



AG Standalone Array Client Administration Guide

Copyright Statement

Copyright©2015 Array Networks, Inc., 1371 McCarthy Blvd, Milpitas, California 95035, USA.
All rights reserved.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and compilation. No part of this document may be reproduced in any form by any means without prior written authorization of Array Networks, Inc. Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

Array Networks, Inc., reserves the right to change any products described herein at any time, and without notice. Array Networks, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Array Networks, Inc. The use and purchase of this product does not convey a license to any patent copyright, or trademark rights, or any other intellectual property rights of Array Networks, Inc.



Warning: Modifications made to the Array Networks unit, unless expressly approved by Array Networks, Inc., could void the user’s authority to operate the equipment.

Declaration of Conformity

We, Array Networks, Inc., 1371 McCarthy Blvd, Milpitas, CA 95035, 1-866-992-7729; declare under our sole responsibility that the product(s) Array Networks, Inc., Array Appliance complies with Part 15 of FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.



Warning: Array Appliance is a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. In a residential area, operation of this equipment is likely to cause harmful interference in which case the user may be required to take adequate measures or product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

About Array Networks

Array Networks is a global leader in networking solutions for connecting users and applications while ensuring performance, availability and security. Using Array, companies can provide access for any user, anywhere, on any device to applications, desktops and services running in either the cloud or the enterprise data center. From Web sites to e-commerce to enterprise applications to cloud services, Array solutions deliver a premium end-user experience and demonstrable security while ensuring that revenue and productivity gains always outweigh CAPEX and OPEX.

Engineered for the modern data center, Array Networks application, desktop and cloud service delivery solutions support the scalability, price-performance, software agility and leading-edge feature innovation essential for successfully transforming today's challenges in mobile and cloud computing into opportunities for mobilizing and accelerating business.

Contacting Array Networks

Please use the following information to contact us at Array Networks:

➤ **Website:**

<http://www.arraynetworks.com/>

➤ **Telephone:**

Phone: (408)240-8700

Toll Free: 1-866-692-7729 (1-866-MY-ARRAY)

Support: 1-877-992-7729 (1-877-99-ARRAY)

Fax: (408)240-8754

Telephone access to Array Networks, Inc. is available Monday through Friday, 9 A.M. to 5 P.M. PST.

➤ **E-mail:**

info@arraynetworks.com

➤ **Address:**

1371 McCarthy Boulevard

Milpitas, California 95035, USA

Table of Contents

Copyright Statement	I
Declaration of Conformity	I
About Array Networks.....	II
Contacting Array Networks	II
Table of Contents	III
1 Installation.....	1
1.1 Download the Installation Package	1
1.2 Installation Process	1
1.2.1 Install the Standalone Array Client on Windows	1
2 How to Use the Standalone Array Client	4
2.1 Use the Standalone Array Client for Windows in UI Mode	4
2.1.1 Create a Profile.....	4
2.1.2 Configure Proxy Settings for the Profile (Optional)	6
2.1.3 Connect to the VPN Server	6
2.1.4 Disconnect from the VPN Server.....	8
2.1.5 View VPN Status	8
2.1.6 Configure Options for the Array Client (Optional).....	10
2.1.7 Exit the Array Client	14
2.1.8 Manage a Profile	14
2.1.9 Import Profile(s).....	15
2.1.10 Export the Profile	16
2.1.11 Start the Logger Tool	16
2.1.12 Obtain Help	17
2.2 Use the Standalone Array Client for Windows in Command Line Mode.....	17
3 Standalone Array Client Customization.....	20
3.1 OEM.ini Customization	20
3.2 Profiles.ini Customization.....	21
4 Limitations	22

Appendix I Integrate with RSA Token Automation	23
I.1 Install RSA SecurID Token Client	23
I.2 Import the Token File to RSA SecurID Token Client	23
I.3 Enable RSA Token with Automation	25
I.4 Authentication with RSA Token with Automation Enabled	26

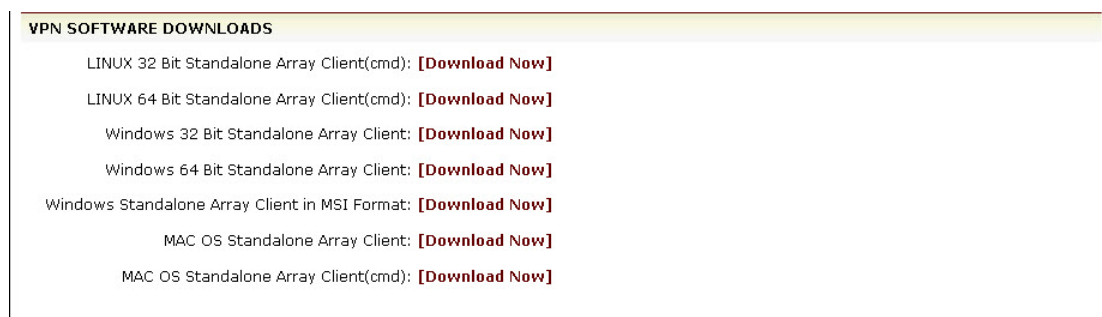
1 Installation

The installation package of the Standalone Array Client for each operating system can be downloaded by the administrator from the AG WebUI. Then, the administrator distributes the installation package to end users for installation and use.

1.1 Download the Installation Package

To download Standalone Array Client for an operating system, the administrator should perform the following action:

Click the **Download Now** action link in the **VPN Software Downloads** area of **Access Methods > VPN > SSL VPN** under the virtual site scope, as shown in the following figure.



Note:

- Windows/Linux 32-bit and 64-bit OSs have different installation packages. The administrator should distribute the installation packages according to end users' OS.
- The Standalone Array Client for Windows/MAC OS supports running in UI mode and command line mode while that for Linux supports running only in command line mode.
- MAC OS use two different Standalone Array Clients to run in UI mode and command line mode respectively while Windows use one Standalone Array Client to run in UI mode and command line mode.

1.2 Installation Process

After obtaining the installation package from the administrator, the end user can install the Standalone Array Client by following the installation process.

1.2.1 Install the Standalone Array Client on Windows

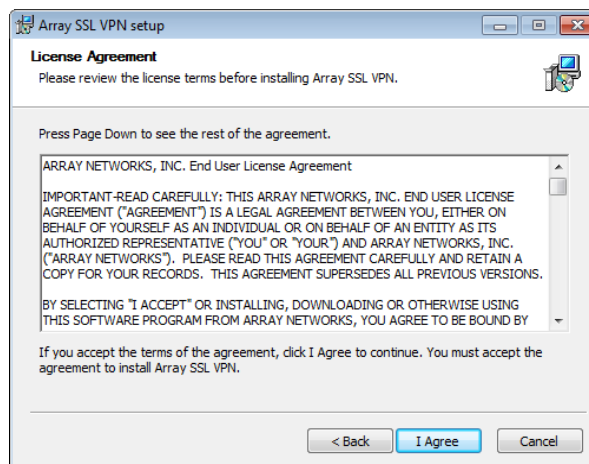
This section describes the installation process of the Standalone Array Client by using “Standalone Array Client for Windows (32-bit)” as an example.

To install the Standalone Array Client on Windows, the end user should perform the following steps:

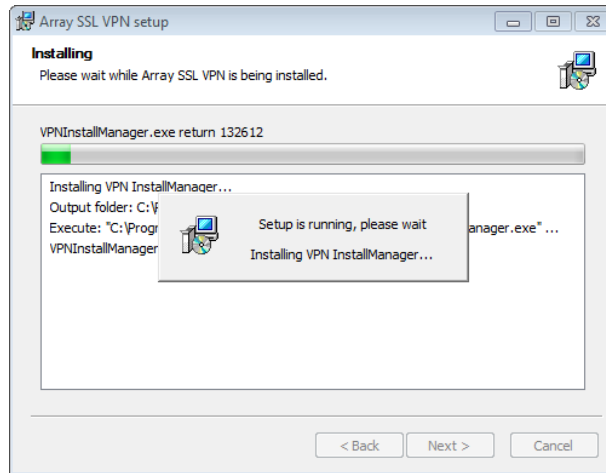
1. Decompress the installation package for the Standalone Array Client (SSLVPNSetup_win32.zip) obtained from the administrator and double click the **SSLVPNSetup.exe** file to install the Standalone Array Client.
2. In the **Welcome to the Array SSL VPN Setup Wizard** window, click the **Next** button to continue, as shown in the following figure.



3. In the displayed **License Agreement** window, click the **I Agree** button to continue if you accept the terms of the agreement.



4. Wait for the Windows to install the Standalone Array Client. By default, the Array SSL VPN will be installed in the path of **\Program Files\Array Networks**.



5. Click the **Finish** button to finish the installation. If you do not want to run the Array SSL VPN immediately, please clear the **Run Array SSL VPN** check box before clicking the **Finish** button.



2 How to Use the Standalone Array Client

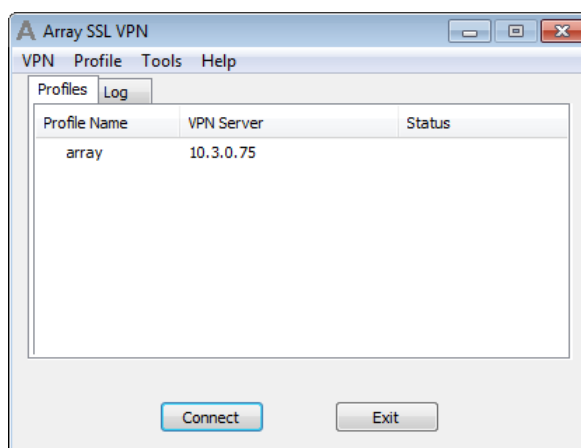
The administrator can use this chapter to give their end users instructions on how to use the Standalone Array Client.

The ways of using the Standalone Array Client in UI mode and in command line mode are different.

2.1 Use the Standalone Array Client for Windows in UI Mode

This section uses the Standalone Array Client installed on Windows as an example.

After opening the Standalone Array Client, the end user will see the following main window.



The main window is consisted of two tabs:

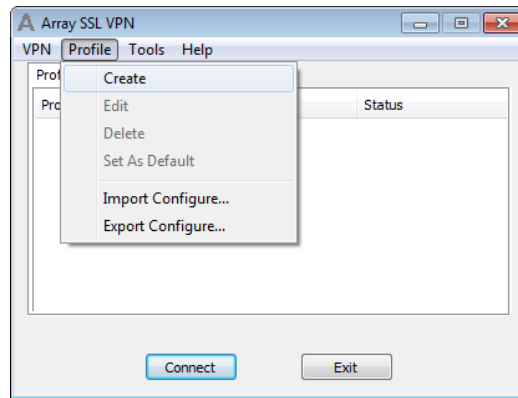
- **Profiles:** displays all profiles, VPN servers, and connection status.
- **Log:** displays the connection information.

2.1.1 Create a Profile

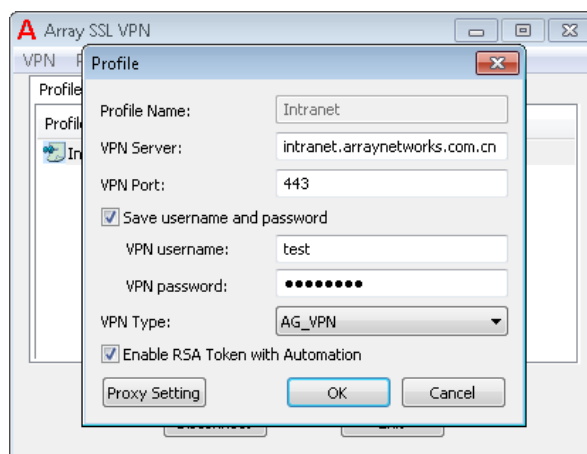
The end user should create a profile for the virtual site before accessing it. The profile records the information about the virtual site, such as the site name and VPN server.

To create a profile for a virtual site, the end user should do as follows:

1. Click the **Profile** menu and select the **Create** command from the prompted menu list, as show in the following figure.



- In the displayed **Profile** window, specify the parameters as required and click the **OK** button, as shown in the following figure.



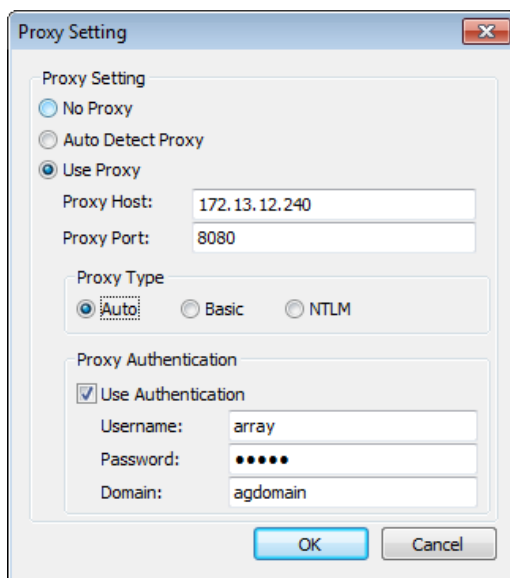
Parameter	Meaning
Profile Name	Specifies the general description of the profile.
VPN Server	Specifies the domain name or IP address of the SSL VPN server.
VPN Port	Specifies the port number of the VPN server.
Save username and password	Specifies whether to use the saved VPN username and VPN password to log into the VPN server on behalf of the end user. <ul style="list-style-type: none"> VPN username: specifies the VPN username to be saved and used. VPN password: specifies the VPN password to be saved and used.
VPN Type	Specifies the type of the VPN. The default value is AG_VPN. If your server is an SPX product, you can also select SPX_L3VPN or SPX_L4VPN.
Enable RSA Token with Automation	Enables the Array Client to automatically obtain the token or password from the RSA SecurID Token Client. To use this check box, you also need to install the RSA SecurID Token client on the PC and import the token file to the RSA SecurID Token client. For more details, refer to Appendix I.

2.1.2 Configure Proxy Settings for the Profile (Optional)

If the Array Client needs to use the outside proxy to access the VPN server, the end user needs to configure the proxy settings for the profile.

To configure proxy settings for the VPN client, the end users should do as follows:

1. Click the **Proxy Setting** button in the **Profile** window and the **Proxy Setting** window will be displayed, as shown in the following figure.

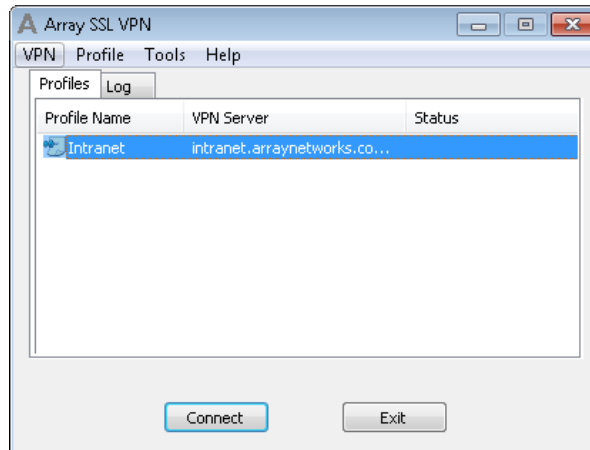


2. If the proxy settings can be auto detected, select the **Auto Detect Proxy** radio button. Otherwise, select the **Use Proxy** radio button and complete the following steps.
3. Specify the **Proxy Host** and **Proxy Port** parameters and set **Proxy Type** to **Auto**, **Basic** or **NTLM** as required.
4. If the proxy server requires authentication, select the **Use Authentication** check box and specifies the parameters **Username**, **Password** and **Domain** for accessing the proxy server.

2.1.3 Connect to the VPN Server

To connect to the VPN server, the end user should do as follows:

1. Under the **Profiles** tab in the main window, select the profile of the VPN server to be accessed and click the **Connect** button, as shown in the following figure.

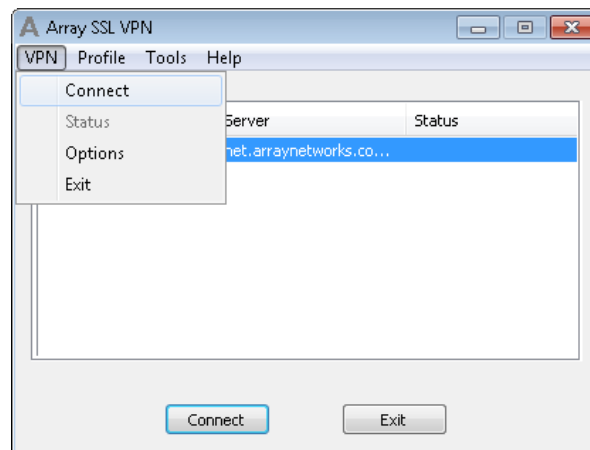


2. Wait for the Array Client to connect to the VPN server. After the VPN server is connected, the Red A icon will be displayed in the Status bar, as shown in the following figure.



Alternatively, the end user can connect to the VPN server by do as follows:

1. Under the **Profiles** tab in the main window, select the profile of the VPN server to be accessed, click the **VPN** menu and select the **Connect** command, as shown in the following figure.



2. Wait for the Array Client to connect to the VPN server.



Note:

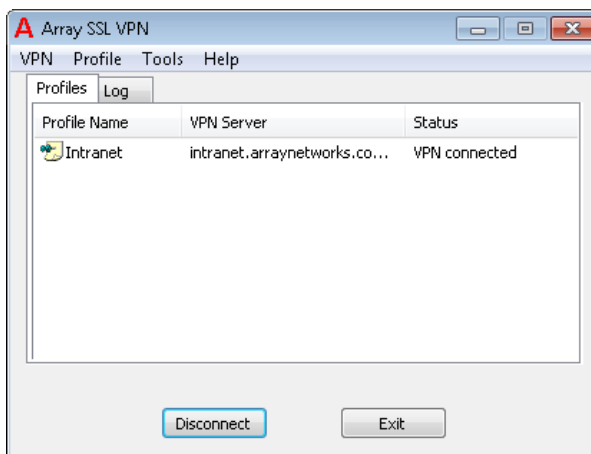
- The end user can click the **Log** tab in the main window to view the VPN connection logs for this connection and all history VPN connection logs.
- After the VPN server is connected, the UI of the Array Client will be hidden. The end user can view the UI of the Array Client by right clicking the Red A icon in the status

bar and select the **Show UI** command from the prompted menu.

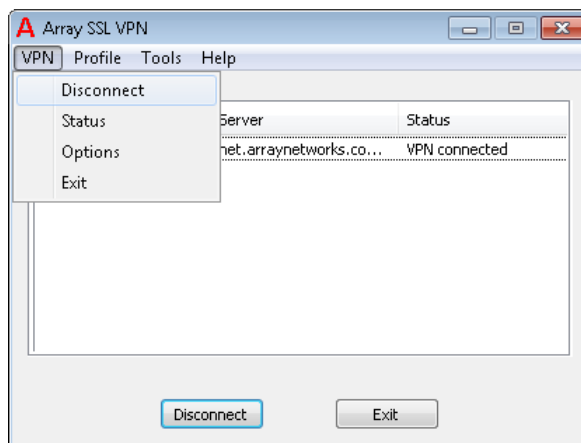
2.1.4 Disconnect from the VPN Server

To disconnect the Array Client from the connected VPN server, the end user should perform any of the following actions:

- Under the **Profiles** tab in the main window, click the **Disconnect** button, as shown in the following figure.

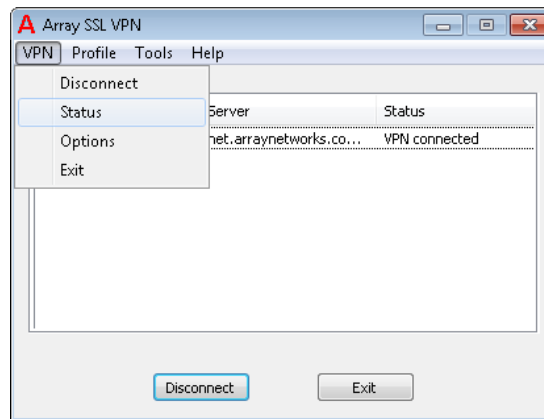


- Click the **VPN** menu and select the **Disconnect** command, as shown in the following figure.

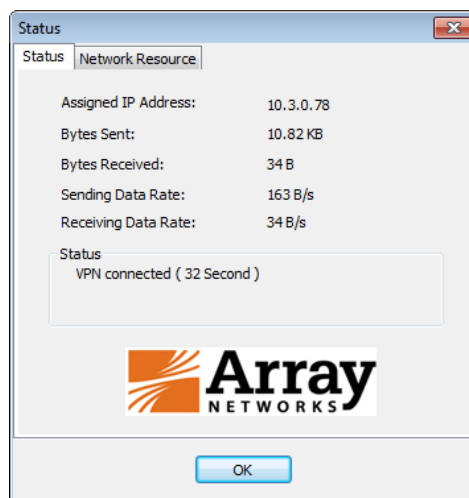


2.1.5 View VPN Status

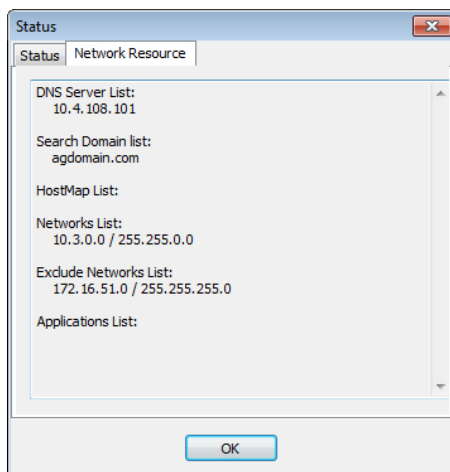
To view the information about the status and network resources of the current VPN connection, the end user should click the **VPN** menu and select the **Status** command from the prompted menu, as shown in the following figure.



The **Status** window will be displayed. The **Status** window is consisted of two tabs: **Status** and **Network Resource**.



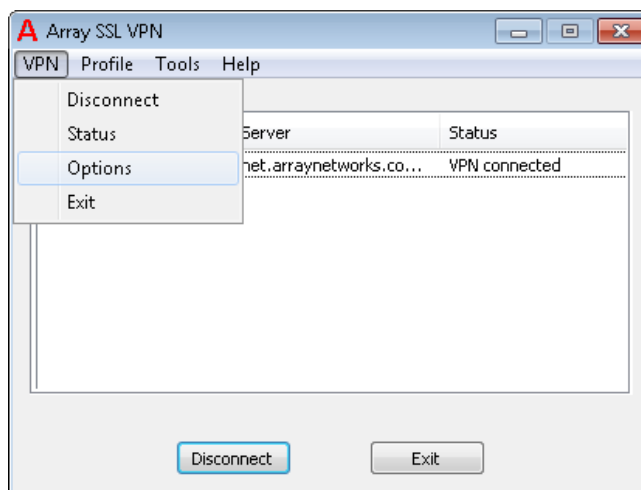
Item	Meaning
Assigned IP Address	The IP address assigned to the Array Client by the VPN server. The IP address is in the Netpool authorized to the end user.
Bytes Sent	The number of bytes sent through the SSL VPN tunnel.
Bytes Received	The number of bytes received through the SSL VPN tunnel.
Sending Data Rate	The sending data rate through the SSL VPN tunnel.
Receiving Data Rate	The receiving data rate through the SSL VPN tunnel.
Status	The status of the SSL VPN tunnel.



Item	Meaning
DNS Server List	The DNS servers used to resolve domain names on the SSL VPN tunnel.
Search Domain List	The DNS domain suffixes.
HostMap List	The static DNS host records configured to speed up the resolving of some domain names.
Networks List	The network resources that the end user can access through the SSL VPN tunnel.
Exclude Networks List	The network resources that the end user is not allowed to access through the SSL VPN tunnel.
Application List	The applications that the end user is allowed to use the SSL VPN tunnel to transmit data.

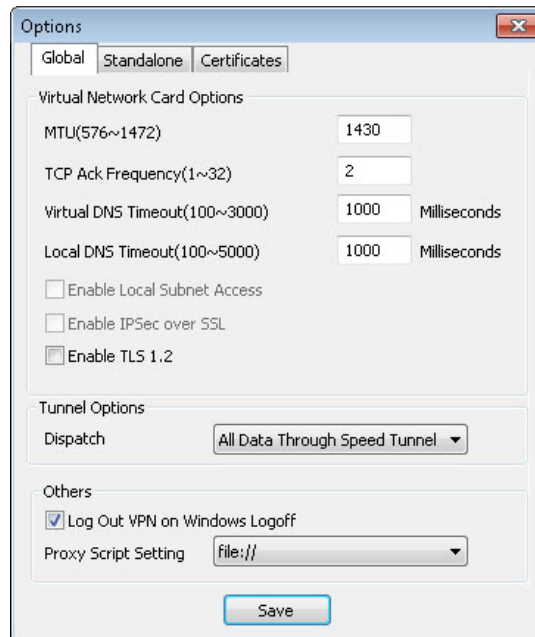
2.1.6 Configure Options for the Array Client (Optional)

End users proficient in network knowledge can configure advanced options for the Array Client. It is recommended not to set these options. To configure advanced options for the Array Client, the end user should click the **VPN** menu and select **Options** from the prompted menu as shown in following figure.



The **Options** window will be displayed. The window consists of three tabs: **Global**, **Standalone** and **Certificates**.

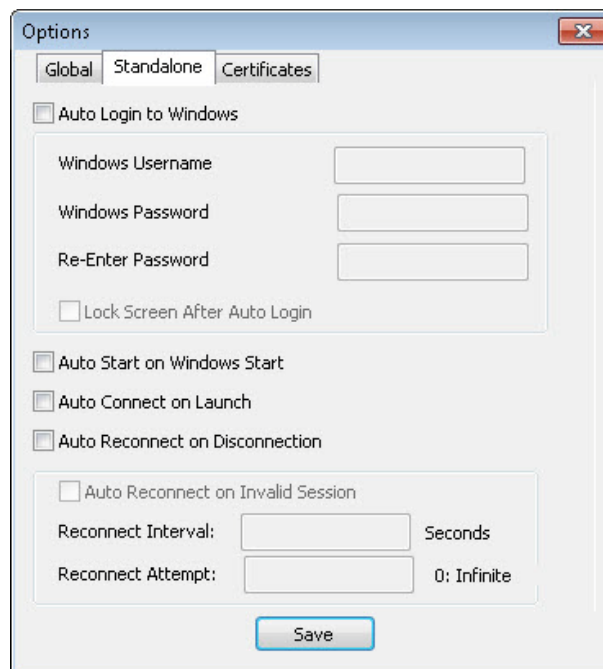
➤ **Global Configuration**



Parameter	Meaning
MTU	Sets the Maximum Transmission Unit for your network environment.
TCP Ack Frequency	Sets the frequency of the data package of TCP Ack. The default value is 2.
Virtual DNS Timeout	Sets an interval at which the Array VPN virtual DNS times out.
Local DNS Timeout	Sets an interval at which the local DNS times out.
Enable Local Subnet Access	Enables the local subnet access. This parameter is available if the administrator sets for the accessing virtual site.
Enable IPsec over SSL	Enables the IPsec over SSL. This parameter is available if the administrator sets for the accessing virtual site.
Enable TLS 1.2	Enables the TLS 1.2 protocol.
Dispatch	<p>Sets the VPN tunnel option. This parameter is available when the Speed Tunnel is enabled. Four options are supported:</p> <ul style="list-style-type: none"> All Data Through TCP Tunnel: All data will be transmitted through the TCP tunnel. TCP Data Through TCP Tunnel: Only TCP data is transmitted through the TCP tunnel and other data is transmitted through the speed tunnel. TCP Data Through Speed Tunnel: TCP data is transmitted through the speed tunnel and other data is transmitted through

Parameter	Meaning
	<p>the TCP tunnel.</p> <ul style="list-style-type: none"> All Data Through Speed Tunnel: All data will be transmitted through the speed tunnel. <p>Note: Speed Tunnel supported by the UDP protocol is faster than the TCP Tunnel.</p>
Log Out VPN on Windows Logoff	Logs out the Array Client when the end user logs off Windows.
Proxy Script Setting	Selects which kind of script path works for your operating system and browser. Two options are supported: file:// and file:/// .

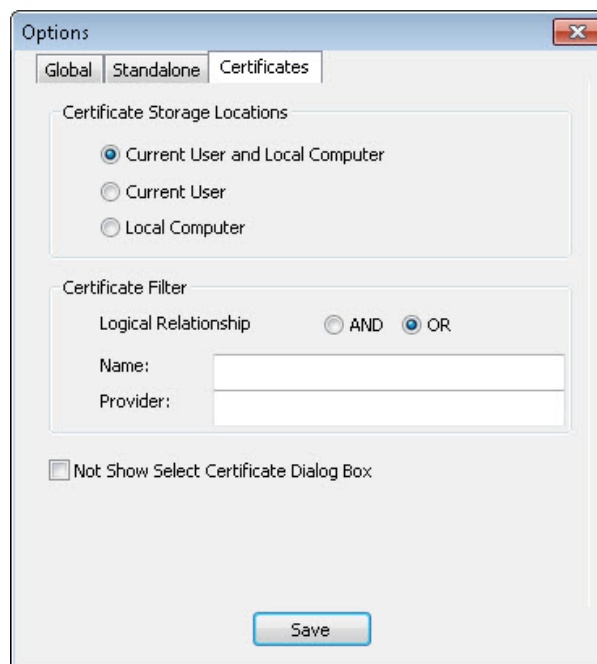
➤ Standalone Configuration



Parameter	Meaning
Auto Login to Windows	Auto logs in to the Windows when the Windows starts. When this check box is selected, the end users also need to specify the parameters Windows Username , Windows Password , and Re-Enter Password .
Lock Screen After Auto Login	Locks the screen after auto login to Windows. This check box is available only when the Auto Login to Windows check box is selected.
Auto Start on Windows Start	Starts the Array Client when the Windows starts.
Auto Connect on Launch	Enables the Array Client to automatically connect to the VPN server in the default profile when the Array Client starts up.
Auto Reconnect VPN on	Enables auto reconnection when the VPN connection is lost.

Parameter	Meaning
Disconnection	After this check box is selected, you also need to specify parameters Reconnect Interval and Reconnect Attempt . If the current VPN connection is lost, auto reconnection will performed at the specified interval for the specified number of reconnection attempts. If Reconnect Attempt is set to 0, auto reconnection attempts are performed for infinite times until the connection is restored or you exit the client.
Auto Reconnect on Invalid Session	Enables auto reconnection when the user session becomes invalid. This check box is available only when the Auto Reconnect on Disconnection check box is selected. After this check box is selected, you also need to specify parameters Reconnect Interval and Reconnect Attempt . If the user session becomes invalid, auto reconnection will performed at the specified interval for the specified number of reconnection attempts. If Reconnect Attempt is set to 0, auto reconnection attempts are performed for infinite times until the user session becomes valid or you exit the client.

➤ Certificates Configuration



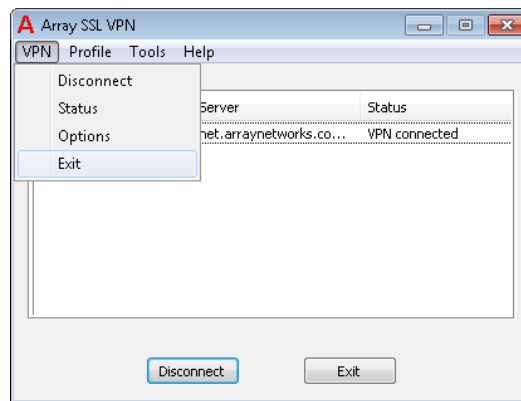
Parameter	Meaning
Certificate Storage Locations	Sets the certificate storage locations. Three options are supported: Current User and Local Computer , Current User , and Local Computer .
Certificate Filter	Configures certificate filter settings. The Name parameter is used to configure a certificate filter based on the certificate name while the Provider parameter is used to configure certificate filter based on the provider. The Logical Relationship parameter is used to specify

Parameter	Meaning
	the logical relationship between two certificate filters. The AND and OR options are supported.
Not Show Select Certificate Dialog Box	Whether to display the select certificate dialog box when the standalone client requires the certificate. When this check box is selected, the select certificate dialog box will not be displayed.

2.1.7 Exit the Array Client

To exit the Array Client, the end user should perform any of the following actions:

- In the main window, click the **Exit** button as shown in following figure.
- Click the **VPN** menu and select **Exit** from the prompted menu as shown in following figure.



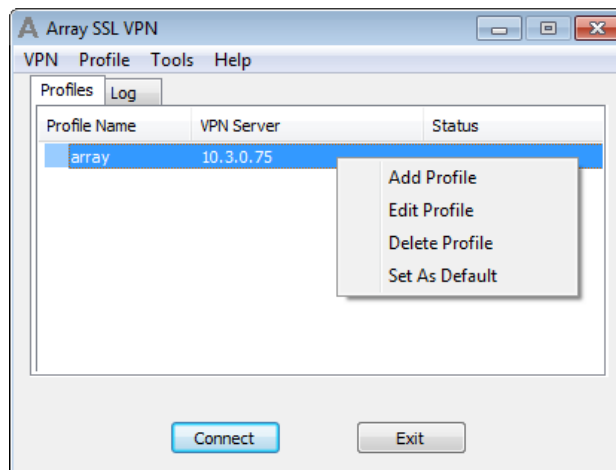
2.1.8 Manage a Profile

After a profile has been created, the end user can perform the following actions on the profile:

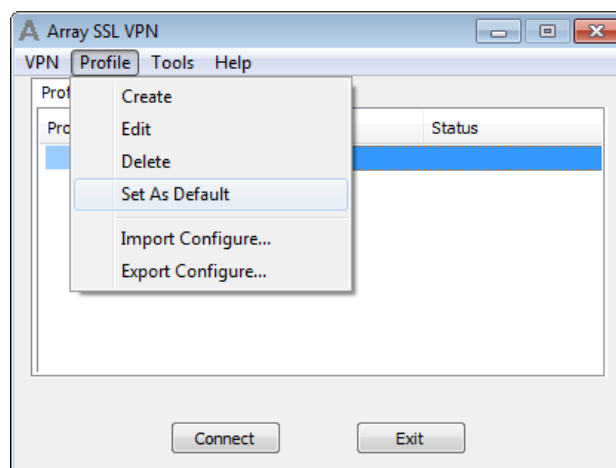
- Edit the profile
- Delete the profile
- Set the profile as default

To edit/delete an existing profile or setting it as the default profile, the end user should perform any of the following actions:

- Under the **Profiles** tab in the main window, right click the profile and select **Edit Profile**, **Delete Profile** or **Set As Default** in the prompted menu as shown in following figure.



- Under the **Profiles** tab in the main window, select the profile, click the **Profile** menu and select **Edit**, **Delete** or **Set As Default** from the prompted menu as shown in following figure.



Note:

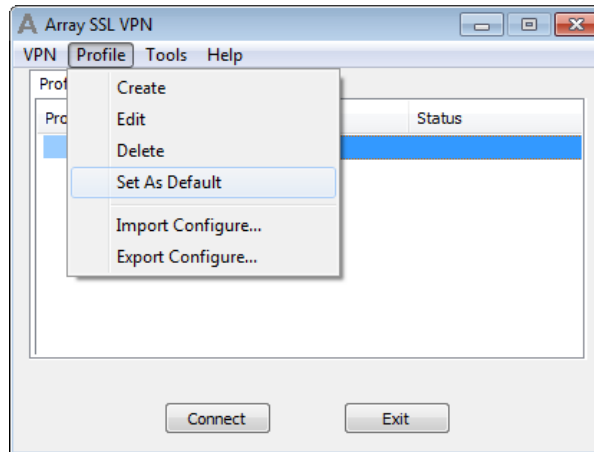
When setting a profile as the default profile, the end user does not need to select the profile before performing the connect action.

2.1.9 Import Profile(s)

The end user can import the profile(s) to the Array Client from an .ini file. The .ini file imported can contain one or more profiles. Only the default profile of the .ini file will be displayed.

To import the profile(s) to the Array Client, the end user should do as follows:

1. Click the **Profile** menu and select **Import Configure** from the prompted menu as shown in following figure.



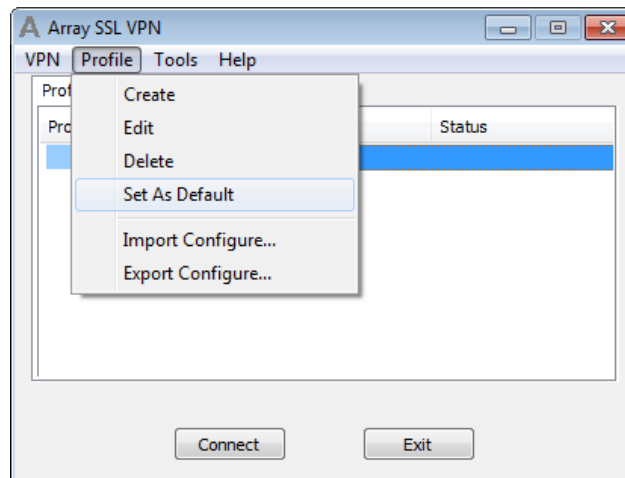
2. Find the .ini file in the local path and complete the import action.

2.1.10 Export the Profile

The end user can export the profile to an .ini file in the local path.

To export the profile, the end user should do as follows:

1. Under the **Profiles** tab in the main window, select the profile, click the **Profile** menu and select **Export Configure** from the prompted menu as shown in following figure.

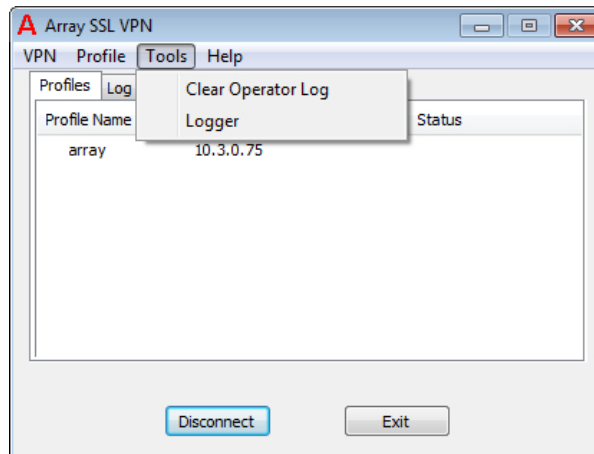


2. Specify the name of the .ini file and local path to save the file and complete the export action.

2.1.11 Start the Logger Tool

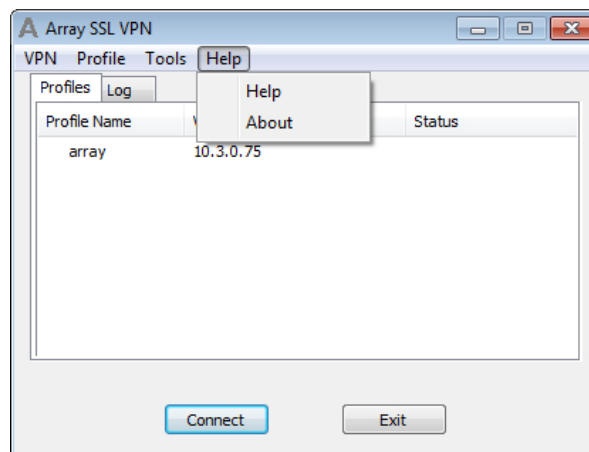
The Logger tool allows every operation performed by the Array Client to be recorded. Such information is very help for the administrator to debug Array Client failures.

To start the Logger tool, the end user should click the **Tools** menu and select **Logger** from the prompted menu, as shown in the following figure.



2.1.12 Obtain Help

The end user can obtain help information about the Array Client from the **Help** menu.



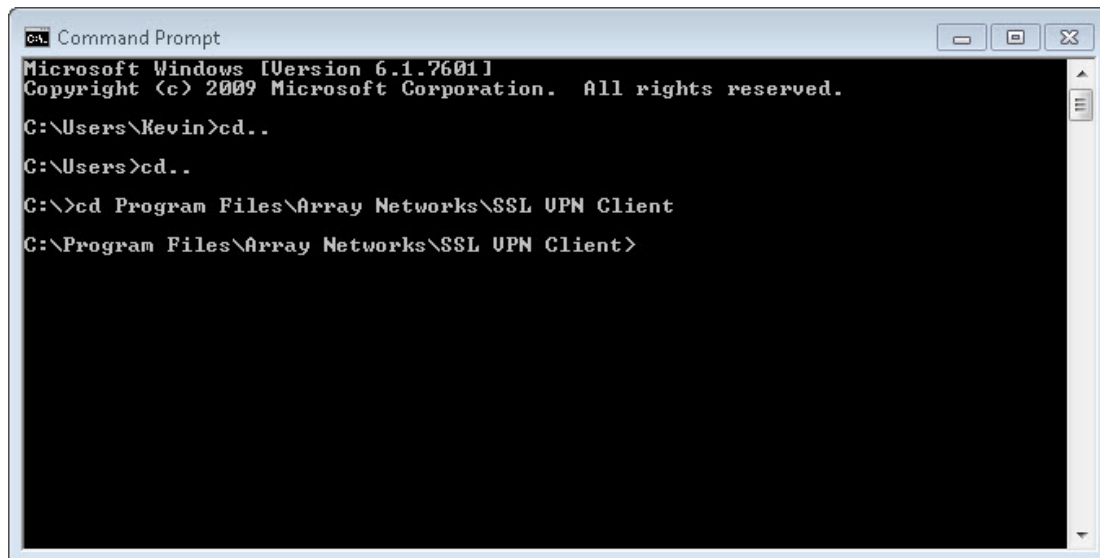
- Click **Help** to view the online help document for using the Array Client.
- Click **About** to view the version information about the Array Client.

2.2 Use the Standalone Array Client for Windows in Command Line Mode

After the Standalone Array Client for Windows has been installed, the end user can use the Standalone Array Client also in command line mode.

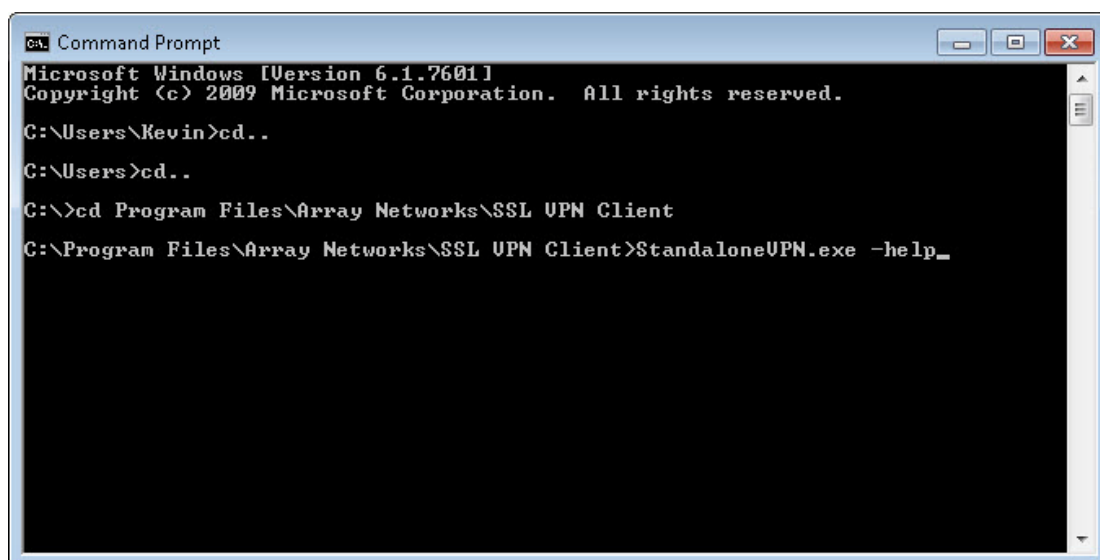
To use the Standalone Array Client in command line mode, the end user should do as follows:

1. Open the cmd.exe program and enter the path of Standalone.exe, for example C:\Program Files\Array Networks\SSL VPN Client.



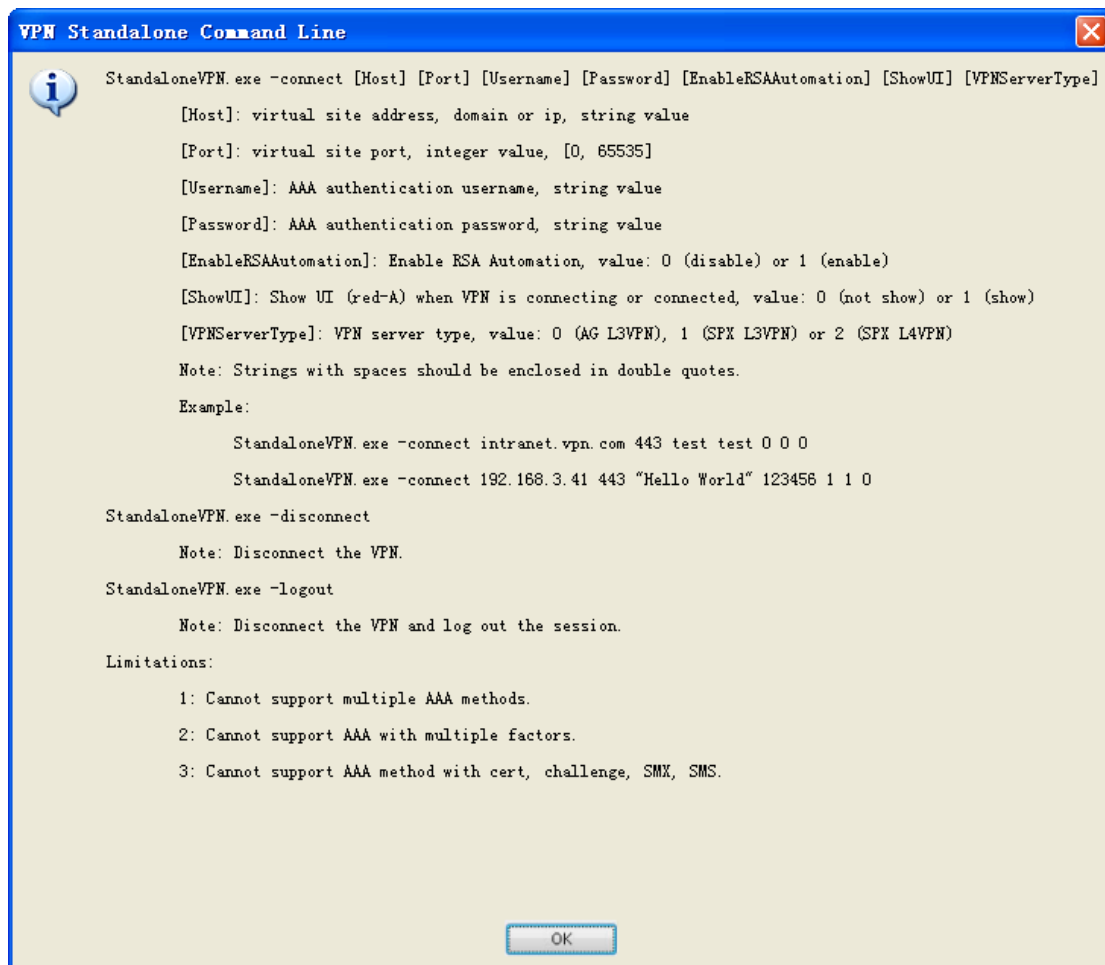
```
ca. Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Kevin>cd..
C:\Users>cd..
C:\>cd Program Files\Array Networks\SSL UPN Client
C:\Program Files\Array Networks\SSL UPN Client>
```

2. Execute the command "**Standalone.exe -help**" to see the help information about the command line mode.



```
ca. Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Kevin>cd..
C:\Users>cd..
C:\>cd Program Files\Array Networks\SSL UPN Client
C:\Program Files\Array Networks\SSL UPN Client>StandaloneUPN.exe -help_
```

3. Use the Standalone Array Client in command line mode according to the prompted window.



```
VPN Standalone Command Line

StandaloneVPN.exe -connect [Host] [Port] [Username] [Password] [EnableRSAAutomation] [ShowUI] [VPNServerType]

[Host]: virtual site address, domain or ip, string value
[Port]: virtual site port, integer value, [0, 65535]
[Username]: AAA authentication username, string value
[Password]: AAA authentication password, string value
[EnableRSAAutomation]: Enable RSA Automation, value: 0 (disable) or 1 (enable)
[ShowUI]: Show UI (red-A) when VPN is connecting or connected, value: 0 (not show) or 1 (show)
[VPNServerType]: VPN server type, value: 0 (AG L3VPN), 1 (SPX L3VPN) or 2 (SPX L4VPN)

Note: Strings with spaces should be enclosed in double quotes.

Example:
    StandaloneVPN.exe -connect intranet.vpn.com 443 test test 0 0 0
    StandaloneVPN.exe -connect 192.168.3.41 443 "Hello World" 123456 1 1 0

StandaloneVPN.exe -disconnect
    Note: Disconnect the VPN.

StandaloneVPN.exe -logout
    Note: Disconnect the VPN and log out the session.

Limitations:
    1: Cannot support multiple AAA methods.
    2: Cannot support AAA with multiple factors.
    3: Cannot support AAA method with cert, challenge, SMX, SMS.

OK
```


3 Standalone Array Client Customization

The administrator can customize the Standalone Array Client for Windows by modifying two files: the OEM.ini file and the Profiles.ini file.

3.1 OEM.ini Customization

OEM.ini file is stored in the installation package. After downloading and unzipping the package, the administrators can easily modify the OEM.ini file. After customization, the administrator needs to zip the package again with the modified OEM.ini file and then provide the updated package to end users.

An OEM.ini file contains two predefined sections: [Startup] and [Settings].

In the [Startup] section, the administrator can customize the following contents:

- **CompanyName:** specifies the company name.
- **ApplicationName:** specifies the (VPN Client) application name.
- **CompanyURL:** specifies the URL of the company's website.
- **ValidCode:** specifies the Valid Code used for Valid Code authentication.



Note: The Valid Code set in the OEM.ini must be same as that configured for the connecting virtual site on the AG. Otherwise, the VPN client is regarded as invalid by AG and the connection to the VPN server will be rejected.

In the [Settings] section, the administrator can customize the following contents:

- **IconOnStartMenu:** controls whether the VPN client icon is displayed on the start menu.
- **IconOnDesktop:** controls whether the icon of the VPN client is displayed on the desktop tray.
- **ChangePasswordURL:** specifies the URL of the change password page.
- **SecondaryProfileNameForReconnect:** specifies the hostname or IP address of the secondary virtual site to reconnect if the reconnection to the primary virtual site defined in the Profiles.ini file has failed for three times.

For detailed configuration description, please refer to the OEM_Help.pdf in the installation package.

3.2 Profiles.ini Customization

Profiles.ini is a configuration file containing one or more profiles with one profile as the default one. Usually, the administrator delivers Profiles.ini to the end users with login credentials. After the end users imported the Profiles.ini, users then can connect to VPN server in the default profile if required.

Array provides a template named profiles_templet.ini in the installation package, with which the administrators can easily create different Profiles.ini files for different end users.

For detailed configuration description, please refer to the section “How to Customize the profiles.ini File” of OEM_Help.pdf in the installation package.

4 Limitations

For the shared virtual site, the end user need to contain the alias name in the VPN Server text box when creating a profile, for example “www.example_test.com/alias1”.

The Standalone Array Client does not support the HTTPS (https://) protocol in the URL.

Appendix I Integrate with RSA Token

Automation

This appendix mainly introduces how to integrate the Standalone Array Client with the RSA SecurID software token. Only the Standalone Array Client for Windows supports this function.

With this function, when the end users try to establish the VPN connection via the Standalone Array Client, they only need to enter the PIN code instead of the token code or password. The Standalone Array Client will obtain the token code or password from the RSA SecurID Token Client. To achieve this goal, the end user needs to install the RSA SecurID Token Client on the PC and import the token file to the RSA SecurID Token Client.

I.1 Install RSA SecurID Token Client

The end user can download the installation package of the client from the official Website of RSA or obtain the installation package from Array Networks's FTP server:

- ftp://lake.arraynetworks.com.cn/R&DPublic/dev4public/AG_Standalone_with_RSA_SecurID_Token/RSA SecurIDToken411.zip (for 32-bit Windows)
- ftp://lake.arraynetworks.com.cn/R&DPublic/dev4public/AG_Standalone_with_RSA_SecurID_Token/RSA SecurIDToken412.zip (for 64-bit Windows)

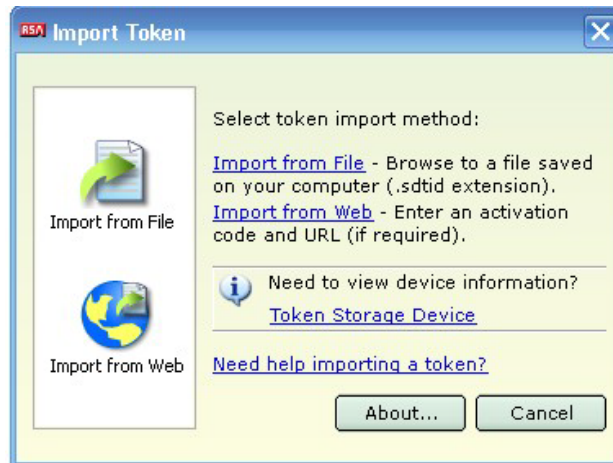
After obtaining the installation package:

- Run "RSA SecurIDTokenAuto411.msi" to install the RSA SecurID Token Client on 32-bit Windows OS.
- Run "RSA SecurIDTokenAuto412x64.msi" to install the RSA SecurID Token Client on 64-bit Windows OS.

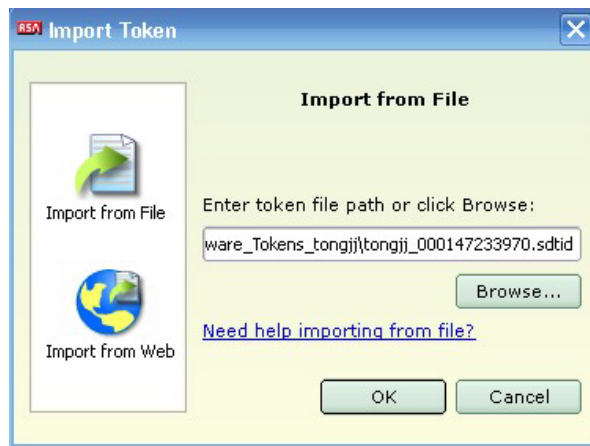
I.2 Import the Token File to RSA SecurID Token Client

To import the token file to the RSA SecurID Token Client, the end user should do as follows:

1. Obtain the token file from the administrator.
2. In the **Import Token** window, click the **Import from File** action link, as shown in the following figure.



3. Specify the path of the token file and click the **OK** button, as shown in the following figure.



After the token file is imported, the token file name will be the only name displayed on UI of the RSA SecurID Token Client, as shown in the following figure.



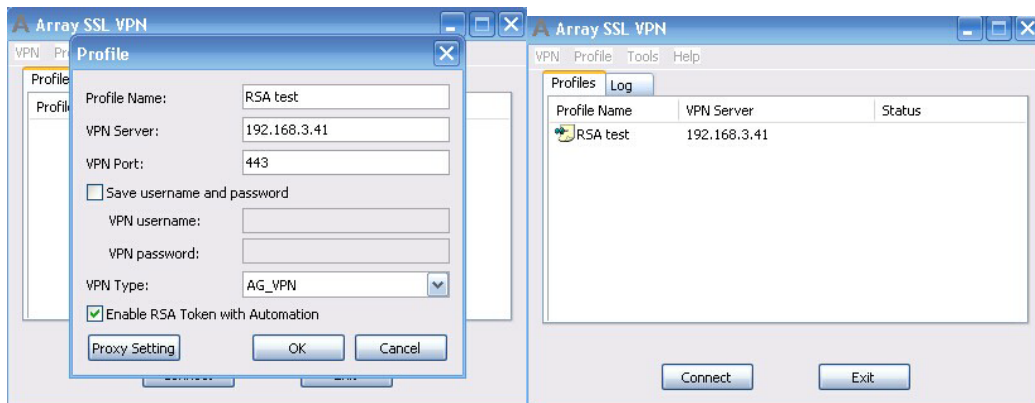
If more than one token file is imported, all the token files can be seen on the UI, as shown in the following figure.




After the token files are imported, you can exit the RSA SecurID Token Client. The Standalone Array Client can obtain the token code or passcode even when the RSA SecurID Token Client is not running.

I.3 Enable RSA Token with Automation

When creating the profile for the virtual site on the Standalone Array Client, select the **Enable RSA Token with Automation** check box, specify other parameters and click the OK button, as shown in the following figure.



 **Note:** This check box can be selected only when the virtual site uses RSA authentication.

The administrator can customize the Standalone Array Client to make this check box selected by default by modifying the OEM.ini file as follows before delivering the installation package to end users:

```
RSATokenAutomation=1 (value: 1-enable, 0-disable)
```

In this case, if the authentication method the virtual site uses is not RSA, such as LocalDB, the end user needs to clear this check box during authentication and enter the correct username and password, as shown in the following figure.



I.4 Authentication with RSA Token with Automation Enabled

➤ Authentication at First Login (Only RSA Authentication Used)

1. Under the **Profiles** tab of the main window, select the profile and click the **Connect** button.
2. In the displayed **Username And Password** dialog box, enter the username in the **Username** text box, leave the **Password** text box empty, and click the **OK** button as shown in the following figure.



3. In the displayed **Enter your new PIN** dialog box, specify the parameters **New PIN** and **Confirm** and click the **OK** button, as shown in the following figure.



Then the Standalone Array Client will perform authentication automatically and establish the VPN tunnel.

➤ **Authentication at Subsequent Logins (Only RSA Authentication Used)**

At subsequent logins, the end user does not need to set the new PIN code.

During the RSA authentication, in the **Username And Password** dialog box, enter the username in the **Username** text box, enter the PIN code in the **Password** text box, and click the **OK** button, as shown in the following figure.



➤ **Authentication at First Login (Multi-factor Authentication Including RSA)**

This part uses the LocalDB+RSA authentication as an example.

1. Under the **Profiles** tab of the main window, select the profile and click the **Connect** button.

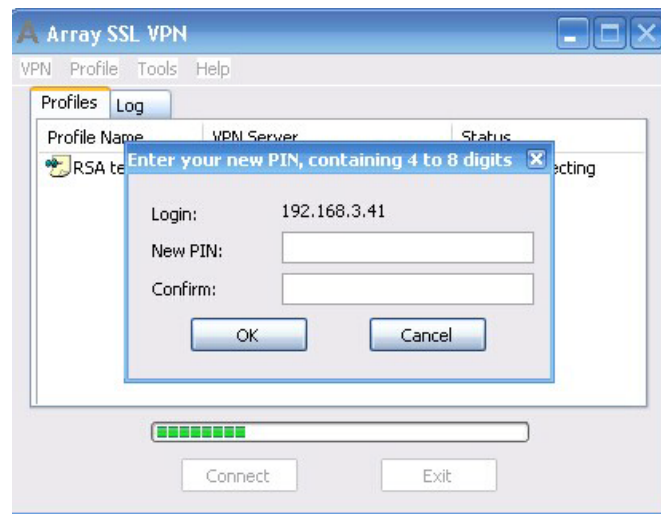
In the displayed Authenticate Information dialog box, select the LocalDB method name from the **Login Method** pane, specify the parameters **Username** and **Password For LocalDB** and click the **OK** button, as shown in the following figure.



2. Select the RSA method name from the **Login Method** pane, specify the parameters **Username**, leave the **Password For Radius** check box empty, and click the **OK** button, as shown in the following figure.



3. In the displayed **Enter your new PIN** dialog box, specify the parameters **New PIN** and **Confirm**, and click the **OK** button, as shown in the following figure.



The Standalone Array Client will perform authentication automatically and establish the VPN tunnel.

➤ **Authentication at Subsequent Logins (Multi-factor Authentication Including RSA)**

At subsequent logins, the end user does not need to set the new PIN code.

During the RSA authentication, Select the RSA method name from the **Login Method** pane, enter the username in the **Username** text box, enter the PIN code in the **Password for Radius** text box, and click the **OK** button, as shown in the following figure.

