NeoAccel makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. NeoAccel shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The product and company names mentioned in this document may be the trademarks of their respective owners. Throughout this document NeoAccel has attempted to distinguish trademarks from descriptive terms by writing the name with the capitalization used by the manufacturer, or by writing the name with initial capital letters. NeoAccel cannot attest to the accuracy of this information. Use of a trademark in this document should not be regarded as affecting the validity of the trademark.

Restrictions
Information in this document is subject to change without notice and does not represent a commitment on the part of NeoAccel. The software described in this manual is furnished according to a license agreement with NeoAccel. The license agreement contains all of the terms and conditions governing your use of the software and documentation, including all warranty rights, limitations of liability, and disclaimers of warranty. Material contained in this document may describe NeoAccel products not available or features not available in your country. No part of this material may be reproduced in any form or by any means without permission in writing from the publisher. Printed in India.

Edition history
Edition 1: November 2007
Edition 2: July 2008
Edition 3: March 2009

Copyright
All Rights Reserved. Copyright (C) 2009, NeoAccel Inc.
Contents

Contents .................................................................................................................................................. 3
Printing History .................................................................................................................................. 4
Conventions .......................................................................................................................................... 5
In This Manual .................................................................................................................................. 7
Audience ............................................................................................................................................... 7
Dynamic IP Address .......................................................................................................................... 8
  Dynamic IP Address Assignment for PHAT Clients ......................................................................... 8
    Add Dynamic IP Address Pool ......................................................................................................... 8
    Associate the IP pool to a Group ....................................................................................................... 10
    Modify Dynamic IP Address Pool .................................................................................................... 12
    Remove Dynamic IP Address Pool .................................................................................................. 13
    Disassociate the dynamic IP address pool from a group ................................................................. 13
    Remove forcefully the Dynamic IP Address Pool ......................................................................... 14
Private Network .................................................................................................................................. 16
  Add a private network profile .......................................................................................................... 16
  Associate the private network profile ............................................................................................... 17
  Modify a private network profile ...................................................................................................... 18
  Remove Private Network Profile Configuration ............................................................................... 19
  Disassociate private network profile from its group ......................................................................... 19
  Remove a Private Network Profile .................................................................................................. 20
  Remove Forcefully Private Network Profile .................................................................................... 20
Logon/Logoff Scripts .......................................................................................................................... 22
  Introduction ........................................................................................................................................ 22
    Add Logon/Logoff Script .................................................................................................................... 22
    Modify Logon/Logoff Script ............................................................................................................... 23
    View Logon/Logoff Script ................................................................................................................... 24
    Associate Logon/Logoff Script to a Group ...................................................................................... 25
    Remove Logon/Logoff Script ............................................................................................................ 27
    Remove Forcefully Logon/Logoff Script ............................................................................................ 28
Client Configuration ............................................................................................................................ 29
  Add a Client Configuration ................................................................................................................ 29
  Assign the Client Configuration to a Group ....................................................................................... 31
  Modify a Client Configuration ............................................................................................................ 32
  Remove a Client Configuration .......................................................................................................... 32
  Reassign the Client Configuration from a group ............................................................................... 33
  Remove Forcefully a Client Configuration ........................................................................................ 34
Creation and Configuration of Installation Package ............................................................................. 35
  Installation Package .......................................................................................................................... 35
    Add a Installation Package ................................................................................................................ 36
    Modify an Installation Package ......................................................................................................... 39
    Remove an Installation Package ....................................................................................................... 40
    Remove Forcefully an Installation Package ..................................................................................... 41
Printing History

The manual printing date and part number indicate its current edition. The printing date will change when a new edition is printed. Minor changes may be made at reprint without changing the printing date. The manual part number will change when extensive changes are made. Manual updates may be issued between editions to correct errors or document product changes. To ensure that you receive the updated or new editions, you should subscribe to the appropriate product support service.

Table 1 Edition History

<table>
<thead>
<tr>
<th>Product number</th>
<th>Revision Date</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>V2.1.2106</td>
<td>November 2007</td>
<td>NeoAccel SSL VPN-Plus™ Release v2.1</td>
</tr>
<tr>
<td>V2.2.2216</td>
<td>July 2008</td>
<td>NeoAccel SSL VPN-Plus™ Release v2.2</td>
</tr>
<tr>
<td>V2.3 2316</td>
<td>March 2009</td>
<td>NeoAccel SSL VPN-Plus™ Release v2.3</td>
</tr>
</tbody>
</table>
Conventions

Following conventions are used in this document

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Italic</strong></td>
<td>Document titles, and manual pages</td>
<td>Refer to NeoAccel SSL VPN-Plus™ User’s Guide for more information</td>
</tr>
<tr>
<td></td>
<td>Provides emphasis</td>
<td>You <em>must</em> install the NeoAccel kernel before installing other components</td>
</tr>
<tr>
<td></td>
<td>Specifies a variable that user should enter in a command</td>
<td>At command prompt, type <code>.displaytunnel tunn_id</code></td>
</tr>
<tr>
<td>Computer</td>
<td>Text and messages on computer screen</td>
<td>Error message is displayed: Bridge utils Package is not installed</td>
</tr>
<tr>
<td></td>
<td>Files and directory names</td>
<td>Run <code>.install.sh</code> script</td>
</tr>
<tr>
<td></td>
<td>Command names</td>
<td>Run <code>.displayprodinfo</code> command</td>
</tr>
<tr>
<td>![Note Icon]</td>
<td>This is a note icon. Notes include helpful background information, as well as reminders that may simplify your process.</td>
<td></td>
</tr>
<tr>
<td>![Warning Icon]</td>
<td>This is a warning icon. Whenever you see this warning symbol, READ THE CONTENTS CAREFULLY. By doing so, you will avoid common pitfalls that many encounter.</td>
<td></td>
</tr>
</tbody>
</table>
## Document Number Manuals

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SVP-UM-2.3-1011-09</td>
<td>NeoAccel Management Console – System Administration</td>
</tr>
<tr>
<td>SVP-UM-2.3-1012-09</td>
<td>NeoAccel Management Console – Gateway Administration</td>
</tr>
<tr>
<td>SVP-UM-2.3-1013-09</td>
<td>NeoAccel Management Console – Users/Groups</td>
</tr>
<tr>
<td>SVP-UM-2.3-1014-09</td>
<td>NeoAccel Management Console – Authorization</td>
</tr>
<tr>
<td>SVP-UM-2.3-1015-09</td>
<td>NeoAccel Management Console – Network Extension</td>
</tr>
<tr>
<td>SVP-UM-2.3-1016-09</td>
<td>NeoAccel Management Console – Portal</td>
</tr>
<tr>
<td>SVP-UM-2.3-1017-09</td>
<td>NeoAccel Management Console – Firewall</td>
</tr>
<tr>
<td>SVP-UM-2.3-1018-09</td>
<td>NeoAccel Management Console – Tools</td>
</tr>
<tr>
<td>SVP-UM-2.3-1019-09</td>
<td>NeoAccel Management Console – SNMP</td>
</tr>
<tr>
<td>SVP-UM-2.3-1020-09</td>
<td>NeoAccel Management Console – Logs</td>
</tr>
</tbody>
</table>

### Online Help

NeoAccel SSL VPN-Plus™ Management Console provides context-sensitive (F1) help and help topics for various operations.
In This Manual

The NeoAccel SSL VPN-Plus™ Network Extension Manual describes the configuration of Dynamic IP, Private Network, Logon/Logoff Client Configuration and Configuration of Installation Package.

Audience

The manual is intended for administrators who are responsible for maintaining the NeoAccel SSL VPN-Plus™ solution.
1 Dynamic IP Address

Dynamic IP Address Assignment for PHAT Clients

- NMC (NeoAccel Management Console) allows you as an administrator, to provide customized IP addressing for the remote users. It provides you with the function of assigning dynamic IP addresses (a feature common to any DHCP server) to all PHAT Client connections.
- Configure and assign the IP pools to groups. If you fail to configure Dynamic IP assignment for the remote users then TCP based applications would only function properly.
- Dynamic IP address Configuration list is the locally defined IP pools you are making available to full client users that are members of this group. These pools are configured in the Network Extension section, Dynamic IP address tab. This only applies to Full Client connections.

Add Dynamic IP Address Pool

1. Click on the node: Network Extension from the Content Panel in the NMC.

2. Click on the sub-node: Dynamic IP Address; A list of already configured IP address pool with its range and the Netmask details is displayed in the Display Screen. Refer to Figure 1.1

3. Click on the button: Add to add an IP pool; a dialog box: Create
Dynamic IP Address Configuration gets displayed. Refer to Figure 1.2

**Figure 1.2: Add IP Pool - General Tab**

4. Select the Tab: **General**.

5. Enter a **Name** for the IP pool that you want to create.

6. Enter the **IP Range** for the pool of IP addresses (for example: 192.168.10.20 to 192.168.10.25)

7. Enter the **Netmask** value to the range of IP addresses.

8. Click on the Tab: **Advanced**; to do DNS settings, the fields available in the advanced tab are all optional. These settings are specifically for PHAT Client. Refer to Figure 1.3
9. Enter the **Primary DNS** (if any). This is an optional field.

10. Enter the **Secondary DNS** (if any). This is an optional field.

11. Enter a **DNS suffix**. This is an optional field.

12. Enter the IP address of the Windows Server in the field: **WINS Server**. This is an optional field.

13. Click on the button: **OK** to add and save the IP pool.  
   Or
   Click on the button: **Cancel** if you do not want to add the IP pool
   To close the dialog box: **Create Dynamic IP Address Configuration**
   without saving any changes.

### Associate the IP pool to a Group

Perform the following steps to associate the IP pool to a particular Group:

1. Click on the tab: **Users/Groups** from the Content Panel in the NMC.

2. Click on the sub-node: **Groups**; A list of Groups with its access policies and group users is displayed in the Display Screen. Refer to Figure 1.4
3. Select the group to associate with, the IP pools created.

4. Click on the button: **Modify**; a dialog box: **Group Access Policies** is displayed. Refer to Figure 1.5
5. Select the tab: **Network Extension**, from the list of tabs displayed.

6. Click on the button: **Add**; a dialog box: **Add Dynamic IP address configurations** is displayed, from the list of ‘Available dynamic IP address’ select the IP address pool that you want to associate with the current group selection. *Refer to Figure 1.6*

![Figure 1.6: List of available dynamic IP addresses](image)

7. Click on the button: **Add** in the dialog box: **Add Dynamic IP address configurations** to save and close the dialog box.

8. Select the priority for the selected IP address pool in the ‘Network Extension’ tab.

9. Click on the button: **OK** in the dialog box: **Group Access Policies**, to save the association between the group and the IP address pool.  
   *Or*  
   Click on the button: **Cancel** to close the dialog box: **Group Access Policies** without saving any changes.

**Modify Dynamic IP Address Pool**

Perform the following steps to modify the dynamic address pool:

1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Dynamic IP Address**; A list of already configured IP address pool with its range and the netmask details is displayed in the Display Screen. *Refer to Figure 1.1*

3. Select the IP pool record that you want to modify.

4. Click on the button: **Modify**; a dialog box: **Modify Dynamic IP Address Configuration** will get displayed. *Refer to Figure 1.7*
4. Do the required modification and Click on the button: **OK** to save your updated configuration.

   Or

   Click on the button: **Cancel** to close the dialog box: **Modify Dynamic IP Address Configuration** without saving any changes.

---

**Remove Dynamic IP Address Pool**

*It is important to disassociate the IP pool addresses from any group association (it may have) before you remove any dynamic IP address pool.*

**Disassociate the dynamic IP address pool from a group**

Perform the following steps to disassociate the dynamic IP address pool from its group:

1. Click on the node: **Users/Groups** from the Content Panel in the NMC.

2. Click on the sub-node: **Groups**; A list of Groups with its access policies and group users is displayed in the Display Screen. Refer to Figure 1.4

3. Select the group from which to disassociate the IP pool created.

4. Click on the button: **Modify**; a dialog box: **Group Access Policies** gets displayed. Refer to Figure 1.5

5. Select the node: **Network Extension**.
6. Select the dynamic IP address configuration that needs to be disassociated from the group (in the Dynamic IP Address Configuration pane) and Click on the button: **Remove**.

7. Click on the button: **OK** in the dialog box: **Group Access Policies** to save the changes made.

Perform the following steps to Remove Dynamic IP Address Pool:

1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Dynamic IP Address**; A list of already configured IP address pool with its range and the netmask details is displayed in the Display Screen. *Refer to Figure 1.1*

3. Select the IP pool record that you want to remove and Click on the button: **Remove**; a confirmation prompt gets displayed. *Refer to Figure 1.8*

4. Click on the button: **Yes** to remove the IP pool record; the action removes the particular IP pool and the IP pool addresses list gets updated.

   Or

   Click on the button: **No** to close the confirmation prompt without saving any changes.

**Remove forcefully the Dynamic IP Address Pool**

*It may so happen that you have a long list of dynamic IP address pools associated with 'n’ number of user groups, and if you have to remove any of them you need to manually disassociate each of them from these user groups, before removing them. This becomes a highly cumbersome job to do. From version 2.3 of SSL VPN-Plus, the NMC provides a separate button called **Remove Forcefully**, wherein you can remove these dynamic IP address pools forcefully without manually disassociating them from any group(s).*

Perform the following steps to Remove Forcefully the Dynamic IP Address Pool:

1. Click on the node: **Network Extension** from the Content Panel in the NMC.
2. Click on the sub-node: **Dynamic IP Address**; A list of already configured IP address pool with its range and the netmask details is displayed in the Display Screen. *Refer to Figure 1.1*

3. Select the IP pool record that you want to remove forcefully and Click on the button: **Remove Forcefully** to remove the selected IP pool without manually disassociating it from the respective user group; a confirmation prompt is displayed. *Refer to Figure 1.9*

4. Click on the button: **Yes** to remove the IP pool record; the action removes the particular IP pool and the IP pool addresses list is updated. 

    Or

Click on the button: **No** to close the confirmation prompt without saving any changes.

**Figure 1.9:**
*Confirmation prompt for the forceful removal of dynamic IP address configuration*
2 Private Network

- Private networks are used to define what networks a user will have access to. It provides the routing for the end-user's access.

- Private network is also used to add routes to the local machine of the (PHAT) Client users to access networks other than the LAN of the Gateway.

- A remote user accesses the private network resources via an established tunnel.

- It is not an ACL. It is possible for a user to manually add routes to access other networks not defined.

- Use ACL’s in combination with the Private Networks listed.

- Either designate any subnets/hosts to the end user tunnel or exclude any subnets/hosts from the end user tunnels.

Within the sub-node: Private Network you can:

- Add a private network profile
- Modify a private network profile
- Remove a private network profile
- Remove Forcefully a private network profile

Figure 2.1: List of Private Network Profiles

Add a private network profile

Perform the following steps to add a private network profile:
1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Private Network**; A list of already configured private network profile details is displayed in the Display Screen. *Refer to Figure 2.1*

3. Click on the button: **Add**; a dialog box: **Create Private Network Profile** Configuration gets displayed. *Refer to Figure 2.2*

4. Enter a **Name** for the private network that you want to create.

5. Enter the IP address for the private network in the field: **Private Network**.

6. Enter the **Private Netmask** for the IP address.

7. Enter the IP address of the Gateway machine for the private network. This is an optional field.

8. Enter a range of port numbers to define the traffic route.

9. Click on the button: **OK** to save the configuration.
   
   Or
   
   Click on the button: **Cancel** to close the dialog box: Create Private Network Profile Configuration without saving any changes.

**Associate the private network profile**

Perform the following steps to associate the private network profile to a particular Group:

1. Click on the node: **Users/Groups** from the Content Panel in the NMC.
2. Click on the sub-node: **Groups**; A list of Groups with its access policies and group users is displayed in the Display Screen. Refer to Figure 1.4

3. Select the group to which you want to associate the private network profile created and click on the button: **Modify**; a dialog box: **Group Access Policies** gets displayed. Refer to Figure 1.5

4. Select the tab: **Network Extension**, in the Private Network List pane, Click on the button: **Add**; a dialog box: **Add Private Networks**, get displayed, from the list of ‘Available Networks’ select the private network profile that you want to associate with the current group selection. Refer to Figure 2.3

![Add Private Networks dialog box](image)

4. Click on the button: **Add** in the dialog box: **Add Private Networks**; it will save and close the dialog box.

5. Select the priority for the selected Private Network Profile in the ‘Network Extension’ tab.

6. Select an option, from the drop-down box: **ICAA**; the additional option includes the option either to exclude or Disable or Enable ICAA (Intelligent Connection Access Architecture)

7. Click on the button: **OK** in the dialog box: **Group Access Policies**, to save the association between the group and the Private Network Profile.

   Or

   Click on the button: **Cancel** to close the dialog box: Group Access Policies without saving any changes.

   - **By default during installation the private network adapter subnet will be auto-created for assignment.**

   - **ICAA is the patent pending technology that enables the remote users to have quick and efficient access to the VPN resources. In certain instances such as VOIP you may need to add the IP address for the VOIP server and set the ICAA option as disabled.**

**Modify a private network profile**
Perform the following steps to modify a private network profile:

1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Private Network**; A list of already configured Private Network Profile details is displayed in the Display Screen. Refer to Figure 2.1

3. Select the profile of a private network that you want to modify.

4. Click on the button: **Modify**; a dialog box: **Modify Private Network Profile Configuration**. Refer to Figure 2.4

5. Do the required modification and Click on the button: **OK** to save and update the configurations.

   Or

   Click on the button: **Cancel** to close the dialog box without saving any changes.

---

**Remove Private Network Profile Configuration**

*It is important to disassociate the private network profile configuration from any group association (it may have) before you remove any private network profile.*

**Disassociate private network profile from its group**

Following are the steps to **disassociate** the **private network profile** from its **group**:

1. Click on the node: **Users/Groups** from the Content Panel in the NMC.

2. Click on the sub-node: **Groups**; A list of Groups with its access policies
and group users is displayed in the Display Screen. Refer figure 1.4

3. Select the group from which you want to disassociate the private network profile created and click on the button: Modify; a dialog box: Group Access Policies gets displayed. Refer figure 1.5

4. Select the tab: Network Extension.

5. Select the dynamic private network profile that needs to be disassociated from the group (in the Private Network List pane) and Click on the button: Remove.

6. Click on the button: OK in the dialog box: Group Access Policies; this will save the changes made.

**Remove a Private Network Profile**

Perform the following steps to Remove a Private Network Profile:

1. Click on the node: Network Extension from the Content Panel in the NMC.

2. Click on the sub-node: Private Network; A list of already configured private network profiles is displayed in the Display Screen. Refer figure 2.1

3. Select the private network profile that you want to remove and Click on the button: Remove; a confirmation prompt gets displayed. Refer to Figure 2.5

4. Click on the button: Yes to remove the private network profile; it closes the confirmation prompt, and removes the particular private network profile. The Private Network Profile Configuration list also gets updated.

   Or

   Click on the button: No to avoid removal of the private network profile to close the confirmation prompt without saving any changes.

**Remove Forcefully Private Network Profile**

It may so happen that you have a long list of private network profiles associated with 'n' number of user groups, and if you have to remove any of them you need to manually disassociate each of them from these user groups, before removing them. This becomes a highly cumbersome job to
do. From version 2.3 of SSL VPN-Plus, the NMC provides a separate button called **Remove Forcefully**, wherein you can remove these dynamic IP address pools forcefully without manually disassociating them from any group(s).

Perform the following steps to Remove Private Network Profile:

1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Private Network**; A list of already configured private network profiles is displayed in the Display Screen. *Refer figure 2.1*

3. Select the private network profile that you want to remove and Click on the button: **Remove Forcefully** to remove the selected network profile without manually *disassociating* it from the respective user group; a confirmation prompt is displayed. *Refer to Figure 2.6*

4. Click on the button: **Yes** to remove the private network profile; it closes the confirmation prompt, and removes the particular private network profile. The Private Network Profile Configuration list also gets updated.

   *Or*

   Click on the button: **No** to avoid removal of the private network profile to close the confirmation prompt without *saving* any changes.
3 Logon/Logoff Scripts

Introduction

- Script can be any batch file: *.bat or VB Script: *.vbs or Java Script: *.js or a shell script: *.sh
- A script is executed on Operating Systems such as Windows, Linux and Macintosh.
- Login/Logoff Scripts integrated with the Client provides you as an administrator, a mechanism to execute a set of operations either after the user login or before the user logs off.
- After the Script is uploaded, associate the script to an existing Group(s), specifically specified as Logon/Logoff and also set their respective priority.

Figure 3.1: List of Logon/Logoff scripts

Following functions are performed under the sub-node: Logon/Logoff Scripts:

- Add Logon/Logoff Script
- Modify logon/Logoff Script
- View Logon/Logoff Script
- Remove Logon/Logoff Script
- Remove Forcefully logon/Logoff Script

Add Logon/Logoff Script

Perform the following steps to add Logon/Logoff Scripts:
1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Logon/Logoff Scripts**; A list of existing Logon/Logoff scripts are displayed in the Display Screen. *Refer figure 3.1*

3. Click on the button: **Add** to add a Logon/Logoff script; a dialog box: **Add** is displayed. *Refer to Figure 3.2*

![Add Script](image)

4. Browse and enter the script file name in the field: **Script**

5. Select (either PHAT/QAT or both) from the option: **Run Script For** to run the Logon/Logoff script on.

6. Click on the button: **Add** to add and save the script file.
   Or
   Click on the button: **Cancel** to close the dialog box: **Add** without saving and changes.

**Modify Logon/Logoff Script**

Perform the following steps to modify an existing Logon/Logoff Script:

1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Logon/Logoff Scripts**; A list of existing Logon/Logoff scripts are displayed in the Display Screen. *Refer figure 3.1*

3. Select the particular Logon/Logoff Script to Modify.

4. Click on the button: **Modify** to modify the particular Logon/Logoff script; a dialog box: **Modify Script** is displayed. *Refer to Figure 3.3*
5. Click on the button: **Modify** to apply the changes.

   Or

   Click on the button: **Cancel** to close the dialog box: **Modify Script**

**View Logon/Logoff Script**

1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Logon/Logoff Scripts**; A list of existing Logon/Logoff scripts are displayed in the Display Screen. Refer figure 3.1

3. Select the particular Logon/Logoff Script to view.

4. Click on the button: **View** to view the particular Logon/Logoff script; a dialog box: **View Script** is displayed. Refer to Figure 3.4

5. Click on the button: **OK** to close the dialog box: **View Script**.
**Associate Logon/Logoff Script to a Group**

Perform the following steps to associate a Logon/Logoff script to any existing group:

1. Click on the node: **Users/Groups** from the Content Panel in the NMC.

2. Click on the sub-node: **Groups**; A list of existing groups are displayed in the Display Screen. Refer figure 3.5

3. Select the particular group to associate Logon/Logoff Scripts with.

4. Click on the button: **Modify** to open the dialog box: **Group Access Policies**.

5. Select Tab: **Logon/Logoff Scripts**. Refer to Figure 3.6
Figure 3.6:
Tab: Logon/Logoff Scripts in the dialog box: Group Access Policies

6. Click on the button: **Add** to open the dialog box: **Add Script. Refer to Figure 3.7**

Figure 3.7: Select scripts for association with the Group

7. Select the available Logon/Logoff script from the displayed list.

8. Click on the button: **Add** in the dialog box: **Add Script** Refer to Figure 3.9; the script gets listed in the Tab: **Logon/Logoff Scripts**.

9. Select and specify the type for each script displayed, from the drop-down box under the column: **Type Refer to Figure 3.8**
Figure 3.8: Select the 'Type' for the script and set its priority.

10. Select a priority for each script displayed from the spinner box under the column: **Priority**. Refer to Figure 3.10

11. Click on the button: **OK** to save the association of the Logon/Logoff Scripts with the selected group.
   Or
   Click on the button: **Cancel** to close the dialog box: **Group Access Policies** without saving any changes.

**Remove Logon/Logoff Script**

*It is important to disassociate the Logon/Logoff scripts from any group association (it may have) before you remove any Logon/Logoff script.*

Perform the following steps to remove Logon/Logoff script:

1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Logon/Logoff Scripts**; A list of existing Logon/Logoff scripts are displayed in the Display Screen. Refer figure 3.1

3. Select the particular Logon/Logoff Script to delete.

4. Click on the button: **Remove** to remove the particular Logon/Logoff script; a confirmation prompt: **Confirm Remove Script** is displayed. Refer to Figure 3.9
Figure 3.9: Confirm Script removal

5. Click on the button: Yes to remove the script.
   Or
   Click on the button: No to close the prompt: Confirm Remove Script without any changes.

Remove Forcefully Logon/Logoff Script

To remove a list of Logon/Logoff scripts already associated with 'n' number of user groups; you need to manually disassociate each of them from these user groups, before removing them. This becomes a highly cumbersome job to do. From version 2.3 of SSL VPN-Plus, the NMC provides a separate button called Remove Forcefully, wherein you can remove these Logon/Logoff scripts forcefully without manually disassociating them from any group(s).

Perform the following steps to remove forcefully a Logon/Logoff script:

1. Click on the node: Network Extension from the Content Panel in the NMC.

2. Click on the sub-node: Logon/Logoff Scripts; A list of existing Logon/Logoff scripts are displayed in the Display Screen. Refer figure 3.1

3. Select the particular Logon/Logoff Script to delete forcefully.

4. Click on the button: Remove Forcefully to remove the selected logon script without manually disassociating it from the respective user group; a confirmation prompt: Confirm Remove Script is displayed. Refer to Figure 3.10

Figure 3.10: Confirm forceful removal of Script

5. Click on the button: Yes to remove the script.
   Or
   Click on the button: No to close the prompt: Confirm Remove Script without any changes.
4 Client Configuration

- The Client Configuration applies to PHAT Client only.

- It provides various options to controlling the end user experience such as Auto-Reconnect and EPS feedback information.

- Client Configuration options are bound to Groups.

- PHAT Client supports application persistence by default from version 2.3 onwards. Applications connected to the private network resources via PHAT Client if disconnected tries to reconnect continuously (a auto-reconnect feature of the Gateway) at the same time the TCP application connection (via PHAT Client) is kept alive so that application persistence is achieved once a successful connection is established.

Configure the following configurations for the PHAT Client users:

- Name
- Auto-Reconnect options
- Idle Timeout – default 30 minutes
- Forced Timeout – default 30 minutes
- Enable System Rescan – for EPS
- Rescan Client System after XX seconds
- Show Endpoint Security details to user
- Uninstall (PHAT) Client on logout
- Fallback to DHCP for IP address assignment
- Keep SSL VPN-Plus™ session alive after Windows logoff

Perform the following functionality in the sub-node: Client Configuration:

- Add Client Configuration.
- Modify Client Configuration.
- Remove Client Configuration.
- Remove Forcefully Client Configuration.

Add a Client Configuration

Perform the following steps to add a client configuration:
1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Client Configuration**; A list of already configured Clients are displayed in the Display Screen.

3. Click on the button: **Add**; a dialog box: **Add Client Configuration** is displayed

4. Enter a **Name** for the (PHAT) Client configuration.

5. Check the checkbox: **Enable auto reconnect**, to automatically reconnect the PHAT client in any event of dropped connection.

6. Either enter a constant value of retries you want the client to try in an attempt to reconnect (by default the constant value is ‘3’) in the field: **Number of retries**

   Or
   
   Check the checkbox: **Infinite Retries**, the client will try infinitely to reconnect to the Gateway in an event of dropped connection.

7. Check the checkbox: **Enable client systems** rescan to let PHAT client to scan the EPS policies of the user’s machine within a particular time interval.

8. Set the time interval for every rescan; enter the value in seconds in the field: **Rescan client system after**.

9. Check the checkbox: **Show Endpoint Security details to user** to display the EPS details to the user at the time of successful authentication.

10. Check the checkbox: **Uninstall client on logout to allow** the (PHAT) Client to uninstall itself as soon as the end-user logs-out. At times the end-user may be asked for a reboot.

11. Check the checkbox: **Fall back to DHCP for IP Address**
**Figure 4.2:** Assigning Client Configuration to a Group

**Assign the Client Configuration to a Group**

Perform the following steps to Assign the Client Configuration to a particular Group:

1. Click on the node: Users/Groups from the Content Panel in the NMC.

2. Click on the sub-node: Groups; A list of Groups with its access policies and group users is displayed in the Display Screen.

3. Select the group to which you want to assign the client configuration created.

4. Click on the button: Modify; a dialog box: Group Access Policies is displayed.

5. Select the node: Network Extension. Refer to Figure 4.2

6. Select the configuration from the drop down box: Client Configuration Name.
7. Click on the button: **OK** in the dialog box: Group Access Policies, to save and apply the change.  
   Or  
   Click on the button: **Cancel** to close the dialog box: Group Access Policies without saving any changes.

**Modify a Client Configuration**

1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Client Configuration**; A list of already configured Clients are displayed in the Display Screen. Refer to Figure 4.3

3. Select a particular configuration that requires modification.

4. Click on the button: **Modify**; a dialog box: **Modify Client Configuration** gets displayed.

5. Do the required modification.

6. Click on the button: **OK** to save and update the modification.  
   Or  
   Click on the button: **Cancel** to close the dialog box: **Modify Client Configuration** without saving any changes.

**Remove a Client Configuration**

It is important to reassign the client configuration from the group before
removing any client configuration.

**Reassign the Client Configuration from a group**

Perform the following steps to re-assign the client configuration from a group:

1. Click on the node: **Users/Groups** from the Content Panel in the NMC.
2. Click on the sub-node: **Groups**; A list of Groups with its access policies and group users is displayed in the Display Screen.
3. Select the group to which is assigned the client configuration you want to remove and click on the button: **Modify**; a dialog box: **Group Access Policies** gets displayed.
4. Select the node: **Network Extension. Refer to Figure 4.4**
5. Select the option, 'Select' from the drop-down: **Client Configuration Name**. This step reassigns the client configuration from its group.
6. Click on the button: **OK** in the dialog box: **Group Access Policies**, to save and apply the change.  
   Or
   Click on the button: **Cancel**; it will close the dialog box: Group Access Policies without saving any changes.

Perform the following steps to **Remove the client configuration**:

1. Click on the node: **Network Extension** from the Content Panel in the NMC.
2. Click on the sub-node: **Client Configuration**; A list of already configured Clients are displayed in the Display Screen. Refer to **Figure 4.3**
3. Select the particular configuration you want to remove.
4. Click on the button: **Remove**; a confirmation prompt is displayed. Refer to **Figure 4.5**
Remove Forcefully a Client Configuration

To remove a list of client configurations already associated with ‘n’ number of user groups; you need to manually disassociate each of them from the respective user groups, before removing them. This becomes a highly cumbersome job to do. From version 2.3 of SSL VPN-Plus, the NMC provides a separate button called **Remove Forcefully**, wherein you can remove these client configurations forcefully without manually disassociating them from any group(s).

Perform the following steps to Remove Forcefully the client configuration:

1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Client Configuration**; A list of already configured Clients are displayed in the Display Screen. **Refer to Figure 4.3**

3. Select the particular configuration you want to remove.

4. Click on the button: **Remove Forcefully** to remove the selected client configuration without manually reassigning to the respective user group; a confirmation prompt is displayed. **Refer to Figure 4.6**

5. Click on the button: **Yes** to close the confirmation prompt and remove the Client Configuration.

   Or

   Click on the button: **No** to close the confirmation prompt without saving any changes.
5 Creation and Configuration of Installation Package

This chapter introduces the configuration of PHAT client installation packages.

Multiple packages can be created and assigned to Groups to allow the administrator to apply different options.

Installation Packages can also be created for

- Linux Operating Systems
- Macintosh OSX operating system 10.4 and above

Installation Package

By default at installation a base client installation package is created named NeoAccel Remote Access. The administrator should remove this base package and configure at least one customized package for user by remote users.

Perform the following functions in the sub-node: **Client Configuration:**

- Add Installation Package.
- Modify Installation Package.
- Remove Installation Package.
- Remove Forcefully Installation Package.

![Figure 5.1: List of Installation Package configurations](image)
Add a Installation Package

1. Click on the node: **Network Extension** from the Navigation Panel in the NMC.

2. Click on the sub-node: **Installation Package**; A list of already configured Installation Packages are displayed in the Content Panel. *Refer to Figure 5.1*

3. Click on the button: **Add**; a dialog box: **Add Installation Package** gets displayed. *Refer to Figure 5.2*
Creation and Configuration of Installation Package

Figure 5.2: Add Installation Package dialog box

4. Enter a name that identifies the network and to which the clients could connect to, in the field: **Profile Name**. The name entered is also visible in the PHAT client drop down selector. *Refer to Figure 5.3*

Figure 5.3: Select a network

5. Enter the IP Address of the SSL VPN-Plus™ Gateway in the field: **Gateway**. This can be a Fully Qualified Domain Name (FQDN)

6. Enter the **Port** number in the field: **Port** that the client will establish a tunnel with. This should correspond with the configured gateway port number, example: 443

7. Click on the button: **Add**, to add single or multiple FQDN or IP addresses to configure client redundancy.  
   Or  
   Select a IP address and Click on the button: **Remove** to remove the IP address

8. Select the option: **Create Linux Client Installations**, to create PHAT client installation files for Linux clients.
9. Select the option: **Create MAC Client Installations**, to create PHAT client installation files for MAC OS-X clients.

10. In the Installation Parameters pane, select the option: **Start client on Logon** to start the PHAT client at Windows logon. After the user logs onto Windows the client will be running waiting for user intervention.

11. Select the option: **Hide Client System Tray Icon** to hide the system tray icon on the Windows sub-node tray from the end users.

12. Select the option: **Allow Remember Password** to allow the end user to save their user logon name and password for future use.

13. Select the option: **Enable Silent Mode Operation** to reduce the number of dialogue boxes presented to an end user.

14. Select the option: **Enable Silent Mode Installation** to silently install the PHAT client.

15. Select the option: **Hide SSL VPN-PlusTM** network adapter to hide the Virtual Adapter from network properties and the system tray.

16. Select the option: **Create Desktop Icon** to place the NeoAccel SSL VPN-PlusTM icon on the end-users desktop for easy accessibility and use.

17. Select the option: **Enforce Server Security Certificate Validation** to have the PHAT client validate the SSL Server Certificate that is bound the gateway.

- By default the remote client’s installable files are found in
  `/opt/sslvpn-plus/wwwroot/phatclient/client`

- If you are creating more than one PHAT client package you must specify a different “name” for the package than the default ‘client’. Using ‘client’ will overwrite the default package.

- If a (PHAT) Client is set in auto launch mode then it would be appropriate if the options: Enable silent mode operation and Enable silent mode installation are selected.

**Associate the Installation Package to a Group**

Perform the following steps to associate the Installation Package to a particular Group:

1. Click on the node: **Users/Groups** from the Content Panel in the NMC.

2. Click on the sub-node: **Groups**; A list of Groups with its access policies and group users is displayed in the Display Screen.

3. Select the group to which you want to associate the Installation
Package created.

4. Click on the button: **Modify**, a dialog box: **Group Access Policies** is displayed.

**Figure 5.4:**
**Associating Installation Package in tab: Portal Resources**

5. Select the tab: **Portal**, scroll down to the section: **PHAT Client Installation Packages List**. Refer to **Figure 5.4**

6. Select the Installation Package profile listed to associate it to the Group selected.

7. Click on the button: **OK** to apply the association.
   
   Or
   
   Click on the button: **Cancel** to close the dialog box: **Group Access Policies** without making any changes.

**Modify an Installation Package**

Perform the following steps to modify an installation package:

1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Installation Package**; A list of already configured Installation Packages are displayed in the Display Screen. Refer to **Figure 5.1**

3. Select an Installation Package and click on the button: **Modify**; a dialog box: **Modify Installation Package** gets displayed. Refer to **Figure 5.5**
Figure 5.5: Modify Installation Package dialog box

4. Do the required modification and click on the button: **OK** to save and update the changes.

   Or

   Click on the button: **Cancel** to close the dialog box: **Modify Installation Package** without saving any changes.

   Except for the fields: **Community Name** and **Output Directory** all the other fields are modifiable.

**Remove an Installation Package**

It is important to reassign the client configuration from the group before removing any client configuration.

Perform the following steps to remove an installation package:

1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Installation Package**; A list of already configured Installation Packages are displayed in the Display Screen. **Refer to Figure 5.1**

3. Select an Installation Package and click on the button: **Remove**; a confirmation prompt gets displayed. **Refer to Figure 5.6**

4. Click on the button: **Yes** to remove the Installation Package; it will close the confirmation prompt and remove the Installation Package.
Or
Click on the button: **No** to close the confirmation prompt without saving any changes.

**Remove Forcefully an Installation Package**

To remove a list of installation packages already associated with ‘n’ number of user groups; you need to manually disassociate each of them from the respective user groups, before removing them. This becomes a highly cumbersome job to do. From version 2.3 of SSL VPN-Plus, the NMC provides a separate button called **Remove Forcefully**, wherein you can remove these installation packages forcefully without manually disassociating them from any group(s).

1. Click on the node: **Network Extension** from the Content Panel in the NMC.

2. Click on the sub-node: **Installation Package**; A list of already configured Installation Packages are displayed in the Display Screen. **Refer to Figure 5.1**

3. Select an Installation Package and click on the button: **Remove Forcefully** to remove the selected installation package without manually disassociating it from the respective user group; a confirmation prompt is displayed. **Refer to Figure 5.7**

![Confirm forceful removal of Client configuration](image)

5. Click on the button: **Yes** to remove the Installation Package; it will close the confirmation prompt and remove the Installation Package. **Or**

Click on the button: **No** to close the confirmation prompt without saving any changes.