

SSL VPN-Plus™

Quick Configuration Guide ver 2.1



SSL VPN-Plus – Components

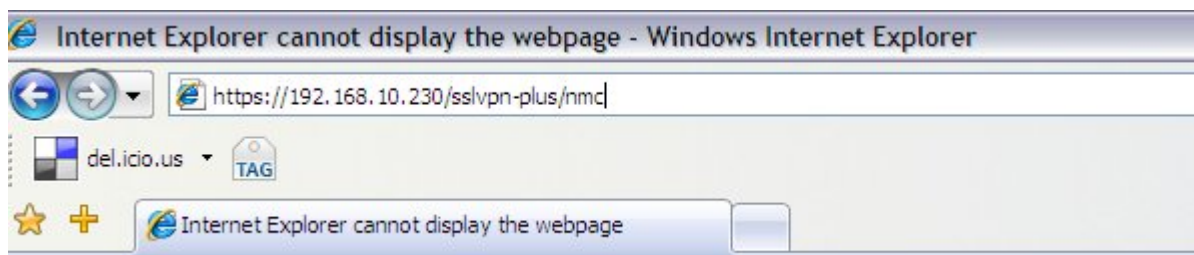
- **SSL VPN-Plus Gateway**
 - Installs on any x86 based hardware, on Linux platform
- **SSL VPN-Plus Management Console**
 - Java based console to manage SSL VPN-Plus gateway
- **SSL VPN-Plus Access Terminals**
 - Web Access Terminal (Clientless SSL VPN) for web-based application access through browser
 - Quick Access Terminal Client for any TCP client-server and web-based application access without installing any client on user machine
 - Private Hyper Access Terminal Client (Full Access Client), an IPSec replacement client for full, simple and transparent network connectivity with complete access control

Prerequisites: Software

- Management Console
 - Require JRE 1.4.2 or above on administrator's PC
- Access Terminals
 - WAT: IE 5.0 & above, Firefox, NetScape
 - QAT: Windows 2000 family & Windows XP family
 - PHAT: Windows 2000 family & Windows XP family, Red Hat 9.0, Red Hat EL 3, Knoppix, Debian, MAC OSX 10.4

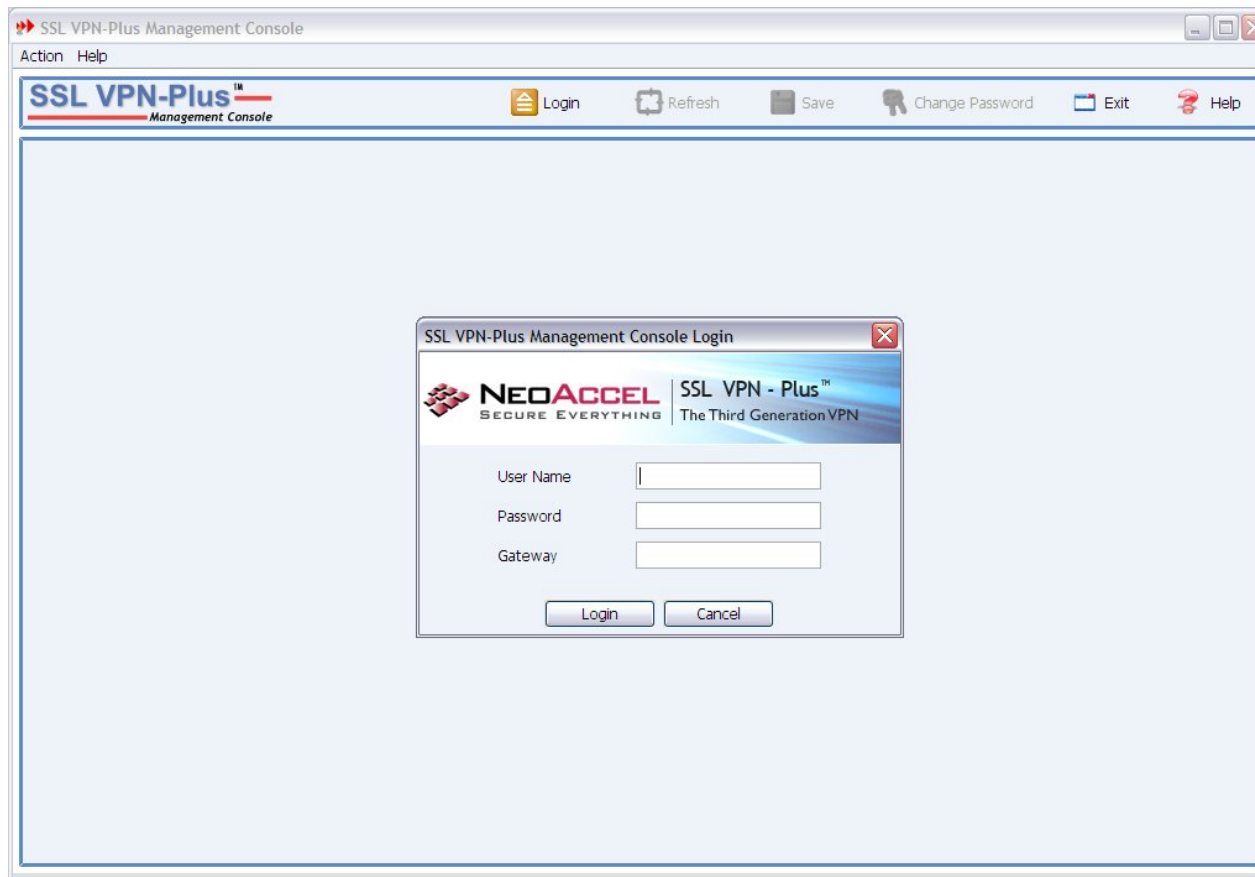
Access Management Console

- Open URL: `https://<WAN side IP address of gateway machine>/sslvpn-plus/nmc/`
 - Example: <https://vpn.corporate.net/sslvpn-plus/nmc/>
- Default WAN IP address is the WAN IP address of eth0 port which is 192.168.10.230
 - <https://192.168.10.230/sslvpn-plus/nmc>



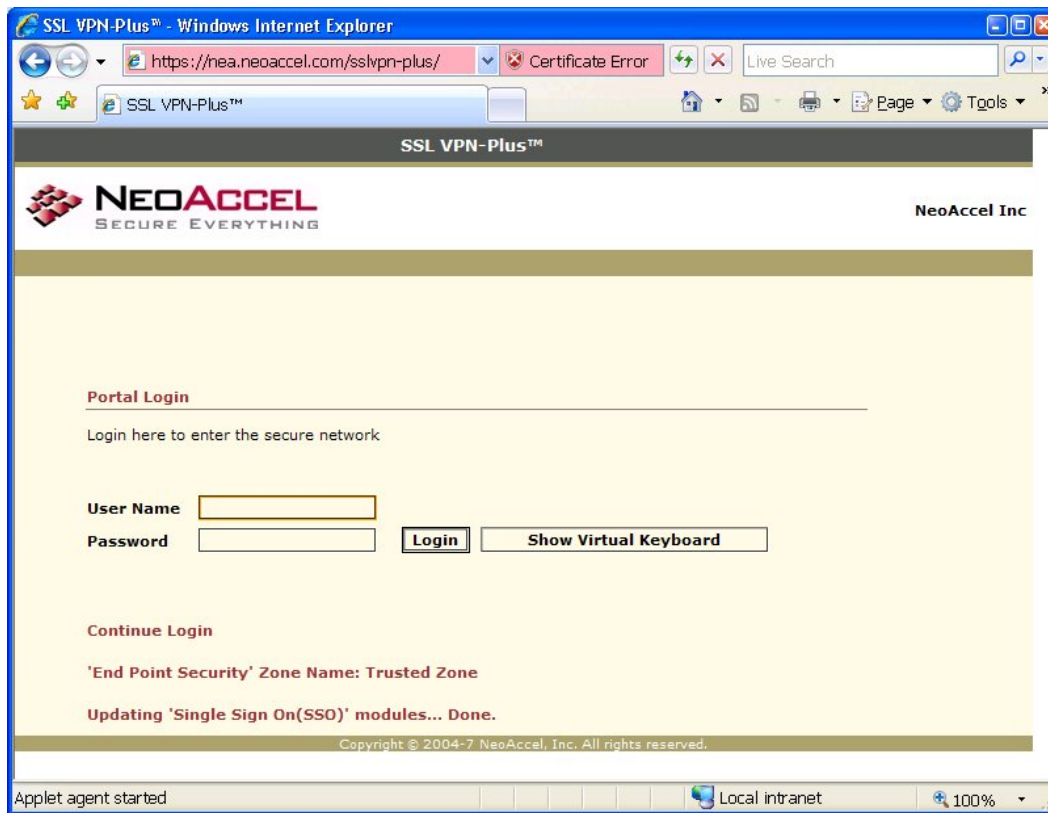
Access Management Console..contd

- Management Console login:
 - Default power-user credentials: admin/admin



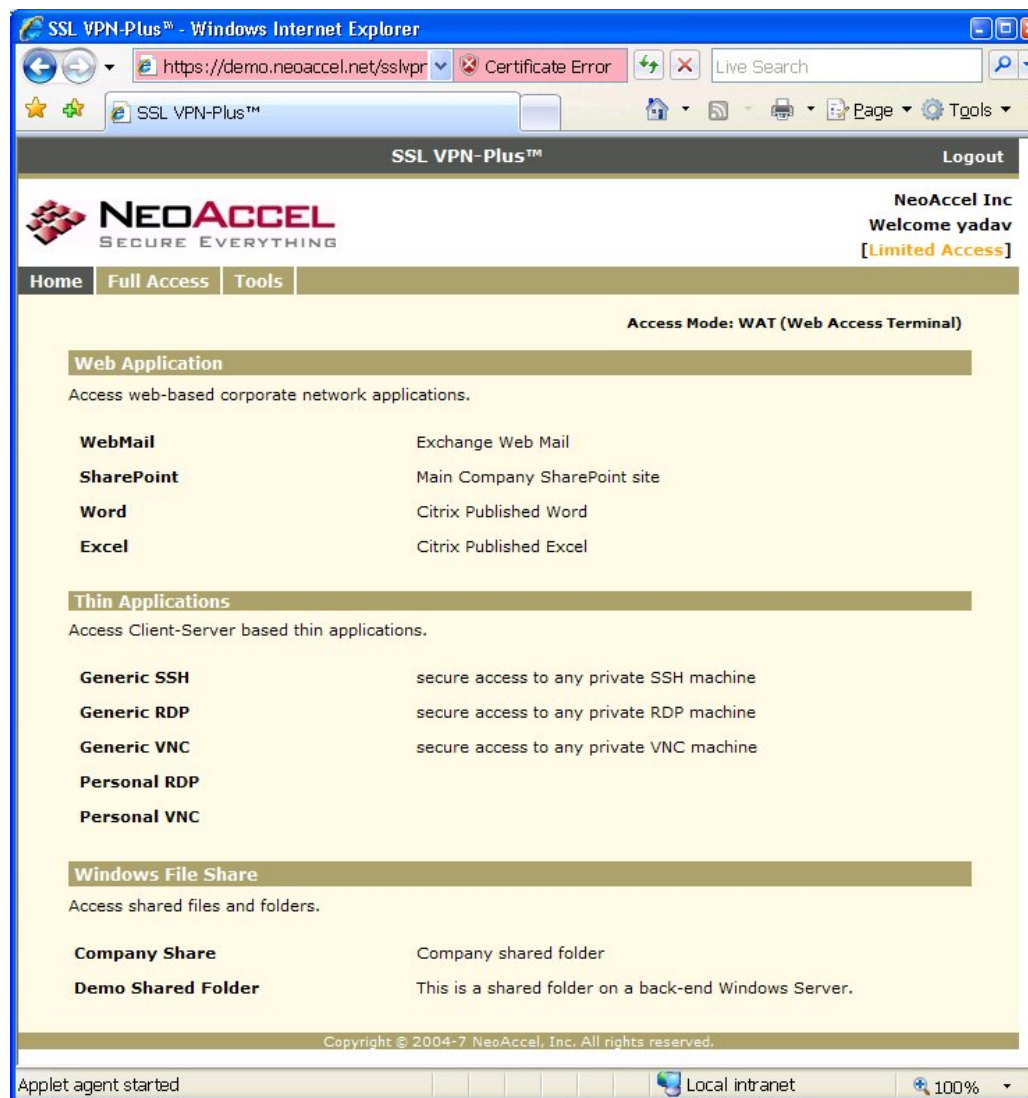
Access SSL VPN-Plus Portal

- Open URL: `https://<WAN side IP address of gateway machine>/sslvpn-plus/`
 - Example: `https://192.168.10.230/sslvpn-plus/`



Access SSL VPN-Plus Portal...contd

- User portal



Access User Portal...contd

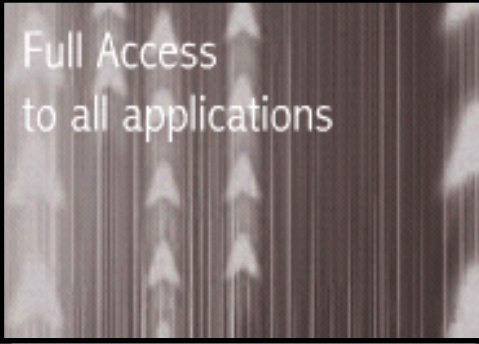
The screenshot shows a web browser window displaying the NeoAccel user portal. The browser title is "SSL VPN-Plus™" and the address bar shows "https://demo.neoaccel.net/sslvpnplus". The page header includes "SSL VPN-Plus™" and a "Logout" link. The NeoAccel logo is prominently displayed with the tagline "NEOACCEL SECURE EVERYTHING". The user is identified as "yadav" with "[Limited Access]". A navigation menu contains "Home", "Full Access", and "Tools". The main content area shows "Access Mode: WAT (Web Access Terminal)" and a "Web Application" section with links for "WebMail" (Exchange Web Mail) and "SharePoint" (Main Company SharePoint site). Three yellow callout boxes point to the "Home" link, the "Full Access" link, and the "Tools" link. A blue callout box points to the "Web Application" section.

Home Page

Full Access Clients (QAT and PHAT)

Tools section – Change Password

SSL VPN-Plus Portal Mode and available access



Configuration



Configuration Ideology

“Who” can access “What” and “How”

- For each group of users, define what all corporate network resources they can access and configure the method of access for users

Basic Steps

- Create resources
 - Define all your corporate application servers and network resources you want to make accessible to users
- Create ACLS
 - Define Access Control Policies to setup fine grain control
- Do Association
 - Associate the resources and ACLS to a group and the access modes
- Define your users or authentication method

Step 1: Create Resources

Why to create Resource?

To configure SSL VPN-Plus access terminals.

Each group sees different resources

Two type of resources

Portal Resources

- Web based application, services or resources user can access from SSL VPN-Plus web portal

• Network Extension Resources

- Client-Server based applications, services, resources user can access using QAT or PHAT.
- Security policy settings for user endpoint machines

Step 1: Create Resources...contd.

Portal Resources

This is the pool of resources that users will be able to view and access from web portal. You need to associate them to group to make them available for member users.

The screenshot shows the NeoAccel management console interface. On the left sidebar, the 'Portal' option is highlighted with an orange oval. The main content area displays a table titled 'Resource' with the following data:

Display Name	Resource Type	Details
Support Intranet	Web Application	http://support/
Exchange (OWA)	Web Application	http://exchangesrv/exchange/
Generic Telnet	Application	ANY/23
Generic SSH	Application	ANY/22
Generic VNC	Application	ANY/5900
Generic RDP	Application	ANY/3389
My fleshares	File Sharing	\\192.168.30.107
192.168.10.5	File Sharing	\\192.168.10.5
192.168.10.97	File Sharing	\\192.168.10.97\
192.168.10.32	File Sharing	\\192.168.10.32\
192.168.10.123	File Sharing	\\192.168.10.123

At the bottom of the table, there are three buttons: 'Add', 'Modify', and 'Remove'.

Web (http/URL) based applications

Shared files/folders/computers

Application Proxy agents/ Terminal emulators

Step 1: Create Resources...contd.

Network Extension Resources

The screenshot shows a web-based configuration interface for Network Extension. On the left is a navigation menu with items: System, SSL VPN-Plus, Users/Groups, Authorization, Network Extension (highlighted with an orange circle), Dynamic IP Address, Private Network, Client Configuration, and Installation Package. The main content area is titled 'Dynamic IP Address Configuration' and contains a table with the following data:

Name	IP Address Range	Netmask
1.0	192.168.1.63 - 192.168.1.64	255.255.255

These resources are used when users will be accessing client server application off the User portal. These resources are created for PHAT (full access) client and QAT (port forwarding) Client.

IP address pool for remote users using PHAT client. Required to assign IP address to remote users to enable full LAN like access.

Private networks that you want PHAT client and QAT client (your remote users) to tunnel traffic for. You can control access to specific host or subnet using ACLs. This is for the information of the SSL VPN-Plus Clients to know what traffic they need to tunnel in.

Create PHAT client installation package so that your remote users can install PHAT client and connect to SSL VPN-Plus gateway through it.

Endpoint security and SSL VPN-Plus client's configuration settings. Enable endpoint cache control and data control from this screen. These are application to WAT, PHAT and QAT

Step 2: Create ACLs

Access Control List

- Why ACLs?
 - Controlling access to each resource
 - Fine grained time based and source based control for each resources

Step 2: Create ACLs...contd.

Create ACLs

Create a pool of access control policies here for all of your available resources. Assign a set of these ACLs to each group in appropriate order to give required access.

Policy Name	Destination IP	Destination Port	Protocol	Action
allow-RDP-5	192.168.10.3 - 19...	3389 - 3389	TCP	ACCEPT
allow-citrix	192.168.10.110 / 32	ANY	TCP	DENY
deny-all	ANY	ANY	ANY	DENY
allow-exchange	192.168.10.174 / 32	110 - 110	TCP	ACCEPT
deny-ping	ANY	ANY	ICMP	DENY

Default access control policy is
ALLOW ALL

Step 3: Associate to group

Associate (Apply) to group

Assign a subset of portal resources, network extension resources and ACLs to facilitate members of this group to start accessing the corporate services.

- What does that mean
 - Associating “Resources” means users will be able to see the resources on portal or tunnel traffic for the network extension resources
 - Associating “ACLs” means, users will have access limited to what ACLs are assigned to the group, **irrespective of associated resources.**

Step 3: Associate to group...contd.

Group Definition screen

Create new group on this screen. Associate portal and network extension resources and ACLs.

Group Name	Group Policy	Group Users
default_group		demo
Dealers	deny-all,deny-ping,allow-citrix	kouji,anurag
Sales	deny-all,allow-citrix,allow-exchange	mike,peter
admin-group	deny-all,deny-ping,allow-RDP-5,allow-citrix,...	tommy,prasad

A default group "default_group" is always present.

Step 3: Associate to group...contd.

Associate ACLs

The screenshot shows the 'Group Access Policies' configuration window. The 'Group Name' field contains 'accounts'. The 'General' tab is selected. A table lists the following policies:

Policy Name	Priority
allow-RDP-5	5
allow-exchange	5
deny-all	6

An 'Add' button is circled in orange. A callout bubble points to it with the text 'Add a new group.' Another callout bubble points to the 'Add Policies' dialog box with the text 'Select ACLs to apply to this group. The selected set decides the net access available to members of this group.' The 'Add Policies' dialog box contains a list of available policies: allow-exchange, allow-citrix, allow-RDP-5, deny-ping, and deny-all.

Step 3: Associate to group...contd.

Associate Portal Resources

Configure portal for group members

Select the portal resources that you want your users to see on portal. Whether SSL VPN-Plus gateway will allow access to these resources is decided by ACLs assigned to this group.

The screenshot shows the 'Group Access Policies' configuration window for the 'accounts' group. The 'Portal' tab is selected, showing the 'Portal Customization' section. The 'Enable Public URL access' checkbox is checked. The 'Web Applications List' contains 'Support Intranet' (checked) and 'Exchange (OWA)' (unchecked). The 'Applications List' contains 'Generic Telnet' (unchecked), 'Generic SSH' (unchecked), 'Generic VNC' (checked), and 'Generic RDP' (checked). The 'File Sharing List' contains 'My fileshares' (checked), '192.168.10.5' (unchecked), '192.168.10.97' (unchecked), '192.168.10.32' (checked), and '192.168.10.123' (unchecked). The 'PHAT client installation package list' contains 'NeoAccel Remote Access' (checked).

Make sure that you associate appropriate access control policies for these resources. See previous slide (ACL Tab).

Step 3: Associate to group...contd.

Associate Network Extension Resources

Configure PHAT and QAT clients

Group Name: test

Access Control Policy | Portal Resources | **Network Extension** | Endpoint Security

Add Network Extension

Start Network Extension client on portal logon

Quick Access Terminal(QAT) client - only TCP Application

Private Hyper Access Transport(PHAT) client - Full Access

Show Quick Access Terminal client access URL

Client Configuration Name: --- Select ---

Tunnel Mode: Split Exclude local subnets

Default Gateway: . . .

Private Network List

ICAA	Name	Network	Priority
Enable	192.168.13.10	192.168.13.10/32	5

Dynamic IP Address Configuration List

Name	IP Address Range	Priority
13.10	192.168.13.11 - 192.168.13.12/24	5

Buttons: Add, Remove

Select this option to enable Hybrid SSL VPN-Plus portal; remote users will be able to access web and client-server applications without any extra step.

Specify network settings for PHAT (full access) client and QAT (port forwarding) clients. These settings will determine remote user traffic routing.

Dynamic IP pool is required only for PHAT client. Private networks are used by both PHAT and QAT client to route SSL VPN traffic.

Step 4: Define Authentication

Create or Define Authentication Methods

Tell SSL VPN-Plus gateway where your user database is present so that it can authenticate the remote user

- What all options are available
 - External authentication servers: RADIUS/AD/LDAP
 - Local Database: Local flat file database maintained by SSL VPN-Plus

Step 4: Define Authentication...contd

Local Database User

Create a user from management console and specify the group to which it belongs to

The screenshot displays the management console interface. On the left, a navigation pane shows 'System', 'SSL VPN-Plus', and 'Users/Groups'. Under 'Users/Groups', there are icons for 'Groups', 'Users', and 'Auth Servers'. The main area shows a 'List of Users' table with the following data:

User Name	User Group
miket	sales
msprasad	sales
peterv	Dealer-ITS
johnlal	
demo	

Overlaid on this is the 'SSL VPN-Plus User-Create' dialog box. It contains the following fields:

- Groups Available:** A dropdown menu with 'marketing' selected.
- User Name:** A text box containing 'vitor.norman'.
- Password:** A text box containing '*****'.
- Re-Type Password:** A text box containing '*****'.

At the bottom of the dialog box are 'OK' and 'Cancel' buttons.

Step 4: Define Authentication...contd

External Authentication Server

Add authentication servers if one already exists in your network



Server Alias	Server Type
employee-radius-server	RADIUS

Step 4: Define Authentication...contd

Sample Authentication Service Settings

Create Server

Basic Configuration

Server type: RADIUS

Server alias name: employee-radius-server

Server IP address: 10 . 1 . 3 . 12

Server port: 1812

Server timeout: 10 sec

Advanced Configuration

Server secret: *****

Retype server secret: *****

NAS IP address: 10 . 1 . 3 . 8

Retry count: 3

Enable Group Extraction

Group attribute name: Class

Create Server

Basic Configuration

Server type: AD

Server alias name: partner-ad-server

Server IP address: 10 . 1 . 3 . 14

Server port: 389

Server timeout: 10 sec

Advanced Configuration

Server search base: CN=Users,DC=corporate,DC=local

Server bind DN: CN=Administrator,CN=Users,DC=corpc

Server bind password: *****

Retype bind password: *****

Login attribute name: sAMAccountName

Search filter: objectClass=*

Enable Group Extraction

Group attribute name: memberOf

Sub attribute name: CN

Step 4: Define Authentication...contd

Associate Authentication method to server instance

Tell SSL VPN-Plus Gateway, which authentication method to use to authenticate incoming users

The screenshot displays the SSL VPN-Plus Gateway configuration interface. On the left is a navigation pane with options like System, SSL VPN-Plus, Gateways, Active Clients, License, Certificates, Administration, Users/Groups, Authorization, Network Extension, and Portal. The main area shows a 'List of Gateways' table with one entry: 'main' on port 443, uptime 0 day 1 hr 10 min, and 0 clients connected. Below this table are 'Add', 'Modify', and 'Remove' buttons. A large yellow arrow points from the 'Modify' button to the 'Modify Gateway' dialog box. The dialog box has three tabs: 'General', 'Authentication', and 'Advanced'. The 'Authentication' tab is active, showing 'Authentication Parameters' with 'Enable Authentication' checked and 'Prevent multiple logons using same username' unchecked. Below this is a table for 'Authentication Servers' with one entry: 'locsrvr' with priority 0. 'Add' and 'Remove' buttons are next to this table. Another yellow arrow points from the 'Add' button to the 'Add Servers' dialog box. The 'Add Servers' dialog box has a title bar with a close button and the text 'Please select auth servers from the list below.' It contains an 'Add' button and a list box labeled 'Available Servers' with two entries: 'locsrvr' and 'employee-radius-server'. 'Add' and 'Cancel' buttons are at the bottom.

Name	Port	Uptime	Clients Connected
main	443	0 day 1 hr 10 min	0

Authentication Server	Priority
locsrvr	0

Available Servers:

- locsrvr
- employee-radius-server

That's All!

That's All

- Open SSL VPN-Plus portal from URL <https://gateway/sslvpn-plus/>
- Authenticate using the credentials of local database user or your external auth server
- Access available resources portal
- If you need full network access, Install PHAT client and log in using that.