Cyberoam
Unified Threat Management

SSL VPN Management Guide

Version 10

Document version 10.00.0302 -1.0-09/08/2010

IMPORTANT NOTICE

Elitecore has supplied this Information believing it to be accurate and reliable at the time of printing, but is presented without warranty of any kind, expressed or implied. Users must take full responsibility for their application of any products. Elitecore assumes no responsibility for any errors that may appear in this document. Elitecore reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

USER'S LICENSE

The Appliance described in this document is furnished under the terms of Elitecore's End User license agreement. Please read these terms and conditions carefully before using the Appliance. By using this Appliance, you agree to be bound by the terms and conditions of this license. If you do not agree with the terms of this license, promptly return the unused Appliance and manual (with proof of payment) to the place of purchase for a full refund.

LIMITED WARRANTY

Software: Elitecore warrants for a period of ninety (90) days from the date of shipment from Elitecore: (1) the media on which the Software is furnished will be free of defects in materials and workmanship under normal use; and (2) the Software substantially conforms to its published specifications except for the foregoing, the software is provided AS IS. This limited warranty extends only to the customer as the original licenses. Customers exclusive remedy and the entire liability of Elitecore and its suppliers under this warranty will be, at Elitecore or its service center's option, repair, replacement, or refund of the software if reported (or, upon, request, returned) to the party supplying the software to the customer. In no event does Elitecore warrant that the Software is error free, or that the customer will be able to operate the software without problems or interruptions. Elitecore hereby declares that the anti virus and anti spam modules are powered by Kaspersky Labs and Commtouch respectively and the performance thereof is under warranty provided by Kaspersky Labs and by Commtouch. It is specified that Kaspersky Lab does not warrant that the Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

Hardware: Elitecore warrants that the Hardware portion of the Elitecore Products excluding power supplies, fans and electrical components will be free from material defects in workmanship and materials for a period of One (1) year. Elitecore's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. The replacement Hardware need not be new or of an identical make, model or part; Elitecore may, in its discretion, replace the defective Hardware (or any part thereof) with any reconditioned product that Elitecore reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware.

DISCLAIMER OF WARRANTY

Except as specified in this warranty, all expressed or implied conditions, representations, and warranties including, without limitation, any implied warranty or merchantability, fitness for a particular purpose, non-infringement or arising from a course of dealing, usage, or trade practice, and hereby excluded to the extent allowed by applicable law.

In no event will Elitecore or its supplier be liable for any lost revenue, profit, or data, or for special, indirect, consequential, incidental, or punitive damages however caused and regardless of the theory of liability arising out of the use of or inability to use the product even if Elitecore or its suppliers have been advised of the possibility of such damages. In the event shall Elitecore's or its supplier's liability to the customer, whether in contract, tort (including negligence) or otherwise, exceed the price paid by the customer. The foregoing limitations shall apply even if the above stated warranty fails of its essential purpose.

In no event shall Elitecore or its supplier be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Elitecore or its suppliers have been advised of the possibility of such damages.

RESTRICTED RIGHTS

CORPORATE HEADQUARTERS

Elitecore Technologies Ltd.
904 Silicon Tower,
Off. C.G. Road,
Ahmedabad – 380015, INDIA
Phone: +91-79-66065606
Fax: +91-79-26407640
Web site: www.elitecore.com , www.cyberoam.com

Contents

Technical Support

You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to Customer care/service department at the following address:

Corporate Office
eLitecore Technologies Ltd.
904, Silicon Tower
Off C.G. Road
Ahmedabad 380015
Gujarat, India.
Phone: +91-79-66065606
Fax: +91-79-26462200
Web site: www.elitecore.com

Cyberoam contact:
Technical support (Corporate Office): +91-79-26400707
Email: support@cyberoam.com
Web site: www.elitecore.com

Visit www.cyberoam.com for the regional and latest contact information.

Typographic Conventions

Material in this manual is presented in text, screen displays, or command-line notation.

Item	Convention	Example
Server		Machine where Cyberoam Software - Server component is installed
Client		Machine where Cyberoam Software - Client component is installed
User		The end user
Username		Username uniquely identifies the user of the system
Part titles	Bold and shaded font typefaces	Report
Topic titles	Shaded font typefaces	Introduction
Subtitles	Bold & Black typefaces	Notation conventions
Navigation link	Bold typeface	**Group Management → Groups → Create** it means, to open the required page click on Group management then on Groups and finally click Create tab
Name of a particular parameter / field / command button text	Lowercase italic type	Enter policy name, replace policy name with the specific name of a policy Or Click Name to select where Name denotes command button text which is to be clicked
Cross references	Hyperlink in different color	refer to Customizing User database Clicking on the link will open the particular topic
Notes & points to remember	Bold typeface between the black borders	**Note**
Prerequisites	Bold typefaces between the black borders	Prerequisite • Prerequisite details

Introduction to SSL VPN

A Virtual Private Network (VPN) is a tunnel that carries private network traffic from one endpoint system to another over a public network such as the Internet without the traffic being aware that there are intermediate hops between the endpoints or the intermediate hops being aware they are carrying the network packets that are traversing the tunnel. The tunnel may optionally compress and/or encrypt the data, providing enhanced performance and some measure of security.

Note

SSL VPN configuration is not available for Cyberoam CR15i models.

VPN is cost-effective because users can connect to the Internet locally and tunnel back to connect to corporate resources. This not only reduces overhead costs associated with traditional remote access methods, but also improves flexibility and scalability.

For business telecommuters or employees working from home, connecting securely to the corporate intranets or extranets to access files or application is essential.

Hence, whenever users access the organization resources from remote locations, it is essential that not only the common requirements of secure connectivity be met but also the special demands of remote clients. These requirements include:

- Connectivity: The remote users must be able to access the organization from various locations, like Internet cafes, hotels, airport etc. The range of applications available must include web applications, mail, file shares, and other more specialized applications required to meet corporate needs.
- Secure connectivity: Guaranteed by the combination of authentication, confidentiality and data integrity for every connection.
- Usability: Installation must be easy. No configuration should be required as a result of network modification at the remote user end. The given solution should be seamless for the connecting user.

To satisfy the above basic requirements, a secure connectivity framework is needed to ensure that remote access to the corporate network is securely enabled.

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

Depending on the access requirement, remote users can access through SSL VPN Client or End user Web Portal (clientless access).

SSL VPN is not supported when Cyberoam is deployed as Bridge.

Concepts of SSL VPN

SSL VPN Access Modes

When a remote user connects to the Cyberoam appliance, the Cyberoam appliance authenticates the user based on user name and password. A successful login determines the access rights of remote users according to user group SSL VPN policy. The user, group and SSL VPN policy specifies whether the connection will operate in Tunnel access mode, Web Access mode or Application Access Mode.

Tunnel Access mode

Tunnel access mode provides access to the Corporate network to remote users through laptops as well as from Internet cafes, hotels, airport etc. It requires an SSL VPN Client at the remote end. Remote users are required to download and install SSL VPN Client from the End-user Web Portal.

SSL VPN client establishes a SSL VPN tunnel over the HTTPS link between the web browser and the Cyberoam appliance to encrypt and send the traffic to the Cyberoam appliance.

To avoid the bandwidth choking, split tunnel can be configured which ensures that only the traffic for the private network is encrypted and tunneled while the Internet traffic is send through the usual unencrypted route.

In this mode, Cyberoam acts as a secure HTTP/HTTPS gateway and authenticates the remote users. On successful authentication, Cyberoam redirects the web browser to the Web portal. Remote users can download SSL VPN client and configuration file for installation. Configuring Tunnel Access mode is a two-step process:

1. Select Tunnel Access mode in VPN SSL policy
2. Assign policy to the user group

For administrators, Cyberoam Web Admin console provides SSL VPN management. Administrator can configure SSL VPN users, access method and policies, network resources, and system and portal settings.

For remote users:

- Access End user Web Portal
- Download and install SSL VPN Client on desktop machine
- Import Configuration files downloaded from End user Web Portal

Web Access mode

Web Access mode provides access to the remote users who are equipped with the web browser only and when access is to be provided to the certain Enterprise Web applications/servers through web browser only. In other words, it offers a clientless network access using any web browser. The feature comprises of an SSL daemon running on the Cyberoam unit and End user Web portal which provides users with access to network services and resources.

In this mode, Cyberoam acts as a secure HTTP/HTTPS gateway and authenticates the remote users. On successful authentication, Cyberoam redirects the web browser to the Web portal from where remote users can access the applications behind the Cyberoam appliance. Configuring Web Access mode is a two-step process:

3. Select Web Access mode in VPN SSL policy
4. Assign policy to the user group

For administrators, Cyberoam Web Admin console provides SSL VPN management. Administrator can configure SSL VPN users, access method and policies, user bookmarks for network resources, and system and portal settings.

For remote users, customizable End user Web Portal enables access to resources as per the configured SSL VPN policy.

With no hassles of client installation, it is truly a “clientless access”.

Application Access Mode

Application Access mode provides access to web applications as well as certain Enterprise applications to the remote users who are equipped with the web browser only. Application access mode also offers a clientless network access using any web browser. The feature comprises of an SSL daemon running on the Cyberoam unit and End user Web portal which provides users with access to network services and resources.

Application access allows remote access to different TCP based applications like HTTP, HTTPS, RDP, TELNET, SSH and FTP without installing client.

In this mode, Cyberoam acts as a secure gateway and authenticates the remote users. On successful authentication, Cyberoam redirects the web browser to the Web portal from where remote users can access the applications behind the Cyberoam appliance. Configuring Application Access mode is a two-step process:

1. Select Application Access mode in VPN SSL policy
2. Assign policy to the User or Group

For administrators, Cyberoam Web Admin console provides SSL VPN management. Administrator can configure SSL VPN users, access method and policies, user bookmarks for network resources, and system and portal settings.

For remote users, customizable End user Web Portal enables access to resources as per the configured SSL VPN policy.

With no hassles of client installation, it is also a “clientless access”.

Prerequisite (Remote User)

- **Microsoft Windows supported** – Windows 2000, Windows XP, Windows 7, Windows Vista and Windows Server 2003.
- **Admin Rights Required** – Remote user must be logged on as Admin user or should have Admin privilege.
- **JRE Installation** – Java Runtime Environment V 1.5 or below.

The basic and common administrative configuration for the three modes of operation can be configured from the Tunnel Access, Web Access and Policy.

Threat Free Tunneling

Entire SSL VPN traffic passes through VPN zone and firewall rules and policies can be applied to VPN zone. Due to this, VPN tunnel traffic (incoming and outgoing) is subjected to virus, spam and inappropriate content checks as well as intrusion attempts. These checks makes sure that there are no viruses, worms, spam, and inappropriate content or intrusion attempts in the VPN traffic

and ensures that traffic passing through tunnel is threat free.

As VPN traffic is, by default subjected to the DoS inspection, Cyberoam also provides a facility by which one can bypass scanning of traffic coming from certain hosts from the VPN zone.

Please note that by default Cyberoam provides VPN zone but whenever the connection is established, port/interface used by the connection is automatically added to the VPN zone and on disconnection; port is automatically removed from the zone.

Threat Free Tunneling is applicable only when SSL VPN tunnel is established through tunnel access mode.

VPN zone is used by both IPSec and SSL VPN traffic.

Network Resources

Network Resources are the components that can be accessed using SSL VPN. SSL VPN provides access to an HTTP or HTTPS server on the internal network, Internet, or any other network segment that can be reached by the Cyberoam. The Administrator can configure Web (HTTP), Secure Web (HTTPS), RDP, Telnet, SSH or FTP bookmarks and internal network resources to allow access to Web-based resources and applications.

If required, custom URL access can also be provided.

Network resources:

- Bookmarks - Web Access mode, Application Access Mode
- Bookmark Groups - Web Access mode, Application Access Mode
- Custom URLs – Not defined as Bookmark - Web Access mode
- Enterprise Private Network resources - Tunnel access mode

Portal

Cyberoam's End-user Web Portal provides remote users with easy access to the network resources through a secure tunnel. Components like bookmarks and other network resources are presented to users through this portal. The portal determines what the remote user sees when they logon to the Cyberoam.

As End-user Web Portal is an entry point to the Corporate network, it is possible to customize the portal interface by including company logo and a customized message to be displayed to users when they log in to the portal to access network resources.

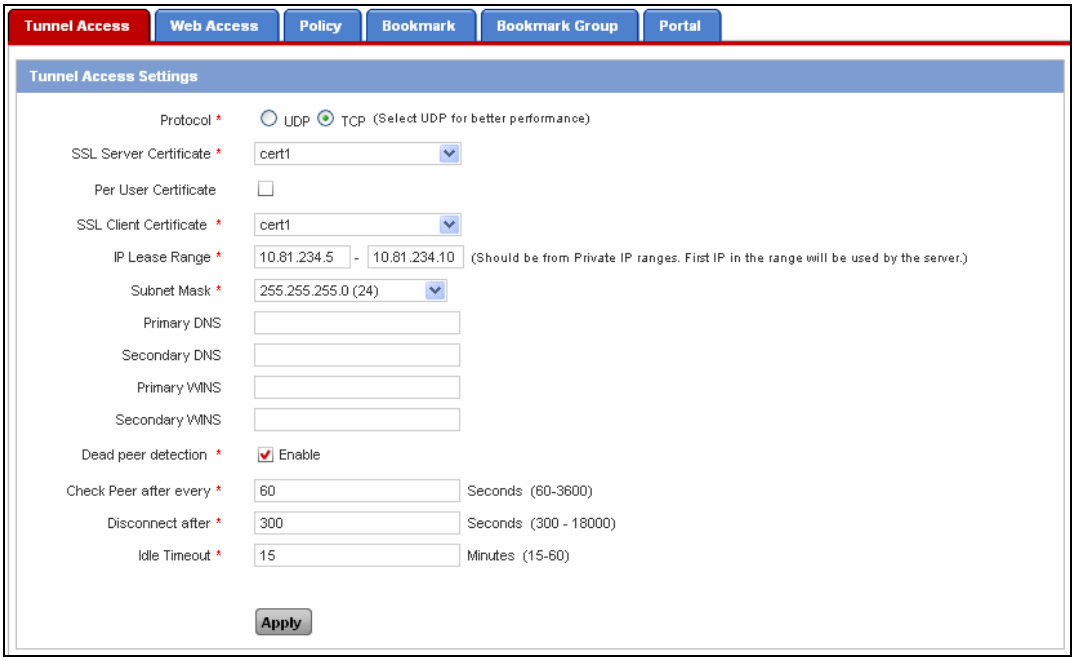
Access Mode Settings

SSL VPN Settings can be configured for all the three modes i.e. Tunnel Access mode, Web Access mode and Application Access mode.

Tunnel Access

Configure Tunnel Access mode for the remote users who are to be provided with the Corporate network access from laptops, Internet cafes, hotels etc. It requires an SSL VPN Client at the remote end. Remote users can download and install SSL VPN Client from the End-user Web Portal.

To configure and update certain parameters globally for Tunnel Access mode, go to **VPN → SSL → Tunnel Access**.



Screen – Tunnel Access Configuration

Screen Elements	Description
Protocol	Select protocol TCP or UDP. Selected network protocol will be the default protocol for all the SSL VPN clients. Connection over UDP provides better performance.
SSL Server Certificate	Select SSL Server certificate from the dropdown list to be used for authentication. If you do not have certificate, generate: **Available options**: Certificate signing request (CSR) using the default CA from Objects → Certificate → Certificate Self-signed certificate from Objects → Certificate → Certificate
Per User Certificate	Click Per User Certificate if you want to use individual user certificate for authentication. 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. Cyberoam automatically generates certificate valid up to 31st December, 2036 for all the users added in Cyberoam.
SSL Client Certificate	Select the SSL Client certificate from the dropdown list if you want to use common certificate for authentication. If you do not have certificate, generate: Self-signed certificate from Objects → Certificate → Certificate The selected certificate is bundled with the Client installer and is downloaded when remote users install SSL client. Remote users/SSL Clients represent the selected certificate to the server

	for authenticating themselves. Same certificate can be used for both SSL Server and Client.
IP Lease Range	Specify the range of IP addresses reserved for the SSL Clients. SSL clients will be leased IP address from the configured pool.
Subnet Mask	Specify Subnet mask.
Primary DNS	Specify IP addresses of Primary DNS servers to be provided for the use of Clients. **Note** Do not assign the private IP address space that is already configured for any ports via Network Configuration.
Secondary DNS	Specify IP addresses of Secondary DNS servers to be provided for the use of Clients.
Primary WINS	Specify IP addresses of Primary WINS servers to be provided for the use of Clients.
Secondary WINS	Specify IP addresses of Secondary WINS servers to be provided for the use of Clients.
Dead Peer Detection	Click “Enable Dead Peer Detection” checkbox to enable Dead Peer Detection.
Check Peer After Every	Specify time interval in the range of 60 to 3600 seconds after which the peer should be checked for its status. Default – 60 seconds.
Disconnect After	Specify time interval in the range of 300 to 1800 seconds after which the connection should be disconnected if peer is not live. Default – 300 seconds.
Idle Timeout	Specify idle timeout. Connection will be dropped after the configured inactivity time and user will be forced to re-login. Default – 15 minutes.

Table – Tunnel Access screen elements

Web Access

Configure Web Access mode for the remote users who are equipped with the web browser only and when access is to be provided to the certain Enterprise Web applications/servers through web browser only. In other words, it is a clientless access.

To configure Web Access mode, go to **VPN → SSL → Web Access**.

Screen – Web Access Configuration

Screen Elements	Description
Idle Timeout	Specify idle timeout. Connection will be dropped after the configured inactivity time and user will be forced to re-login. Default – 10 minutes.

Table – Web Access screen elements

Application Access

Configure Application Access mode for the remote users who are equipped with the web browser only and when access is to be provided to the certain Enterprise Web applications/servers through web browser only. It is also a clientless access.

Application access allows remote access to different TCP based applications like HTTP, HTTPS, RDP, TELNET, SSH and FTP without installing client.

To configure Application Access mode, follow these steps:

1. Select Application Access mode in VPN SSL policy and add URL bookmarks that can be accessed by remote users. To configure SSL VPN policies, go to Add SSL VPN Policy.
2. Assign policy to the User or Group from Identity menu.

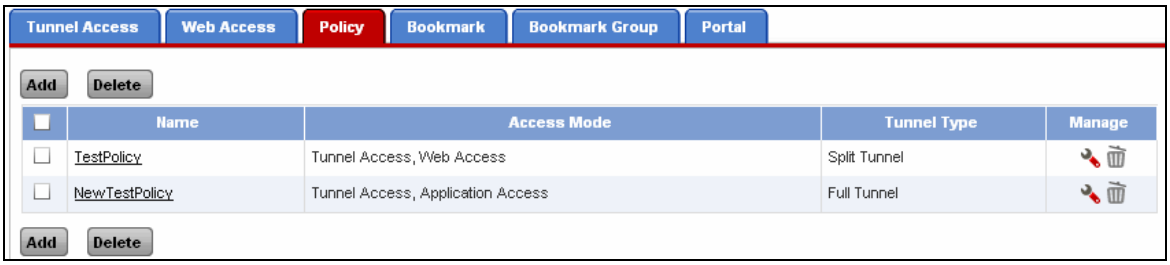
Policy

SSL VPN policy determines access mode available to the remote users and also controls the access to the private network (corporate network) in the form bookmarks.

To configure SSL VPN Policies, go to **VPN → SSL → Policy**. You can:

- Add
- View
- Edit – Click the Edit icon in the Manage column against the SSL VPN Policy to be modified. Edit SSL VPN Policy is displayed in a new window which has the same parameters as the Add SSL VPN Policy window.
- Delete – Click the Delete icon in the Manage column against a SSL VPN Policy to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the SSL VPN Policy. To delete multiple SSL VPN policies, select them and click the Delete button.

Manage SSL VPN Policies



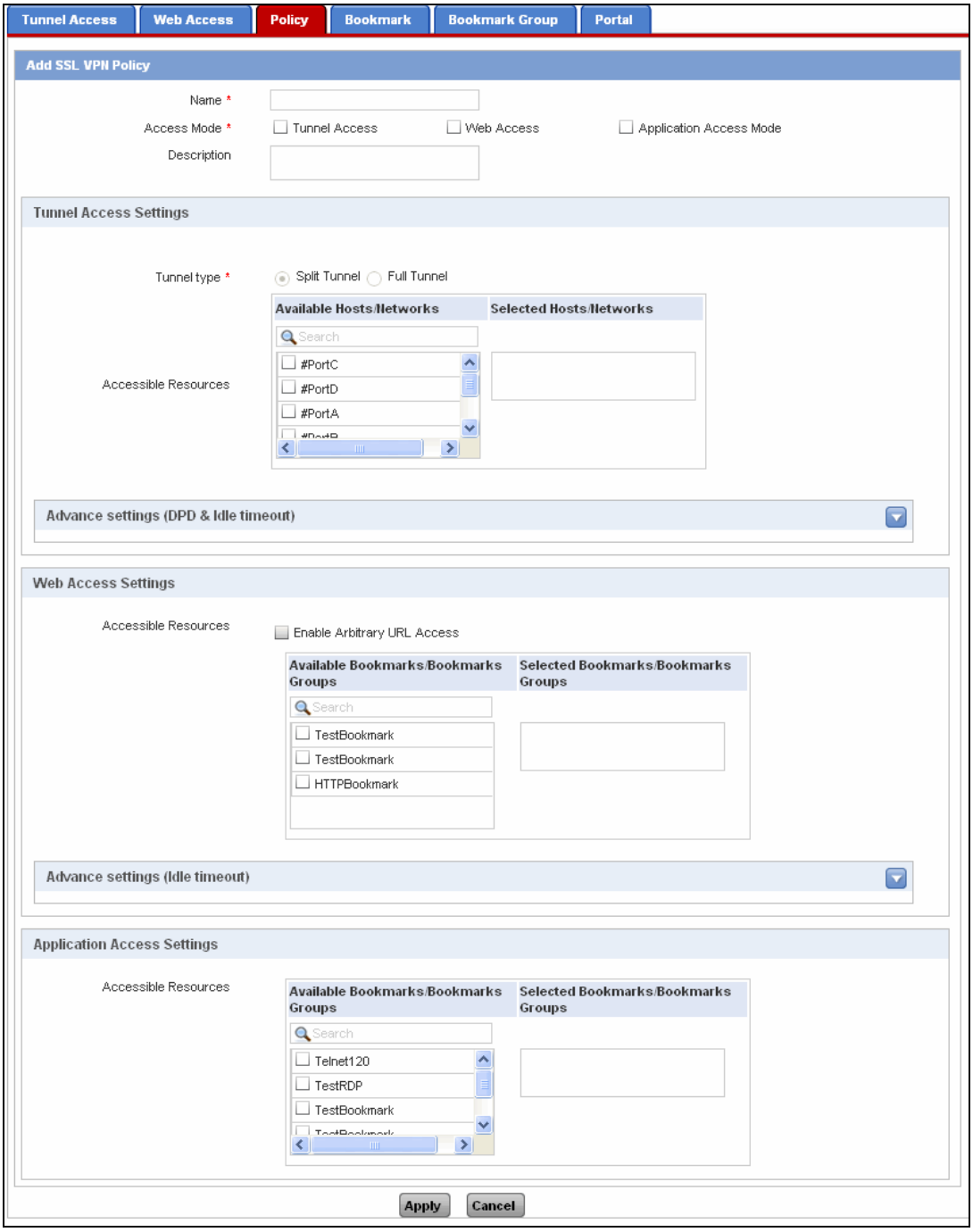
Screen – Manage SSL VPN Policies

Screen Elements	Description
Add Button	Add a new SSL VPN Policy
Name	Name of the SSL VPN Policy
Access Mode	Access Mode of the Policy: Tunnel Access, Web Access or Application Access
Tunnel Type	Type of Tunnel established: Split or Full Tunnel
Edit Icon	Edit the SSL VPN Policy
Delete Button	Delete the SSL VPN Policy Alternately, click the delete icon against the policy to be deleted.

Table – Manage SSL VPN Policies screen elements

SSL VPN Policy Parameters

To add or edit SSL VPN policies, go to **VPN → SSL → Policy**. Click Add Button to add a new policy or Edit Icon to modify the details of the policy.



Screen – Add SSL VPN Policy

Screen Elements	Description
Name	Name to identify the SSL VPN policy
Access Mode	Select the access mode by clicking the appropriate option.

	Available options: **Tunnel Access Mode** – for the remote users who are to be provided with the Corporate network access from laptops, Internet cafes, hotels etc. It requires an SSL VPN Client at the remote end. Remote users can download and install SSL VPN Client from the End-user Web Portal. **Web Access Mode** – for the remote users who are equipped with the web browser only and when access is to be provided to the certain Enterprise Web applications/servers through web browser only. It provides clientless network access using any web browser through End-user Web Portal. Remote users are authenticated by Cyberoam and redirected to the End-user Web Portal through which Enterprise Web applications/servers can be accessed. **Application Access Mode** – for the remote users who are equipped with the web browser only and when access is to be provided to the certain Enterprise applications/servers through web browser only. It provides clientless network access using any web browser through End-user Web Portal. Remote users are authenticated by Cyberoam and redirected to the End-user Web Portal through which Enterprise applications can be accessed. Applications are opened in the browser itself.
Description	Specify SSL VPN Policy Description
Tunnel Access Mode	
Tunnel Type	Select tunnel type. Tunnel type determines how the remote user's traffic will be routed. **Available options**: • **Split Tunnel** - ensures that only the traffic for the private network is tunneled and encrypted • **Full Tunnel** – ensures not only private network traffic but other Internet traffic is tunneled and encrypted. By default, split tunnel is enabled.
Accessible Resources	Accessible Resources allows restricting the access to the certain hosts of the private network. User's access to private network is controlled through his SSL VPN policy while Internet access is controlled through his Internet Access policy. 'Available Host/Network' list displays the list of available hosts and network. All the hosts added from Hosts menu, IP Host will be displayed in the list. Select or Clear the Hosts to add or remove from the list. 'Selected Host/Network' list displays the list of Host/Network that remote user can access.

DPD Settings	One can customize and override the global Dead Peer Detection setting. To use Global settings, click “Use Global Settings” To override the Global settings, click “Override Global Settings” Click “Enable DPD” checkbox to enable Dead Peer Detection check at regular interval whether peer is live or not. Specify time interval after which the peer should be checked for its status. Default – 60 seconds Specify time interval after which the connection should be disconnected if peer is not live. Default – 300 seconds
Idle Timeout	Connection will be dropped after the configured inactivity time and user will be forced to re-login. One can use the global settings or customize the idle timeout. To use Global settings, click “Use Global Settings”. Default – 15 minutes To override the Global settings, click “Override Global Settings” and specify idle timeout. Range: 15-60 minutes
Web Access Mode	
Accessible Resources	Accessible Resources also allows restricting the access to the bookmarks. Click ‘Enable Arbitrary URL Access’ to enable the access to custom URLs. ‘Available Bookmarks/Bookmarks Group’ list displays the list of available resources. All the Bookmarks/Bookmarks Group added will be displayed in the list. Select or Clear the Bookmarks to add or remove from the list. ‘Selected Bookmarks/Bookmarks Group’ list displays the list of Bookmarks/Bookmarks Group that remote user can access.
Idle Timeout	Connection will be dropped after the configured inactivity time and user will be forced to re-login. One can use the global settings or customize the idle timeout. To use Global settings, click “Use Global Settings”. Default – 10 minutes To override the Global settings, click “Override Global Settings” and specify idle timeout. Range: 10-60 minutes
Application Access Mode	

Accessible Resources	Accessible Resources also allows restricting the access to the bookmarks. 'Available Bookmarks/Bookmarks Group' list displays the list of available resources. All the Bookmarks/Bookmarks Group added will be displayed in the list. Select or Clear the Bookmarks to add or remove from the list. 'Selected Bookmarks/Bookmarks Group' list displays the list of Bookmarks/Bookmarks Group that remote user can access.

Table – Add SSL VPN Policy screen elements

Bookmark

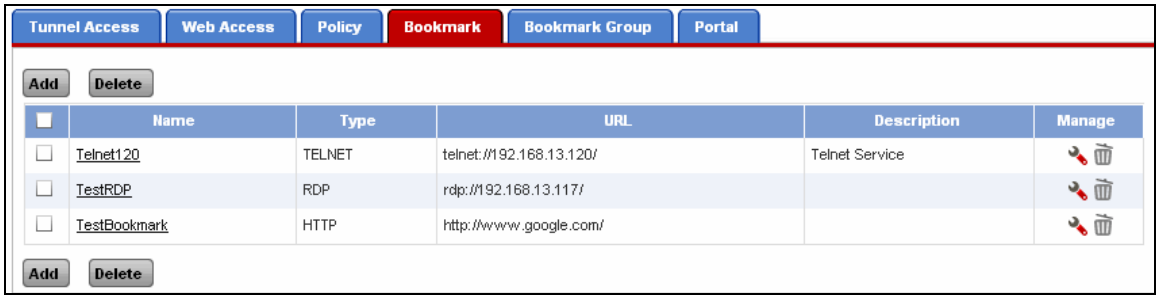
Bookmarks are the resources whose access will be available through End-user Web portal. You can create also a group of bookmarks that can be configured in SSL VPN Policy.

These resources will be available in Web Access mode only and is to be configured in SSL VPN Policy.

To manage Bookmarks, go to **VPN → SSL → Bookmark**. You can:

- Add
- View
- Edit – Click the Edit icon in the Manage column against the Bookmark to be modified. Edit Bookmark pop-up window is displayed which has the same parameters as the Add Bookmark window.
- Delete – Click the Delete icon in the Manage column against a Bookmark to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Bookmark. To delete multiple Bookmarks, select them and click the Delete button.

Manage Bookmarks



Screen – Manage Bookmarks

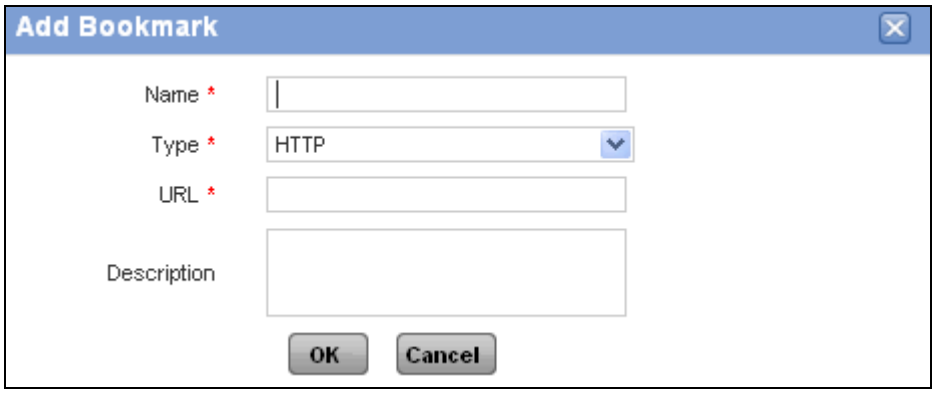
Screen Elements	Description
Add Button	Add a new Bookmark
Name	Name for the Bookmark
Type	Type of Bookmark selected: HTTP, HTTPS, RDP, Telnet, SSH

	or FTP
URL	URL for which the bookmark is created
Description	Bookmark Description
Edit icon	Edit the Bookmark
Delete Button	Delete the Bookmark Alternately, click the delete icon against the bookmark to be deleted.

Table – Manage Bookmarks screen elements

Bookmark Parameters

To add or edit bookmarks, go to **VPN → SSL → Bookmark**. Click Add Button to add a new bookmark or Edit Icon to modify the details of the bookmark.



Screen – Add Bookmark

Screen Elements	Description
Bookmark Name	Name to identify the Bookmark.
Type	Select the type of Bookmark **Available Options**: HTTP HTTPS RDP Telnet SSH FTP
URL	Specify the URL of the website for which the bookmark is to be created.
Description	Specify Bookmark Description

Table – Add Bookmark screen elements

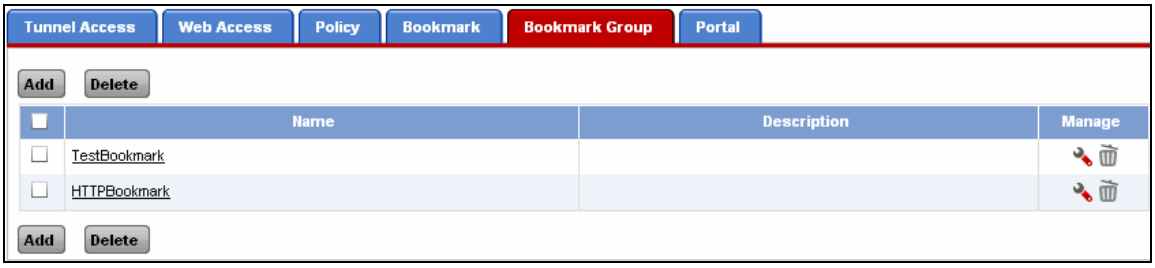
Bookmark Group

To manage Bookmark Groups, go to **VPN → SSL → Bookmark Group**. You can:

- Add

- View
- Edit – Click the Edit icon in the Manage column against the Bookmark Group to be modified. Edit Bookmark Group pop-up window is displayed which has the same parameters as the Add Bookmark Group window.
- Delete – Click the Delete icon in the Manage column against a Bookmark Group to be deleted. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Bookmark Group. To delete multiple Bookmark Groups, select them and click the Delete button.

Manage Bookmark Groups



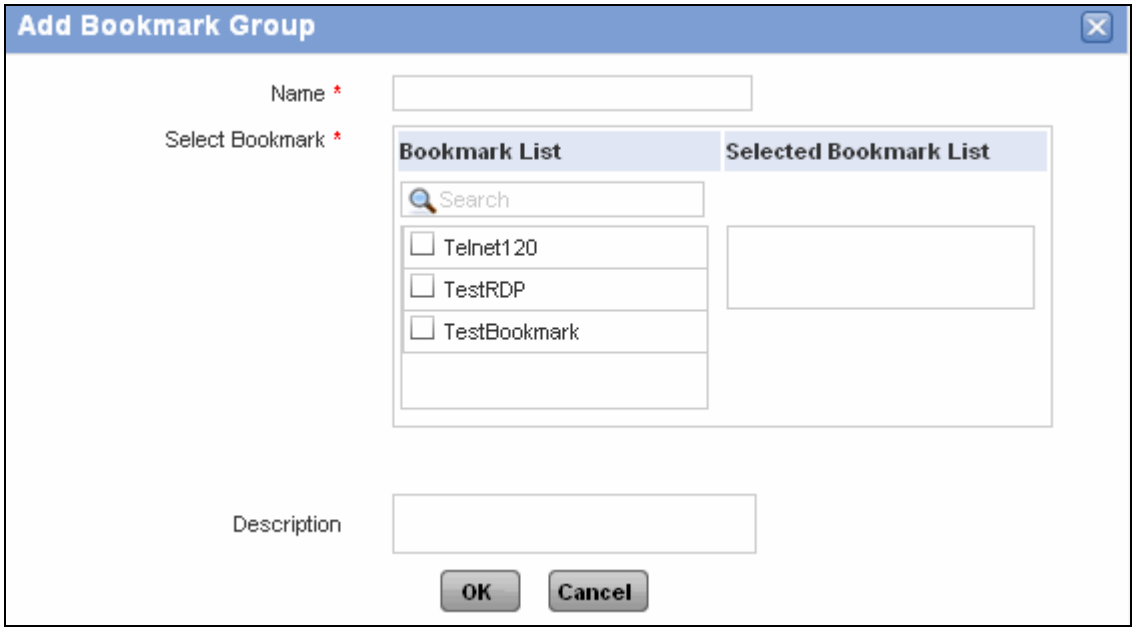
Screen – Manage Bookmark Groups

Screen Elements	Description
Add Button	Add a new Bookmark Group
Name	Name for the Bookmark Group
Description	Bookmark Group Description
Edit	Edit the Bookmark Group
Delete Button	Delete the Bookmark Group Alternately, click the delete icon against the bookmark group to be deleted.

Table – Manage Bookmark Group screen elements

Bookmark Group Parameters

To add or edit bookmarks, go to **VPN → SSL → Bookmark Group**. Click Add Button to add a new bookmark group or Edit Icon to modify the details of the bookmark group.



Screen – Add Bookmark Group

Screen Elements	Description
Bookmark Group Name	Name to identify the Bookmark Group.
Select Bookmark	Select bookmarks to be grouped. 'Available Bookmarks' list displays the list of bookmarks that can be added to the group. 'Selected Bookmarks' list displays the list of bookmarks that are included in the group. Select or clear the Bookmarks to add or remove from the list
Description	Specify Bookmark Group Description

Table – Add Bookmark Group screen elements

Portal

As End-user Web Portal is an entry point to the Corporate network, Cyberoam provides flexibility to customize the Portal page to offer consistent logon/log off page. This page can be exclusive to your business including your business name and logo.

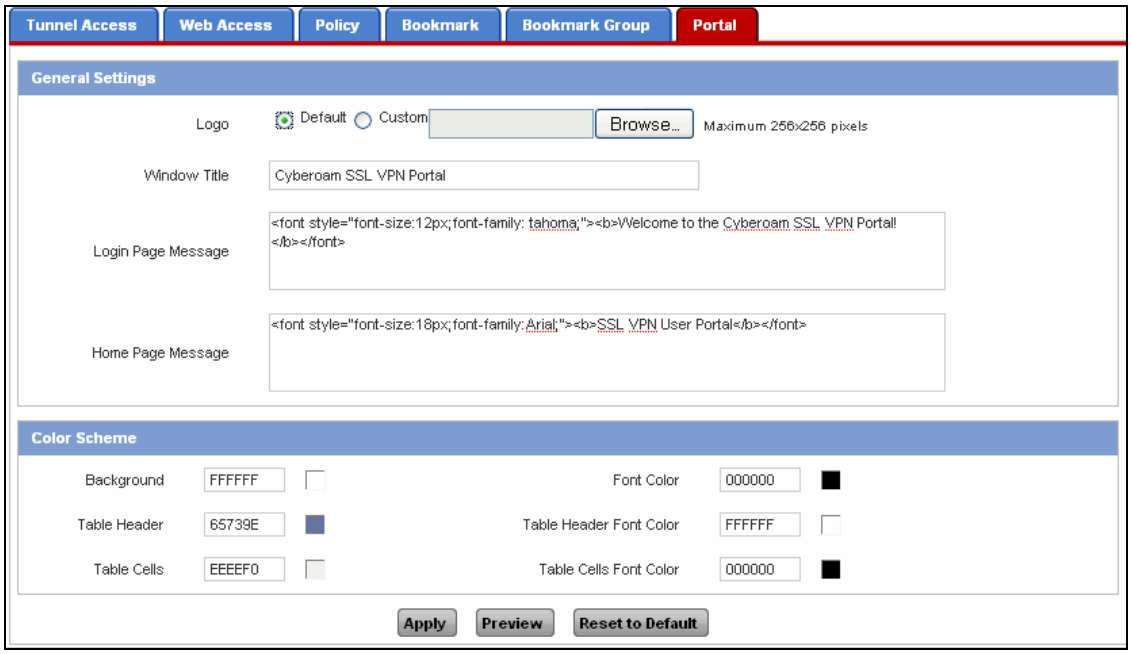
Cyberoam Administrator needs to provide End user Web portal URL - https://<WAN IP address of Cyberoam:port> to the remote users. Use default port: 8443 unless customized. Confirm port number from **System → Administration → Settings** before forwarding URL to the remote user.

Remote users can download SSL VPN client, and Configuration file from the portal. All the downloadable components will be displayed only if the remote user is allowed the "Full" access".

A list of all the bookmarks will be displayed to Remote user. URL Address bar will also be

displayed to the user, if allowed in the User SSL VPN policy. User can type the URL in the Address bar to access other URLs than bookmarks.

To customize the SSL VPN user portal, go to **VPN → SSL → Portal**.



Screen – SSL VPN User Portal

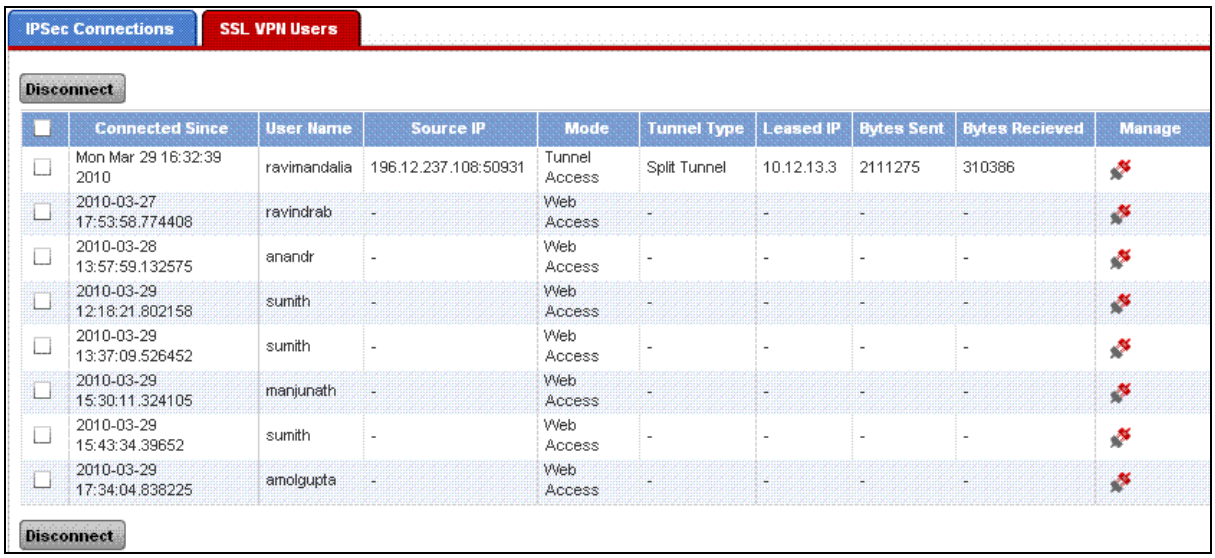
Screen Elements	Description
Logo	To upload the custom logo, specify Image file name to be uploaded else click “Default”. Use “Browse” button to select the complete path. The image size should not exceed 256 X 256 pixels.
Window Title	Change the Window title if required.
Login Page Message	Specify message to be displayed on the Portal login page
Home Page Message	Specify message to be displayed on the Portal. This message can reflect your business or even a welcome message.
Color Scheme	Customize the color scheme of the portal if required. Specify the color code or click the square box to pick the color.
Preview Button	Click to view the custom settings before saving the changes.
Reset to Default Button	Click to revert to default settings

Table – SSL VPN Portal screen elements

Live SSL VPN Users

To view the list of all the currently logged on SSL VPN users through both the access modes, go to **VPN → Live Connections → SSL VPN Users**.

Page displays important parameters like Username, Source and leased IP address, Access mode, date and time when connection was established, tunnel type and data transferred. If the connection is established through Web Access mode, only username, access mode and date and time when connection was established will be displayed. Page allows administrator to disconnect any of the live user.



Screen – Live SSL VPN Users