How To – Configure SSL VPN in Cyberoam

Applicable Version: 10.00 onwards

Overview

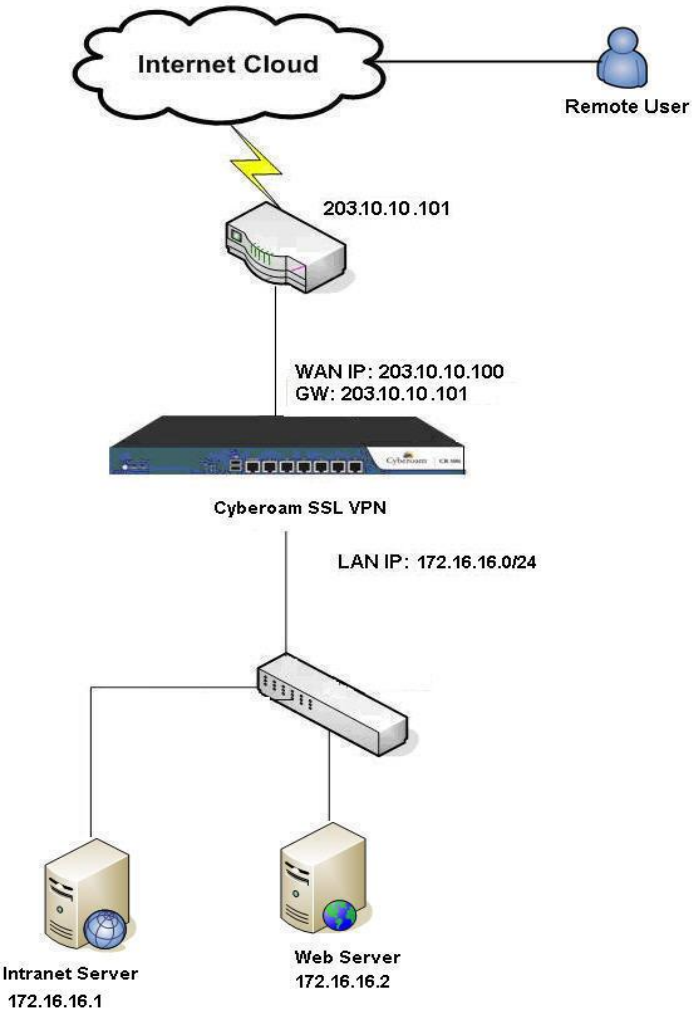
SSL (Secure Socket Layer) VPN provides simple-to-use, secure access for remote users to the corporate network from anywhere, anytime. It enables creation of point-to-point encrypted tunnels between remote user and company's internal network, requiring combination of SSL certificates and a username/password for authentication.

Cyberoam allows remote users access to the corporate network in 3 Modes:

- **Tunnel Access Mode**: User gains access through a remote SSL VPN Client.
- **Web Access Mode**: Remote users can access SSL VPN using a web browser only, i.e., clientless access.
- **Application Access Mode**: users can access web applications as well as certain enterprise applications through a web browser, i.e., clientless access.

Scenario

Configure SSL VPN in Cyberoam such that the remote user shown in the diagram below is able to access the Web and Intranet Servers in the company's internal network. The user is to have Full Access, i.e., Tunnel, Web and Application Access. The network particulars given below are used as an example throughout this article.



Network Parameters

Configuration Parameter	Value
Cyberoam WAN IP	203.10.10.100
LAN Network	172.16.16.0/24
Intranet Server IP	172.16.16.1
Web Server IP	172.16.16.2
IP Range Leased to user after successful connection through SSL VPN	10.10.10.1 to 10.10.10.254

Configuration

Configure SSL VPN in Cyberoam by following the steps given below. All configurations are to be done from Web Admin Console using 'Administrator' profile.

Step 1: Generate Default Certificate Authority

To generate the default Certificate Authority, go to **System→ Certificate → Certificate Authority** and click **Default** CA.

Update the Default CA as shown below.

Click **OK** to generate Default Certificate Authority.

Note:

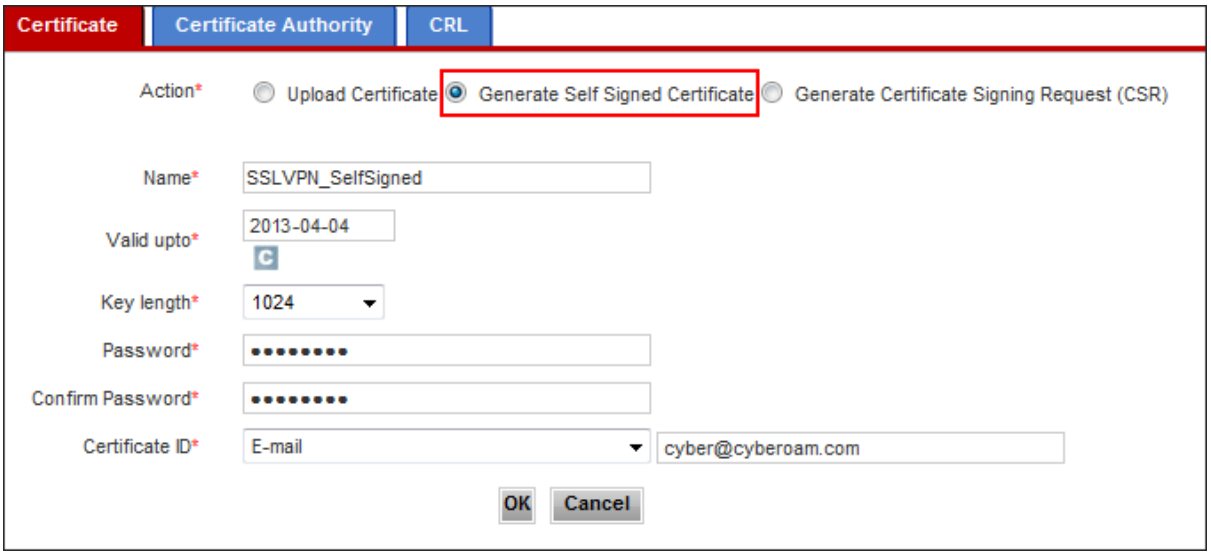
If the customer is using an external certificate authority, then upload the same from **System → Certificate → Certificate Authority**.

Step 2: Create self-signed Certificate

To create a self-signed Certificate, go to **System** → **Certificate** → **Certificate** and click **Add**. Generate a Self Signed Certificate using the parameters given below.

Parameter Description

Parameter	Value	Description
Action	**Generate Self Signed Certificate**	Specify action for certificate generation
Certificate Name	**SSLVPN_SelfSigned**	Name to identify the Certificate.
Valid upto	**April 04, 2013**	Specify certificate validity period using Calendar
Key length	**1024**	Select key length, i.e., number of bits used to construct the key.
Password	**cyberoamabc**	Password for a Certificate used for authentication
Certificate ID	**E-mail: cyber@cyberoam.com**	Specify Certificate ID.

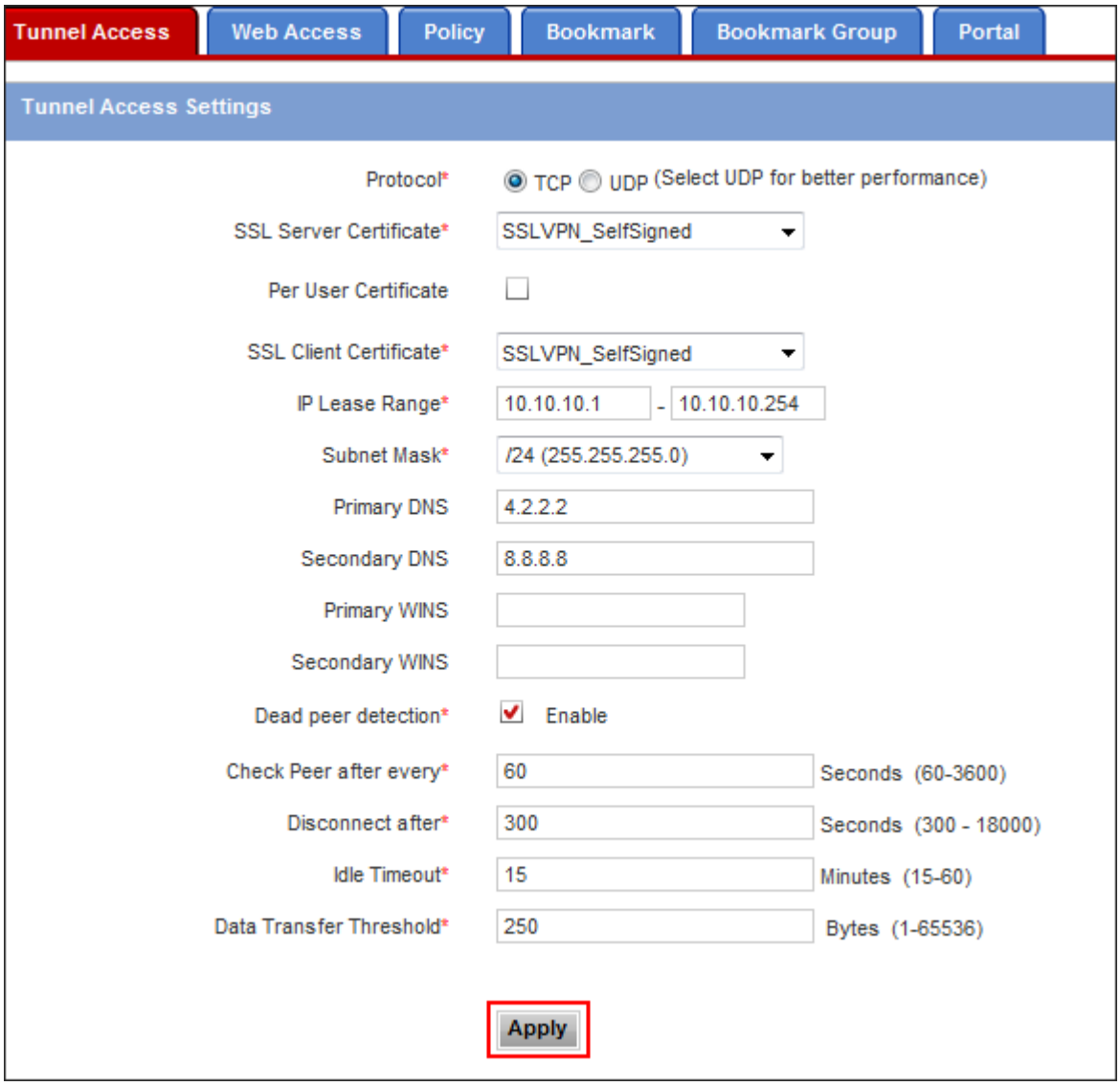


Click **OK** to create the certificate.

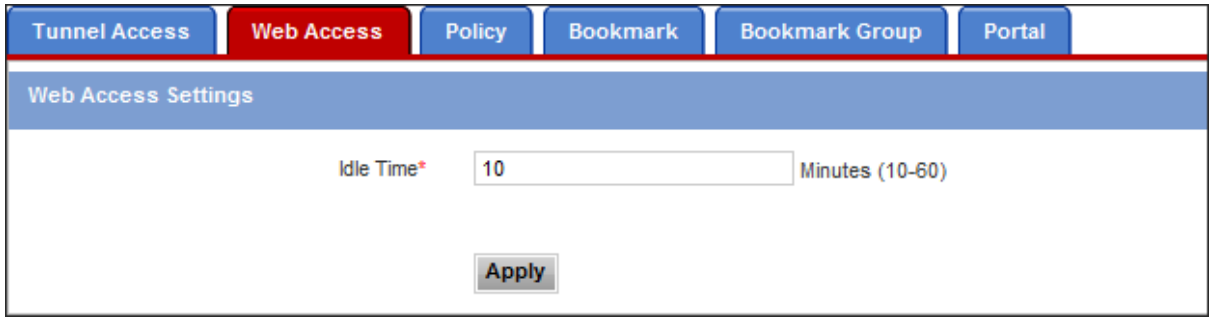
Step 3: Configure SSL Global Parameters

To set global parameters for tunnel access, go to **VPN → SSL → Tunnel Access** and configure tunnel access settings with following values:

Parameter	Value	Description
Protocol	**TCP**	Select default protocol for all the SSL VPN clients.
SSL Server Certificate	**SSLVPN_SelfSigned**	Select SSL Server certificate from the dropdown list to be used for authentication
Per User Certificate	**Disabled**	SSL server uses certificate to authenticate the remote client. One can use the common certificate for all the users or create individual certificate for each user
SSL Client Certificate	**SSLVPN_SelfSigned**	Select the SSL Client certificate from the dropdown list if you want to use common certificate for authentication
IP Lease Range	**10.10.10.1 to 10.10.10.254**	Specify the range of IP addresses reserved for the SSL Clients
Subnet Mask	**255.255.255.0**	Specify Subnet mask
Primary DNS	**4.2.2.2**	Specify IP address of Primary DNS
Secondary DNS	**8.8.8.8**	Specify IP address of Secondary DNS
Enable DPD	**Enabled**	Click to enable Dead Peer Detection.
Check Peer after every	**60**	Specify time interval in the range of 60 to 3600 seconds after which the peer should be checked for its status.
Disconnect after	**300**	Specify time interval in the range of 300 to 1800 seconds after which the connection should be disconnected if peer is not live.
Idle Time Out	**15**	Specify idle timeout. Connection will be dropped after the configured inactivity time and user will be forced to re-login.
Data Transfer Threshold	**250**	Once the idle timeout is reached, before dropping the connection, appliance will check the data transfer. If data transfer is more than the configured threshold, connection will be dropped.



To set global Idle Time for Web Access Mode, go to **VPN → SSL → Web Access** and set Idle Time as shown below.

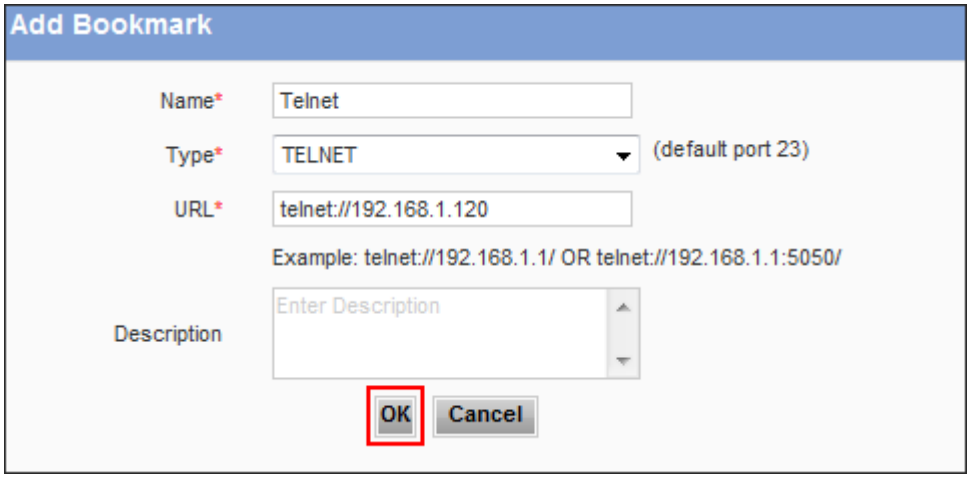


Step 4: Create Bookmarks

Bookmarks are the resources whose access is available through SSL VPN Web portal. You can also create a group of bookmarks that can be configured in SSL VPN Policy. These resources are available in Web and Application Access mode only.

To create Bookmark, go to **VPN → SSL → Bookmark** and click **Add**. Create Bookmark using following parameters.

Parameter	Value	Description
Name	**Telnet**	Name to identify Bookmark.
Type	**TELNET**	Specify type of bookmark.
URL	**telnet://192.168.1.120**	Specify URL at which telnet sessions are allowed to remote users.



Click **OK** to create Bookmark.

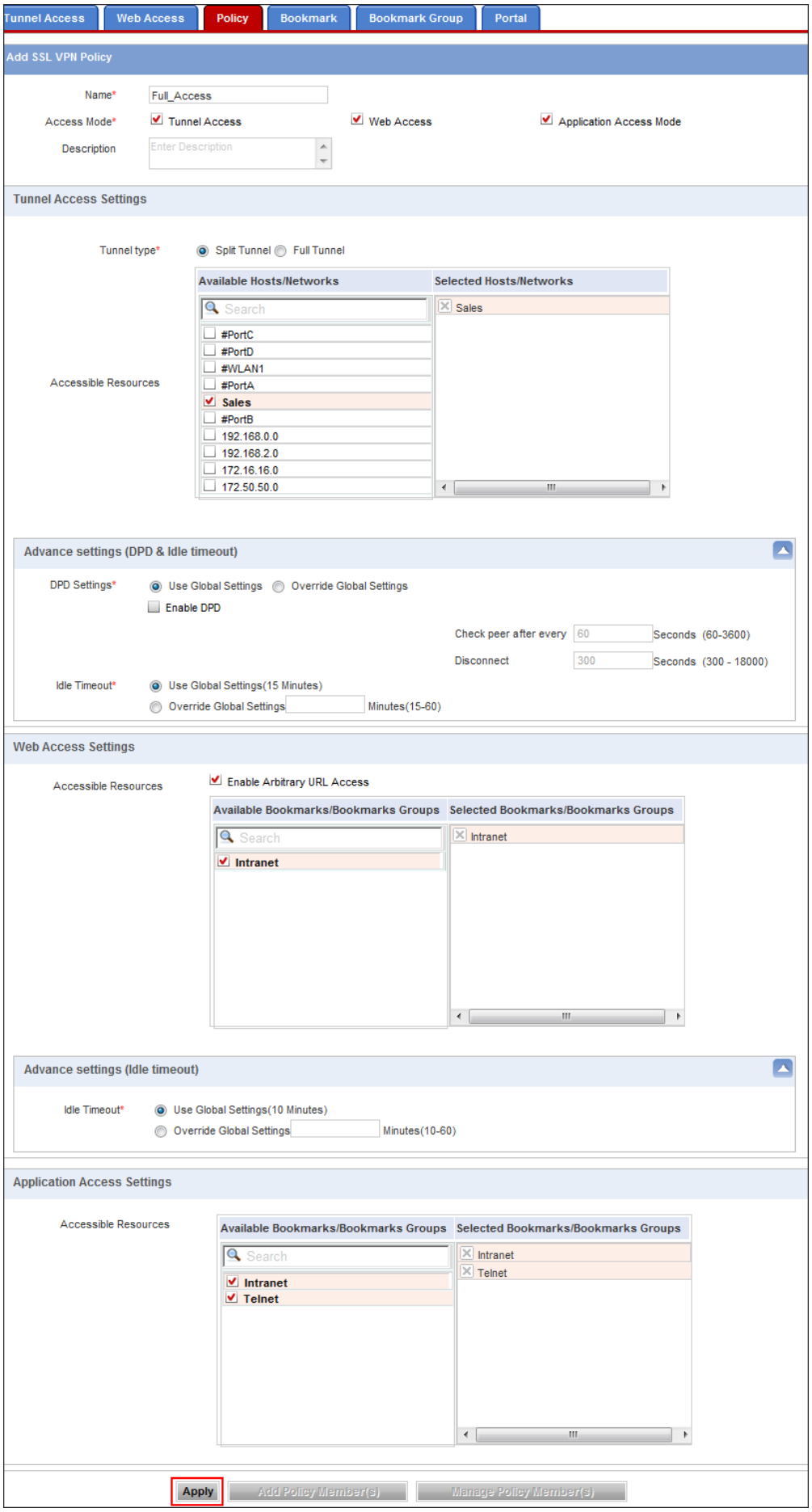
Similarly, create a bookmark **Intranet** of type HTTP to allow access to the internal Intranet server. Intranet is accessible in Web as well as Application Access Mode, while Telnet is accessible in Application Access Mode.

Step 5: Configure SSL VPN Policy

To configure SSL VPN policy, go to **VPN → SSL → Policy** and click **Add**. Create policy using parameters given below.

Parameter Description

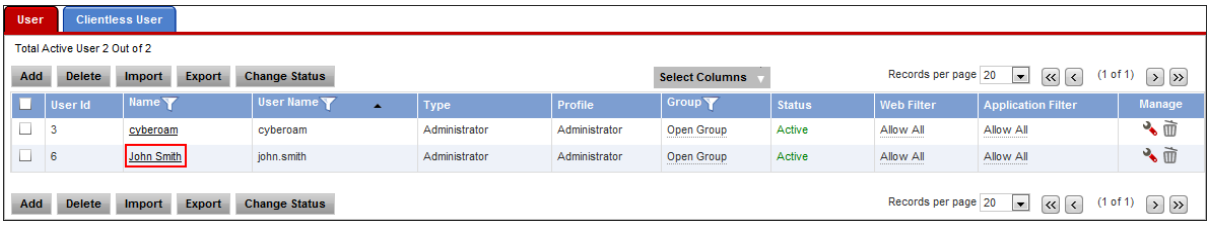
Parameter	Value	Description
Add SSL VPN Policy		
Name	**Full_Access**	Name to identify the SSL VPN policy
Access Mode	**Tunnel Access Mode** **Web Access Mode** **Application Access Mode**	Select the access mode by clicking the appropriate option.
Tunnel Access Settings		
Tunnel Type	**Split Tunnel**	Select tunnel type. Tunnel type determines how the remote user's traffic will be routed.
Accessible Resources	**Sales**	Select Hosts or Networks that remote user can access.
DPD Settings	**Use Global Settings**	You can customize and override the global Dead Peer Detection setting.
Idle Time out	**Use Global Settings**	You can use the global settings or customize the idle timeout.
Web Access Settings		
Enable Arbitary URL Access	**Enabled**	Enable to access custom URLs not defined as Bookmarks.
Accessible Resources	**Intranet**	Select Bookmarks/Bookmarks Group that remote user can access.
Idle Time out	**Use Global Settings**	You can use the global settings or customize the idle timeout.
Application Access Settings		
Accessible Resources	**Intranet** **Telnet**	Select Bookmarks/Bookmarks Group that remote user can access.


Tunnel Access
Web Access
Policy
Bookmark
Bookmark Group
Portal
Add SSL VPN Policy
Name*
Full_Access
Access Mode*
Tunnel Access
Web Access
Application Access Mode
Description
Enter Description
Tunnel Access Settings
Tunnel type*
Split Tunnel
Full Tunnel
Accessible Resources
Available Hosts/Networks
Selected Hosts/Networks
Search
Sales
#PortC
#PortD
#WLAN1
#PortA
Sales
#PortB
192.168.0.0
192.168.2.0
172.16.16.0
172.50.50.0
Advance settings (DPD & Idle timeout)
DPD Settings*
Use Global Settings
Override Global Settings
Enable DPD
Check peer after every
60
Seconds (60-3600)
Disconnect
300
Seconds (300 - 18000)
Idle Timeout*
Use Global Settings(15 Minutes)
Override Global Settings
Minutes(15-60)
Web Access Settings
Accessible Resources
Enable Arbitrary URL Access
Available Bookmarks/Bookmarks Groups
Selected Bookmarks/Bookmarks Groups
Search
Intranet
Intranet
Advance settings (Idle timeout)
Idle Timeout*
Use Global Settings(10 Minutes)
Override Global Settings
Minutes(10-60)
Application Access Settings
Accessible Resources
Available Bookmarks/Bookmarks Groups
Selected Bookmarks/Bookmarks Groups
Search
Intranet
Telnet
Intranet
Telnet
Apply
Add Policy Member(s)
Manage Policy Member(s)

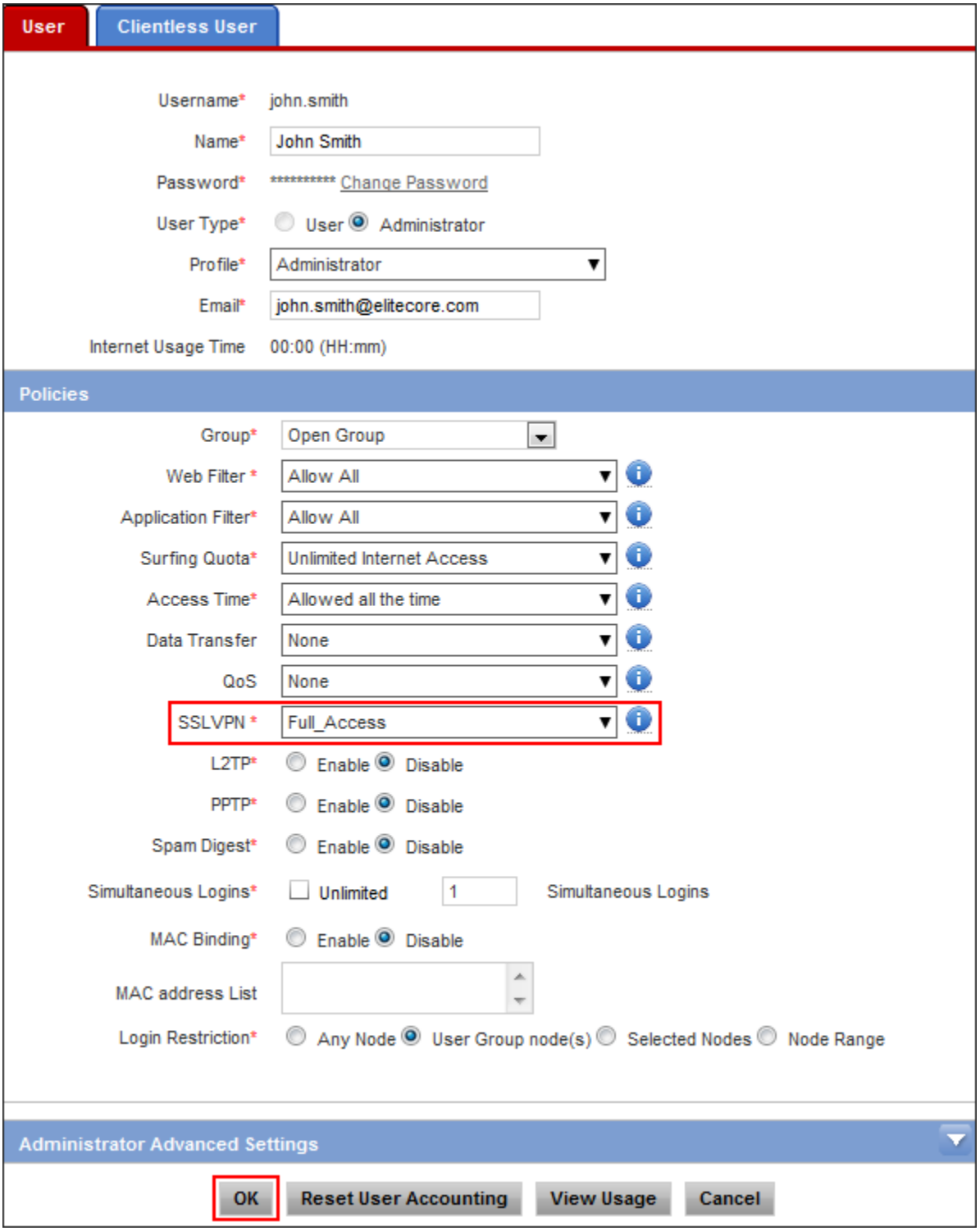
Step 6: Apply SSL VPN Policy on User

To apply SSL VPN policy on user, follow the steps given below.

Go to **Identity → Users → User** and select the user to which policy is to be applied. Here we have applied it on user John Smith.



Under Policies section, select Full_Access for SSL VPN as shown below.



Click **OK** to update the user's SSL VPN Policy.

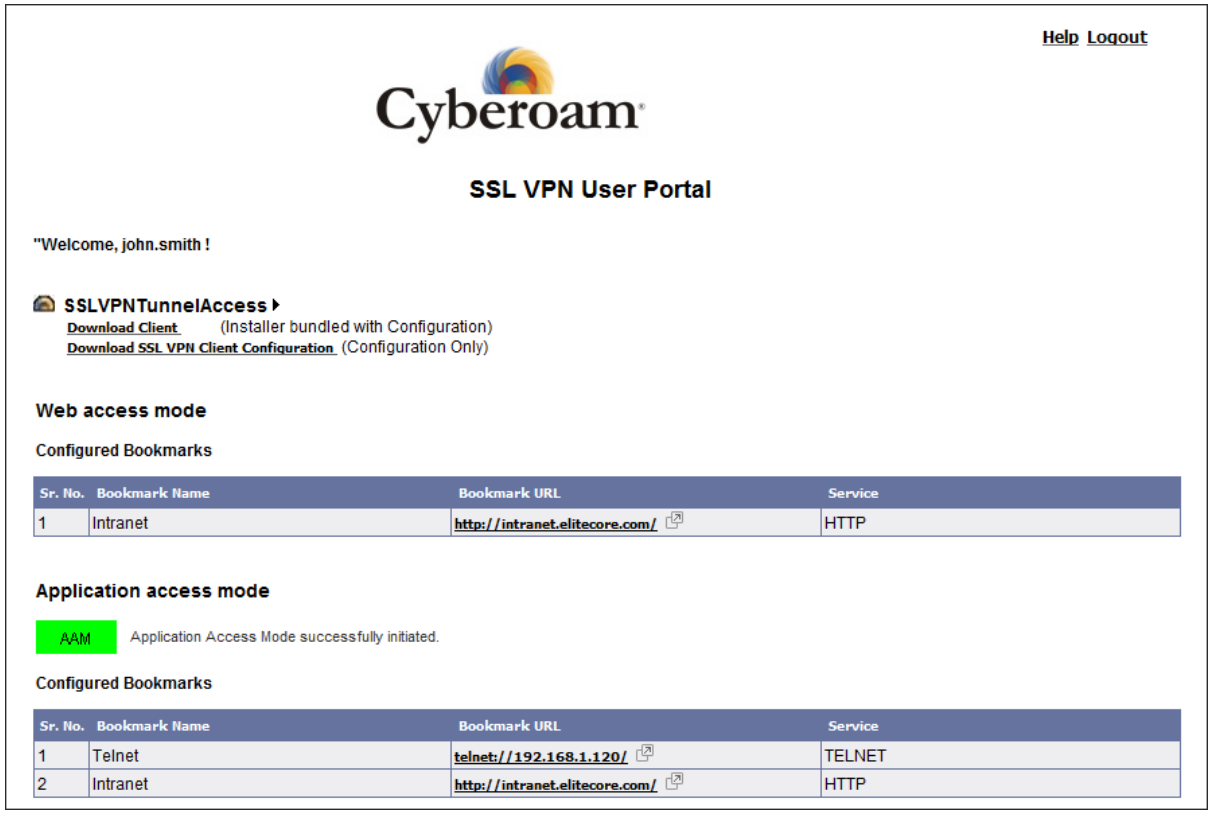
Step 7: Download and Install SSL VPN Client at Remote End

Remote users can login to Cyberoam SSL VPN Portal by browsing to https://<WAN IP address of Cyberoam:port> and logging in.

Note:

Use default port: 8443 unless customized. Access is available only to those users who have been assigned an SSL VPN policy.

User is directed to the Main Page which displays Tunnel, Web or Application Access Mode section according to policy applied on user.



For Tunnel Access, user needs to access internal resources through an SSL VPN Client.

- Download the SSL VPN client by clicking "**Download Client**" and follow the on-screen instructions.
- Install the client on the remote user's system.
- On complete installation, the CrSSL Client icon appears in the system tray. Login to the Client and access the company's internal network through SSL VPN.

For Web and Application Access, user can access internal resources using web browser, i.e., clientless access. In this, user needs to browse to https://<WAN IP address of Cyberoam:port> and login.