



## How To – Configure SSL VPN in Cyberoam

**Applicable Version: 10.00 onwards**

### Overview

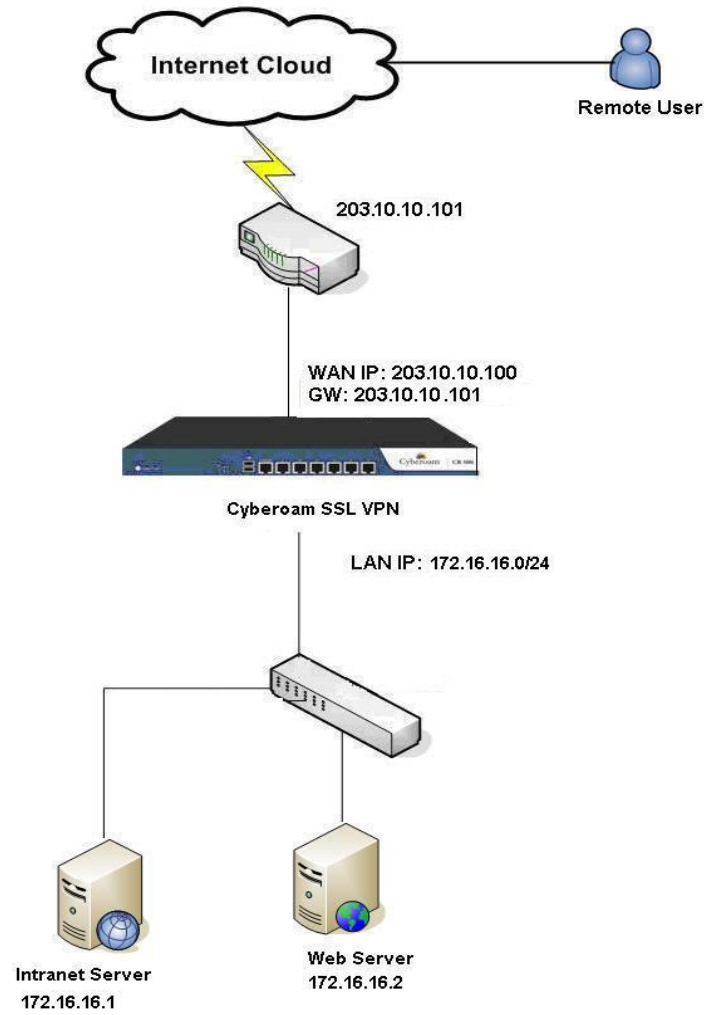
SSL (Secure Socket Layer) VPN provides simple-to-use, secure access for remote users to the corporate network from anywhere, anytime. It enables creation of point-to-point encrypted tunnels between remote user and company's internal network, requiring combination of SSL certificates and a username/password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

The screenshot shows the 'Certificate Authority' configuration form. The form has three tabs: 'Certificate', 'Certificate Authority' (selected), and 'CRL'. The form fields are as follows:

Field	Value	Notes
Name*	Default	
Country Name *	United States	Dropdown menu
State*	Texas	
Locality Name*	Houston	(eg. city name)
Organization Name*	EliteCore Technologies	(eg. company name)
Organization Unit Name*	Production	(eg. department name)
Common Name*	elitecore	(eg. server's hostname)
Email Address*	cyber@cyberoam.com	
CA Password	*****	<a href="#">Change Password</a>

Buttons at the bottom: OK, Download, Cancel.

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

Certificate

Certificate Authority

CRL

Action\*  Upload Certificate  Generate Self Signed Certificate  Generate Certificate Signing Request (CSR)

Name\*

Valid upto\*  C

Key length\*  ▼

Password\*

Confirm Password\*

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	<b>TCP</b>	Select default protocol for all the SSL VPN clients.
SSL Server Certificate	<b>SSLVPN_SelfSigned</b>	Select SSL Server certificate from the dropdown list to be used for authentication
Per User Certificate	<b>Disabled</b>	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	<b>SSLVPN_SelfSigned</b>	Select the SSL Client certificate from the dropdown list if you want to use common certificate for authentication
IP Lease Range	<b>10.10.10.1 to 10.10.10.254</b>	Specify the range of IP addresses reserved for the SSL Clients
Subnet Mask	<b>255.255.255.0</b>	Specify Subnet mask
Primary DNS	<b>4.2.2.2</b>	Specify IP address of Primary DNS
Secondary DNS	<b>8.8.8.8</b>	Specify IP address of Secondary DNS
Enable DPD	<b>Enabled</b>	Click to enable Dead Peer Detection.
Check Peer after every	<b>60</b>	Specify time interval in the range of 60 to 3600 seconds after which the peer should be checked for its status.
Disconnect after	<b>300</b>	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	<b>15</b>	Specify idle timeout. Connection will be dropped after the configured inactivity time and user will be forced to re-login.
Data Transfer Threshold	<b>250</b>	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.

**Tunnel Access** | Web Access | Policy | Bookmark | Bookmark Group | Portal

### Tunnel Access Settings

Protocol\*  TCP  UDP (Select UDP for better performance)

SSL Server Certificate\* SSLVPN\_SelfSigned

Per User Certificate

SSL Client Certificate\* SSLVPN\_SelfSigned

IP Lease Range\* 10.10.10.1 - 10.10.10.254

Subnet Mask\* /24 (255.255.255.0)

Primary DNS 4.2.2.2

Secondary DNS 8.8.8.8

Primary WINS

Secondary WINS

Dead peer detection\*  Enable

Check Peer after every\* 60 Seconds (60-3600)

Disconnect after\* 300 Seconds (300 - 18000)

Idle Timeout\* 15 Minutes (15-60)

Data Transfer Threshold\* 250 Bytes (1-65536)

**Apply**

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

**Tunnel Access** | **Web Access** | Policy | Bookmark | Bookmark Group | Portal

### Web Access Settings

Idle Time\* 10 Minutes (10-60)

**Apply**

#### 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	<b>Telnet</b>	Name to identify Bookmark.
Type	<b>TELNET</b>	Specify type of bookmark.
URL	<b>telnet://192.168.1.120</b>	Specify URL at which telnet sessions are allowed to remote users.

**Add Bookmark**

Name\*

Type\*  (default port 23)

URL\*

Example: telnet://192.168.1.1/ OR telnet://192.168.1.1:5050/

Description

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



Tunnel Access | Web Access | **Policy** | Bookmark | Bookmark Group | Portal

---

Add SSL VPN Policy

Name\*

Access Mode\*  Tunnel Access  Web Access  Application Access Mode

Description

---

Tunnel Access Settings

Tunnel type\*  Split Tunnel  Full Tunnel

Accessible Resources

Available Hosts/Networks	Selected Hosts/Networks
<input type="text" value="Search"/> <ul style="list-style-type: none"> <li><input type="checkbox"/> #PortC</li> <li><input type="checkbox"/> #PortD</li> <li><input type="checkbox"/> #WLAN1</li> <li><input type="checkbox"/> #PortA</li> <li><input checked="" type="checkbox"/> Sales</li> <li><input type="checkbox"/> #PortB</li> <li><input type="checkbox"/> 192.168.0.0</li> <li><input type="checkbox"/> 192.168.2.0</li> <li><input type="checkbox"/> 172.16.16.0</li> <li><input type="checkbox"/> 172.50.50.0</li> </ul>	<input checked="" type="checkbox"/> Sales

---

Advance settings (DPD & Idle timeout)

DPD Settings\*  Use Global Settings  Override Global Settings

Enable DPD

Check peer after every  Seconds (60-3600)

Disconnect  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
<input type="text" value="Search"/> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Intranet</li> </ul>	<input checked="" type="checkbox"/> 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
<input type="text" value="Search"/> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Intranet</li> <li><input checked="" type="checkbox"/> Telnet</li> </ul>	<input checked="" type="checkbox"/> Intranet <input checked="" type="checkbox"/> Telnet

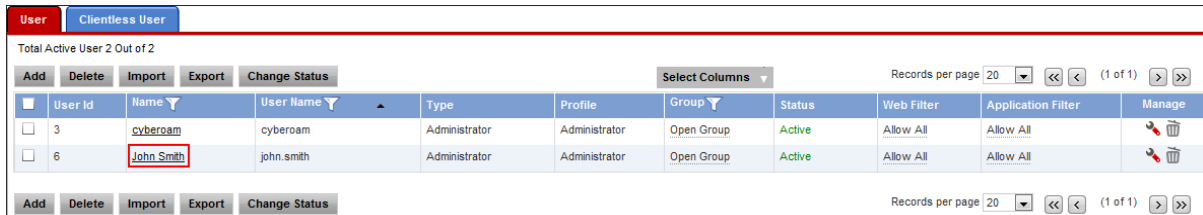
---

**Apply**





## 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.



The screenshot shows the 'User' management interface in Cyberoam. At the top, there are tabs for 'User' and 'Clientless User'. Below the tabs, it indicates 'Total Active User 2 Out of 2'. There are action buttons: 'Add', 'Delete', 'Import', 'Export', and 'Change Status'. A 'Select Columns' dropdown is also present. The table below lists two users:

User Id	Name	User Name	Type	Profile	Group	Status	Web Filter	Application Filter	Manage
3	cyberoam	cyberoam	Administrator	Administrator	Open Group	Active	Allow All	Allow All	 
6	John Smith	john.smith	Administrator	Administrator	Open Group	Active	Allow All	Allow All	 

At the bottom, there are more action buttons: 'Add', 'Delete', 'Import', 'Export', and 'Change Status'. The 'Records per page' is set to 20, and it shows '(1 of 1)' records.

Under Policies section, select Full\_Access for SSL VPN as shown below.

**User** | Clientless User

Username\* john.smith  
Name\* John Smith  
Password\* \*\*\*\*\* [Change Password](#)  
User Type\*  User  Administrator  
Profile\* Administrator  
Email\* john.smith@elitecore.com  
Internet Usage Time 00:00 (HH:mm)

**Policies**

Group\* Open Group  
Web Filter\* Allow All  
Application Filter\* Allow All  
Surfing Quota\* Unlimited Internet Access  
Access Time\* Allowed all the time  
Data Transfer None  
QoS None  
**SSLVPN\* Full\_Access**  
L2TP\*  Enable  Disable  
PPTP\*  Enable  Disable  
Spam Digest\*  Enable  Disable  
Simultaneous Logins\*  Unlimited  Simultaneous Logins  
MAC Binding\*  Enable  Disable  
MAC address List  
Login Restriction\*  Any Node  User Group node(s)  Selected Nodes  Node Range

**Administrator Advanced Settings**

**OK** Reset User Accounting View Usage Cancel

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.



The screenshot displays the Cyberoam SSL VPN Portal login interface. At the top, the Cyberoam logo is centered. Below it, the text "Welcome to the Cyberoam SSL VPN Portal!" is displayed. A blue error message box with the text "Invalid username or password" is overlaid on the login form. The form contains two input fields: "Username:" with the value "John.Smith" and "Password:" with the value "\*\*\*\*\*". A "Login" button is positioned below the password field.

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

[Help](#) [Logout](#)




## SSL VPN User Portal

"Welcome, john.smith !

**SSLVPNTunnelAccess ▶**  
[Download Client](#) (Installer bundled with Configuration)  
[Download SSL VPN Client Configuration](#) (Configuration Only)

**Web access mode**



Configured Bookmarks

Sr. No.	Bookmark Name	Bookmark URL	Service
1	Intranet	<a href="http://intranet.elitecore.com/">http://intranet.elitecore.com/</a> 	HTTP


**Application access mode**

AAM Application Access Mode successfully initiated.

Configured Bookmarks

Sr. No.	Bookmark Name	Bookmark URL	Service
1	Telnet	<a href="telnet://192.168.1.120/">telnet://192.168.1.120/</a> 	TELNET
2	Intranet	<a href="http://intranet.elitecore.com/">http://intranet.elitecore.com/</a> 	HTTP

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.