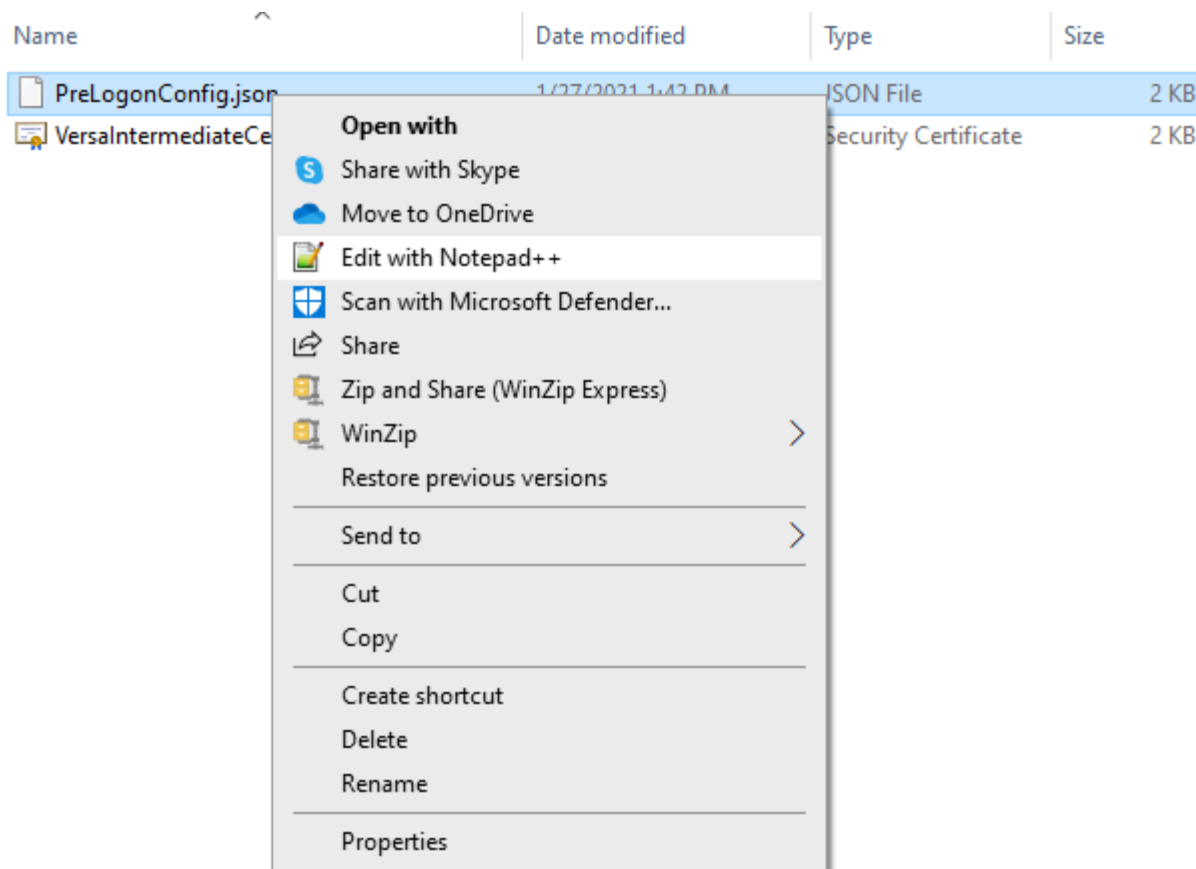
```
C:\Program Files (x86)\Versa Secure Access>VersaSecureAccessClientConsole.exe --prelogon_config
C:\Users\user\Desktop\PrelogonConfig\PreLogonConfig.json --trusted_root_ca_certificate
C:\Users\user\Desktop\PrelogonConfig\VersaIntermediateCertificateAuthority1.cer --silent
453 [1] INFO Versa Secure Access (null) - Starting application in prelogon_config mode. Version 7.2.11_
51ee8fb6
515 [1] DEBUG Versa Secure Access (null) - Prelogon configuration initiated
515 [1] DEBUG Versa Secure Access (null) - Verifying and Applying Prelogon Configuration
2062 DEBUG Versa Secure Access (null) - Prelogon Configuration Applied Successfully!
```

4. Reboot the device to display the network sign-in option on the locked screen. For more information, see [Example of Pre-Logon using SASE Client](#), below.

Edit the Pre-Logon Configuration File Controls

You can edit the pre-logon configuration file to change the control settings.

1. Select the pre-logon configuration file (here, PreLogonConfig.json) and right-click to edit the file using. Here, Notepad ++ is used.



2. To edit the pre-logon control options, edit the fields displayed under PrelogonControl at the top of the file.

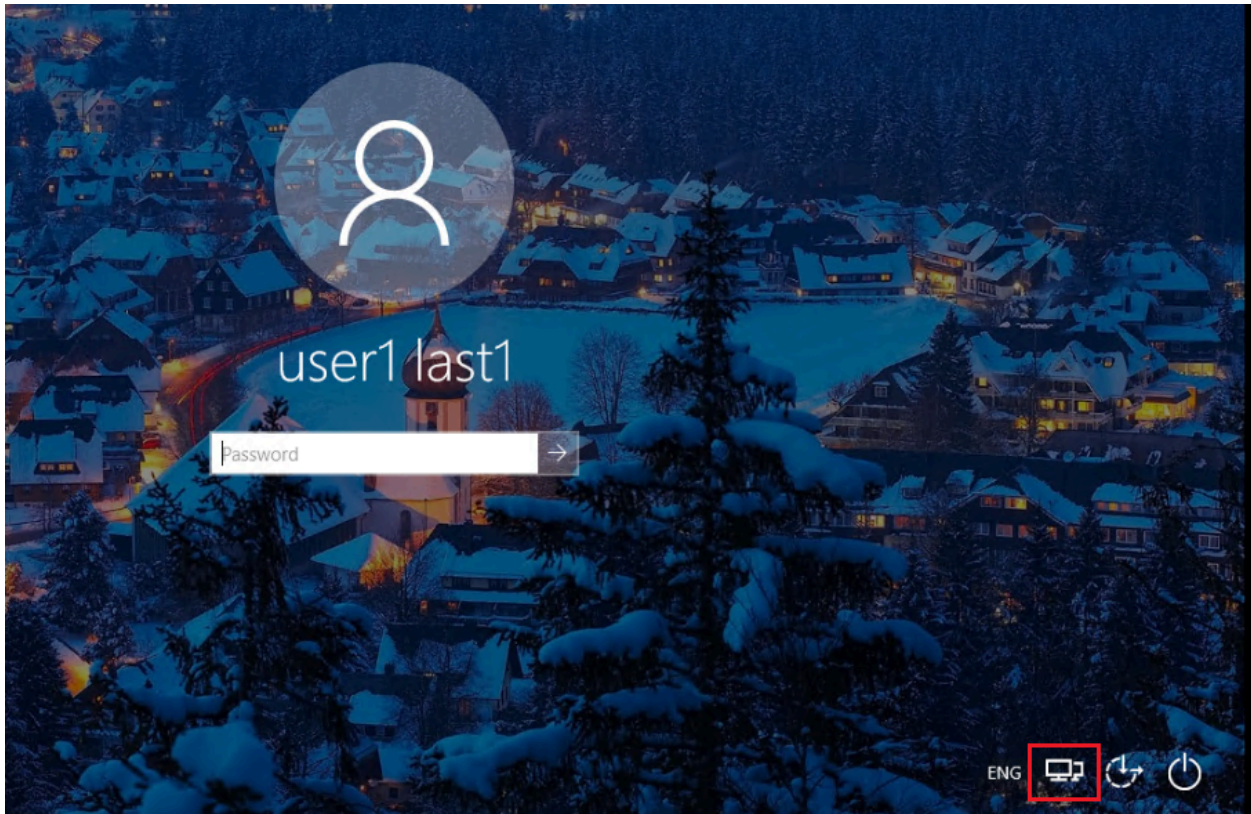
```
"PrelogonControl": {  
  "PrelogonDisconnectOnConnect": false,  
  "AutoPrelogonDisconnectTimeoutMins": 5  
},
```

- a. To disconnect pre-logon when a user registers on the VSA portal and connects after login, change the PrelogonDisconnectOnConnect value to "true." The default is "false."
 - b. To disconnect the pre-logon connection after a number of minutes, update the AutoPrelogonDisconnectTimeoutMins value. The default is 60 minutes, and the range is 5 through 120 minutes.
3. Save the file.
 4. Follow the steps described in [Configure Pre-Logon Settings](#), above, to update the pre-logon configuration file on the endpoint machine.

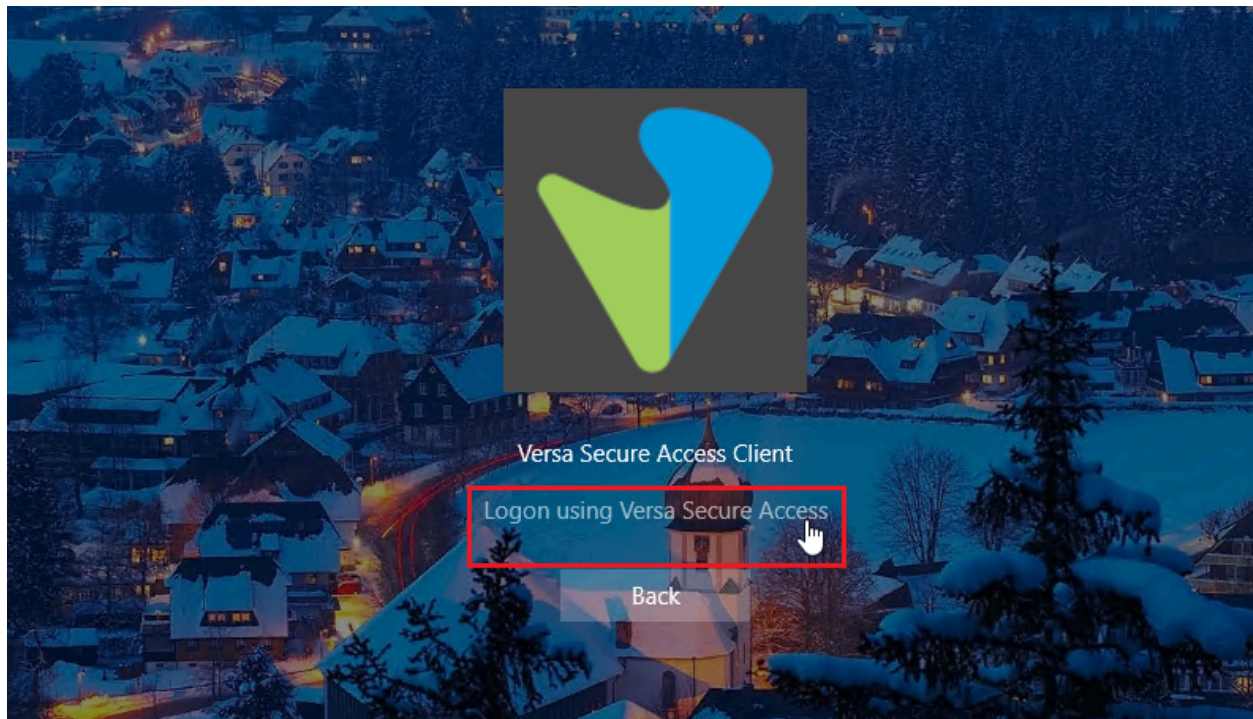
Example of Pre-Logon using SASE Client

After you configure pre-logon on SASE client application, new users who do not have connectivity to your network's Active Directory can log in to the network. The example screens in this section show how a new user can log in to the network.

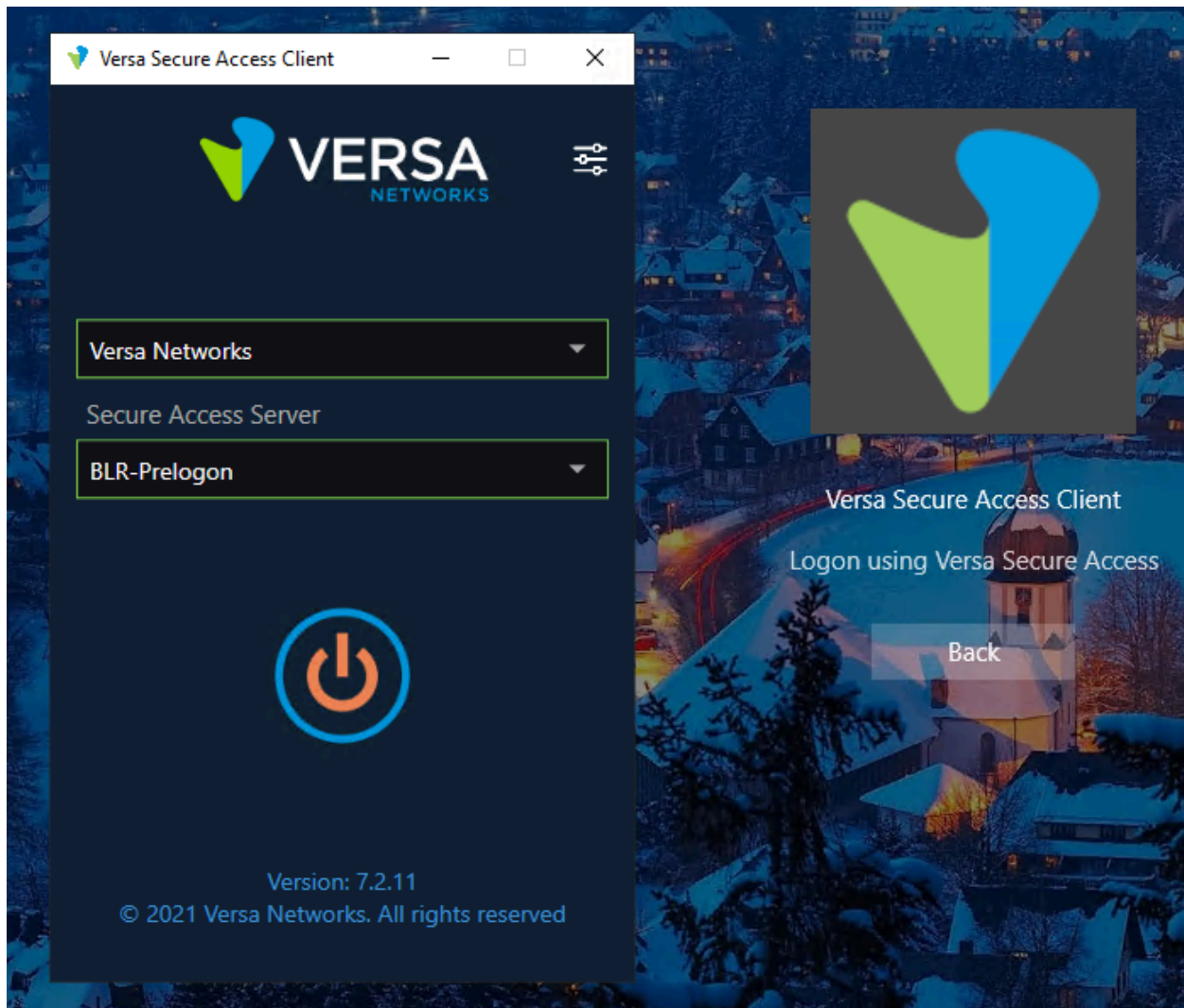
1. After you configure pre-logon on an endpoint machine, when a new user logs in, the network sign-in option displays on the locked screen.



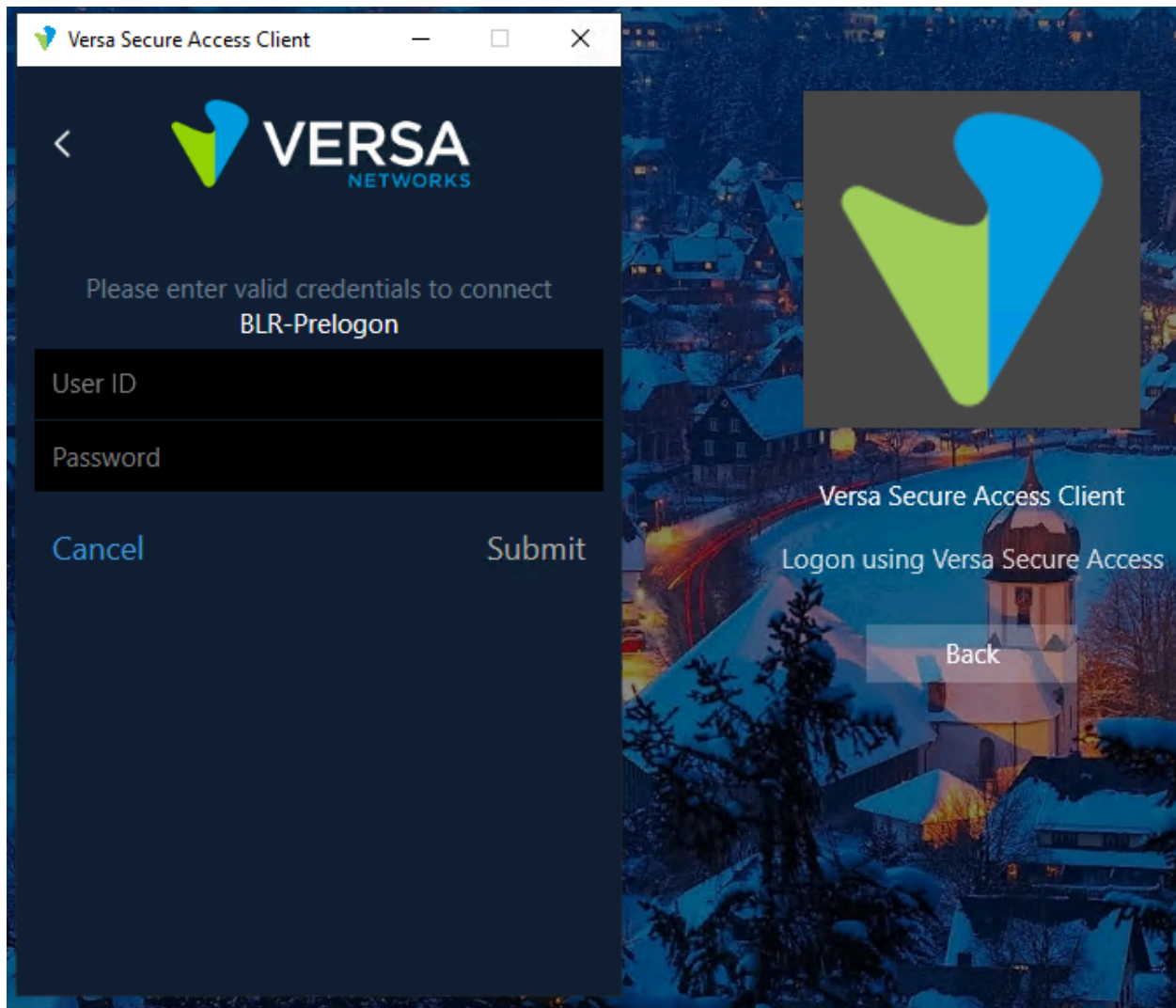
2. When the user clicks the Network sign-in, the following screen displays.



3. To login, the user clicks Logon Using Versa Secure Access. The SASE client login screen displays.



4. When the user clicks Connect, the option to enter login credentials displays.



5. The user then enters the user ID and password provided by the network administrator, and clicks Submit to log in to the network.

Supported Software Information

Releases 7.2.5 of Versa Secure Access Client and later support all content described in this article.

Additional Information

[Configure the Versa Secure Access Service](#)

[Configure Versa Secure Access Subscriptions](#)

[Use the Versa SASE Client Application](#)

[Versa Secure Access Client Quick Start](#)

[https://docs.versa-networks.com/Security_Service_Edge_\(SSE\)/Configuration_from_Director/Versa_SASE_Client/Configure_...](https://docs.versa-networks.com/Security_Service_Edge_(SSE)/Configuration_from_Director/Versa_SASE_Client/Configure_...)

Updated: Wed, 23 Oct 2024 08:43:48 GMT

Copyright © 2024, Versa Networks, Inc.