Important Notice

Cyberoam Technologies Pvt. Ltd. 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. Cyberoam Technologies Pvt. Ltd. assumes no responsibility for any errors that may appear in this document. Cyberoam Technologies Pvt. Ltd. reserves the right, without notice to make changes in product design or specifications. Information is subject to change without notice.

USER’S LICENSE

Use of this product and document is subject to acceptance of the terms and conditions of Cyberoam End User License Agreement (EULA) and Warranty Policy for Cyberoam UTM Appliances.

You will find the copy of the EULA at [http://www.cyberoam.com/documents/EULA.html](http://www.cyberoam.com/documents/EULA.html) and the Warranty Policy for Cyberoam UTM Appliances can be found in [http://kb.cyberoam.com](http://kb.cyberoam.com).

RESTRICTED RIGHTS

Copyright 1999 - 2015 Cyberoam Technologies Private Ltd. All rights reserved. Cyberoam, Cyberoam logo are trademark of Cyberoam Technologies Pvt. Ltd.

Corporate Headquarters

Cyberoam House,
Saigulshan Complex, Opp. Sanskruti,
Beside White House, Panchwati Cross Road,
Ahmedabad - 380006, GUJARAT, INDIA.
Tel: +91-79-66216666
Fax: +91-79-26407640 Web site: [www.cyberoam.com](http://www.cyberoam.com)
Contents

Preface ........................................................................................................................................... 4
  Technical Support .......................................................................................................................... 5
Introduction ..................................................................................................................................... 6
Appliance Administrative Interfaces ............................................................................................... 7
  Web Admin Console ...................................................................................................................... 7
  Command Line Interface (CLI) Console ....................................................................................... 8
  Cyberoam Central Console (CCC) ............................................................................................... 8
Web Admin Console ......................................................................................................................... 9
  Web Admin Language ................................................................................................................... 9
  Supported Browsers ...................................................................................................................... 10
  Login procedure .......................................................................................................................... 11
  Log out procedure ....................................................................................................................... 12
  Menus and Pages ......................................................................................................................... 13
  Page ........................................................................................................................................... 15
  Icon bar ...................................................................................................................................... 16
  List Navigation Controls ............................................................................................................ 16
  Tool Tips .................................................................................................................................... 17
  Status Bar ................................................................................................................................... 17
  Common Operations .................................................................................................................... 18
Virus ................................................................................................................................................ 20
Cyberoam Gateway Anti Virus ........................................................................................................ 21
  Enable Anti Virus scanning ........................................................................................................ 22
  Email ......................................................................................................................................... 23
    Configuration file Size Scanning Restriction ........................................................................... 23
    SMTP/S Scanning Rules ............................................................................................................ 25
    POP/IMAP Scanning Rules ........................................................................................................ 29
    Address Group .......................................................................................................................... 30
HTTP/S ............................................................................................................................................ 33
  Configuration ............................................................................................................................... 33
  HTTP Scanning Rules .................................................................................................................. 36
  HTTPS Scanning Exceptions ....................................................................................................... 38
FTP ................................................................................................................................................... 40
Quarantine ...................................................................................................................................... 41
Preface

Cyberoam (Unified Threat Management) UTM appliances offer identity-based comprehensive security to organizations against blended threats - worms, viruses, malware, data loss, identity theft; threats over applications viz. Instant Messengers; threats over secure protocols viz. HTTPS; and more. They also offer wireless security (WLAN) and 3G wireless broadband and analog modem support can be used as either Active or Backup WAN connection for business continuity.

Cyberoam integrates features like stateful inspection firewall, VPN, Gateway Anti Virus and Anti-Spyware, Gateway Anti-Spam, Intrusion Prevention System, Content & Application Filtering, Data Leakage Prevention, IM Management and Control, Layer 7 visibility, Bandwidth Management, Multiple Link Management, Comprehensive Reporting over a single platform.

Cyberoam has enhanced security by adding an 8th layer (User Identity) to the protocol stack. Advanced inspection provides L8 user-identity and L7 application detail in classifying traffic, enabling Administrators to apply access and bandwidth policies far beyond the controls that traditional UTMs support. It thus offers security to organizations across layer 2 - layer 8, without compromising productivity and connectivity.

Cyberoam UTM appliances accelerate unified security by enabling single-point control of all its security features through a Web 2.0-based GUI. An extensible architecture and an ‘IPv6 Ready’ Gold logo provide Cyberoam the readiness to deliver on future security requirements.

Cyberoam provides increased LAN security by providing separate port for connecting to the publicly accessible servers like Web server, Mail server, FTP server etc. hosted in DMZ which are visible the external world and still have firewall protection.

- Note
- Default Web Admin Console username is ‘admin’ and password is ‘admin’
- Cyberoam recommends that you change the default password immediately after installation to avoid unauthorized access.
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
Cyberoam House,
Saigulshan Complex, Opp. Sanskruti,
Beside White House, Panchwati Cross Road,
Ahmedabad - 380006, GUJARAT, INDIA.
Tel: +91-79-66216666
Fax: +91-79-26407640
Web site: www.cyberoam.com

Cyberoam contact:
Technical support (Corporate Office): +91-79-66216565
Email: support@cyberoam.com
Web site: www.cyberoam.com

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

Welcome to Cyberoam’s – Anti Virus User guide.

This Guide provides information on how to configure Cyberoam Anti Virus solution and helps you manage and customize the Appliance to meet your organization’s various requirements including creating groups and users and assigning policies to control web as well as application access.

Note

All the screen shots in this Guide have been taken from NG series Appliances using (Internet Explorer) IE browser. Different browser might render GUI in different ways. The features and functionalities however remain unchanged across all Appliances.
Appliance Administrative Interfaces

Appliance can be accessed and administered through:

1. Web Admin Console
2. Command Line Interface Console
3. Cyberoam Central Console

Administrative Access An administrator can connect and access the Appliance through HTTP, HTTPS, telnet, or SSH services. Depending on the Administrator login account profile used for access, an administrator can access number of Administrative Interfaces and Web Admin Console configuration pages.

Appliance is shipped with two administrator accounts and four administrator profiles.

<table>
<thead>
<tr>
<th>Administrator Type</th>
<th>Login Credentials</th>
<th>Console Access</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Super Administrator</td>
<td>admin/admin</td>
<td>Web Admin Console CLI console</td>
<td>Full privileges for both the consoles. It provides read-write permission for all the configuration performed through either of the consoles.</td>
</tr>
<tr>
<td>Default</td>
<td>cyberoam/cyber</td>
<td>Web Admin console only</td>
<td>Full privileges. It provides read-write permission for all the configuration pages of Web Admin console.</td>
</tr>
</tbody>
</table>

Note

We recommend that you change the password of both the users immediately on deployment.

Web Admin Console

Web Admin Console is a web-based application that an Administrator can use to configure, monitor, and manage the Appliance.

You can connect to and access Web Admin Console of the Appliance using HTTP or a HTTPS connection from any management computer using web browser:

1. HTTP login: http://<LAN IP Address of the Appliance>
2. HTTPS login: https://<LAN IP Address of the Appliance>

For more details, refer section Web Admin Console.
Command Line Interface (CLI) Console

Appliance CLI console provides a collection of tools to administer, monitor and control certain Appliance component. The Appliance can be accessed remotely using the following connections:

1. Remote login Utility – TELNET login
To access Appliance from command prompt using remote login utility – Telnet, use command TELNET <LAN IP Address of the Appliance>. Use default password “admin”.

2. SSH Client (Serial Console)
SSH client securely connects to the Appliance and performs command-line operations. CLI console of the Appliance can be accessed via any of the SSH client using LAN IP Address of the Appliance and providing Administrator credentials for authentication.

Note
Start SSH client and create new Connection with the following parameters:
Host – <LAN IP Address of the Appliance>
Username – admin
Password – admin

Use CLI console for troubleshooting and diagnose network problems in details. For more details, refer version specific Console Guide available on http://docs.cyberoam.com/.

Cyberoam Central Console (CCC)

Distributed Cyberoam Appliances can be centrally managed using a single Cyberoam Central Console (CCC) Appliance, enabling high levels of security for Managed Security Service Provider (MSSPs) and large enterprises. To monitor and manage Cyberoam using CCC Appliance you must:

1. Configure CCC Appliance in Cyberoam
2. Integrate Cyberoam Appliance with CCC using: Auto Discovery or Manually
Once you have added the Appliances and organized them into groups, you can configure single Appliance or groups of Appliances.

For more information, please refer CCC Administrator Guide.
Web Admin Console

CyberoamOS uses a Web 2.0 based easy-to-use graphical interface termed as Web Admin Console to configure and manage the Appliance.

You can access the Appliance for HTTP and HTTPS web browser-based administration from any of the interfaces. Appliance when connected and powered up for the first time, it will have a following default Web Admin Console Access configuration for HTTP and HTTPS services.

<table>
<thead>
<tr>
<th>Services</th>
<th>Interface/Zones</th>
<th>Default Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>LAN, WAN</td>
<td>TCP Port 80</td>
</tr>
<tr>
<td>HTTPS</td>
<td>WAN</td>
<td>TCP Port 443</td>
</tr>
</tbody>
</table>

The administrator can update the default ports for HTTP and HTTPS services from **System > Administration > Settings**.

Web Admin Language

The Web Admin Console supports multiple languages, but by default appears in English. To cater to its non-English customers, apart from English, Chinese-Simplified, Chinese-Traditional, Hindi, Japanese and French languages are also supported. Administrator can choose the preferred GUI language at the time of logging on.

Listed elements of Web Admin Console will be displayed in the configured language:

- Dashboard Doclet contents
- Navigation menu
- Screen elements including field & button labels and tips
- Error messages
Supported Browsers

You can connect to the Web Admin Console of the Appliance using HTTP or a secure HTTPS connection from any management computer using one of the following web browsers:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Internet Explorer</td>
<td>Version 8+</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Version 3+</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>All versions</td>
</tr>
<tr>
<td>Safari</td>
<td>5.1.2(7534.52.7)+</td>
</tr>
<tr>
<td>Opera</td>
<td>15.0.1147.141+</td>
</tr>
</tbody>
</table>

The minimum screen resolution for the management computer is 1024 X 768 and 32-bit true x-color.

The Administrator can also specify the description for firewall rule, various policies, services and various custom categories in any of the supported languages.

All the configuration done using Web Admin Console takes effect immediately. To assist you in configuring the Appliance, the Appliance includes a detailed context-sensitive online help.
Login procedure

The log on procedure authenticates the user and creates a session with the Appliance until the user logs off.

To get to the login window, open the browser and type the LAN IP Address of Cyberoam in the browser's URL box. A dialog box appears prompting you to enter username and password.

![Login Screen](image)

**Screen – Login Screen**

<table>
<thead>
<tr>
<th>Screen Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Enter user login name. If you are logging on for the first time after installation, use the default username.</td>
</tr>
<tr>
<td>Password</td>
<td>Specify user account password. Dots are the placeholders in the password field. If you are logging on for the first time after installation with the default username, use the default password.</td>
</tr>
<tr>
<td>Language</td>
<td>Select the language. The available options are Chinese-Simplified, Chinese-Traditional, English, French, and Hindi. Default – English</td>
</tr>
<tr>
<td>Log on to</td>
<td>To administer Cyberoam, select ‘Web Admin Console’. To view logs and reports, select “Reports”. To login into your account, select “My Account”.</td>
</tr>
<tr>
<td>Login button</td>
<td>Click to log on the Web Admin Console.</td>
</tr>
</tbody>
</table>

**Screen – Login screen elements**

The Dashboard appears as soon as you log on to the Web Admin Console. It provides a quick and fast overview of all the important parameters of your Appliance.
Log out procedure

To avoid un-authorized users from accessing Cyberoam, log off after you have finished working. This will end the session and exit from Cyberoam.

To log off from the Appliance, click the button located at the top right of any of the Web Admin Console pages.
Menus and Pages

The Navigation bar on the leftmost side provides access to various configuration pages. This menu consists of sub-menus and tabs. On clicking the menu item in the navigation bar, related management functions are displayed as submenu items in the navigation bar itself. On clicking submenu item, all the associated tabs are displayed as the horizontal menu bar on the top of the page. To view a page associated with the tab, click the required tab.

The left navigation bar expands and contracts dynamically when clicked on without navigating to a submenu. When you click on a top-level heading in the left navigation bar, it automatically expands that heading and contracts the heading for the page you are currently on, but it does not navigate away from the current page. To navigate to a new page, first click on the heading, and then click on the submenu you want navigate to. On hovering the cursor upon the up-scroll icon or the down-scroll icon , automatically scrolls the navigation bar up or down respectively.

The navigation menu includes following modules:

- System – System administration and configuration, firmware maintenance, backup - restore
- Objects – Configuration of various policies for hosts, services, schedules and file type
- Networks – Network specific configuration viz., Interface speed, MTU and MSS settings, Gateway, DDNS
• Identity – Configuration and management of User and user groups
• Firewall – Firewall Rule Management
• VPN – VPN and SSL VPN access configuration
• IPS – IPS policies and signature
• Web Filter – Web filtering categories and policies configuration
• Application Filter – Application filtering categories and policies configuration
• WAF – Web Application Filtering policies configuration. Available in all the models except CR15iNG and CR15wiNG.
• IM – IM controls
• QoS – Policy management viz., surfing quota, QoS, access time, data transfer
• Anti Virus – Antivirus filtering policies configuration
• Anti Spam – Anti Spam filtering policies configuration
• Traffic Discovery – Traffic monitoring
• Logs & Reports – Logs and reports configuration

Note
Use F1 key for page-specific help.
Use F10 key to return to Dashboard.

Each section in this guide shows the menu path to the configuration page. For example, to reach the Zone page, choose the Network menu, then choose Interface sub-menu from the navigation bar, and then choose Zone tab. Guide mentions this path as Network > Interface > Zone.
A typical page looks as shown in the below given image:
Icon bar

The Icon bar on the upper rightmost corner of every page provides access to several commonly used functions like:

1. **Dashboard** – Click to view the Dashboard
2. **Wizard** – Opens a Network Configuration Wizard for a step-by-step configuration of the network parameters like IP Address, subnet mask and default gateway for your Appliance.
3. **Report** – Opens a Reports page for viewing various usage reports. Integrated Logging and Reporting solution - iView, to offer wide spectrum of 1000+ unique user identity-based reporting across applications and protocols and provide in-depth network visibility to help organizations take corrective and preventive measures.

   This feature is not available for CR15xxxx series of Appliances.

4. **Console** – Provides immediate access to CLI by initiating a telnet connection with CLI without closing Web Admin console.
5. **Logout** – Click to log off from the Web Admin Console.
6. **More Options** – Provides options for further assistance. The available options are as follows:
   - **Support** – Opens the customer login page for creating a Technical Support Ticket. It is fast, easy and puts your case right into the Technical Support queue.
   - **About Product** – Opens the Appliance registration information page.
   - **Help** – Opens the context – sensitive help page.
   - **Reset Dashboard** – Resets the Dashboard to factory default settings.
   - **Lock** – Locks the Web Admin Console. Web Admin Console is automatically locked if the Appliance is in inactive state for more than 3 minutes. To unlock the Web Admin Console you need to re-login. By default, Lock functionality is disabled. Enable Admin Session Lock from **System > Administration > Settings**.
   - **Reboot Appliance** – Reboots the Appliance.
   - **Shutdown Appliance** – Shut downs the Appliance.

List Navigation Controls

The Web Admin Console pages display information in the form of lists that are spread across the multiple pages. Page Navigation Control Bar on the upper right top corner of the list provides navigation buttons for moving through the list of pages with a large number of entries. It also includes an option to specify the number entries/records displayed per page.
Tool Tips

To view the additional configuration information use tool tip. Tool tip is provided for many configurable fields. Move the pointer over the icon to view the brief configuration summary.

Status Bar

The Status bar at the bottom of the page displays the action status.

```plaintext
Status : ✓ Country Host 'Sydney_Office' has been added successfully.

Status : ⚠ User could not be registered. User or User group with the same name already exists, choose a different name.
```
Common Operations

Adding an Entity

You can add a new entity like policy, group, user, rule, ir host by clicking the Add button available on most of the configuration pages. Clicking this button either opens a new page or a pop-up window.

![Add and Delete buttons](image)

Editing an Entity

All the editable entities are hyperlinked. You can edit any entity by clicking either the hyperlink or the Edit icon under the Manage column.

![Interface Name and Status](image)

Deleting an Entity

You can delete an entity by selecting the checkbox and clicking the Delete button or Delete icon.

![Groups](image)

To delete multiple entities, select individual entity and click the Delete button.

![Groups](image)
To delete all the entities, select ✔ in the heading column and click the Delete button.

Sorting Lists

To organize a list spread over multiple pages, sort the list in ascending or descending order of a column attribute. You can sort a list by clicking a column heading.

- Ascending Order icon ▼ in a column heading indicates that the list is sorted in ascending order of the column attribute.
- Descending Order icon ▲ in a column heading indicates that the list is sorted descending order of the column attribute.

Filtering Lists

To search specific information within the long list spread over multiple pages, filter the lists. Filtering criteria vary depending on a column data and can be a number or an IP address or part of an address, or any text string combination.

To create filter, click the Filter icon in a column heading. When a filter is applied to a column, the Filter icon changes to 🔍.

Configuring Column Settings

By default on every page all columnar information is displayed but on certain pages where a large number of columnar information is available, all the columns cannot be displayed. It is also possible that some content may not be of use to everyone. Using column settings, you can configure to display only those numbers of columns which are important to you. To configure column settings, click Select Column Settings and select the checkbox against the columns you want to display and clear the checkbox against the columns which you do not want to display. All the default columns are greyed and not selectable.
Virus

A Virus is a self-replicating malicious code that spreads by attaching itself to an application program, any executable system component, or documents and leaves no obvious signs of its presence.

Viruses are hard to detect, easy to propagate, and difficult to remove.

With the number of computer users growing and the exchange of information via the Internet and Email increasing in volume, virus scares are becoming an almost an everyday occurrence. Real mass attacks have become commonplace, and the consequences are serious, resulting in financial loss for individuals and corporations alike.

The number of threats, frequency, and speed of attacks is increasing every day. Anti Virus protection is therefore a priority for anyone who uses a computer.

Although viruses are transmitted mainly through Emails or attachments to an Email note and Internet downloads, a diskette or CD can also be a source of infection. Therefore, the task of comprehensive protection against potential threats now extends beyond simple regular virus scans to real time Anti Virus protection.
Cyberoam Gateway Anti Virus

The Appliance Anti Virus solution as a part of unified solution along with Anti Spam and IPS (Intrusion Prevention System), provides real time virus scanning that protects all network nodes – workstations, files servers and mail system from known and unknown attacks like worms, viruses, Trojans, spyware, adware, Spam, hackers and all other cyber threats.

Cyberoam Anti Virus scans the following traffic as it passes through it:
- HTTP
- HTTPS
- FTP
- SMTP
- SMTP over SSL
- POP3
- IMAP

For extra protection, you can also configure to block specified file types. You can use this feature to stop files that might contain new viruses. Additional filtration of messages from configured IP Address and URL decreases the load on the server when scanning Email traffic for viruses.

It allows to:
- Scan Email messages for viruses.
- Detect infected, suspicious, and password-protected attachments and message.
- Perform Anti Virus processing of infection revealed in Email messages by scanning.
- Provide additional Email Traffic scanning for protocols namely SMTP, SMTP over SSL, POP3 and IMAP.
- Define policies to take appropriate action based on the protocol i.e. define action policy on how to handle SMTP/SMTP over SSL/POP3/FTP/ HTTP/HTTPS traffic if infection is detected.
- Limit HTTP and FTP threshold file size for scanning.
- Notify senders, recipients, and the administrator about messages containing infected, suspicious, or password protected attachments
- Quarantine messages - Quarantine feature allows to isolate and move infected and suspicious mails in a quarantine directory defined by a network administrator.
- Customize the Anti Virus protection of incoming and outgoing Email messages by defining scan policies.

The Appliance Gateway Anti Virus is fully compatible with all the mail systems and therefore can be easily integrated into the existing network.

The Appliance Gateway Anti Virus module is an add-on module, which needs to be subscribed before use.
• FTP
• Quarantine

Note
SMTP/S means both SMTP and SMTP over SSL. Entire configurations done will be applicable to both the traffic. Also, SMTP over SSL and SMTP/S terms are used interchangeably but they mean the same.

Enable Anti Virus scanning
Enable Anti Virus scanning from Firewall Rules. While Anti Virus settings can be configured for system-wide use, they can also be implemented with specific settings on a per user basis. Refer to Cyberoam User Guide, Firewall section for creating Firewall Rules and enabling the Anti Virus scanning.

To enable Anti Virus scanning, go to Firewall > Rule, open an existing Firewall Rule and then in Advanced Settings, enable AV & AS Scanning.

You can enable Anti Virus scanning by creating a Firewall Rule for:
• Zone
• User/User Group
• Host/Host Group
Email

The Appliance offers comprehensive Email Security, preventing sophisticated forms of zero-hour threats and blended attacks involving spam, botnets, phishing, spyware and more. The basic Email protection configuration includes configuring Email threshold size for scanning, specifying the action to be taken if the virus is detected, blocking mails based on sender or recipient, and blocking mails with certain file types.

- Configuration
- SMTP/S Scanning Rules
- POP/IMAP Scanning Rules
- Address Group

Configuration file Size Scanning Restriction

Use the configuration tab to configure scanning of file size restriction for all the SMTP/S, POP and IMAP mails.

To configure restrictions, go to Anti Virus > EMail > Configuration.

Screen Elements | Description
--- | ---
General Configuration
SMTP/S Mails Greater Than Size | Specify maximum file size (in KB) for scanning. Files exceeding this size received through SMTP/S will not be scanned.

Default - 1024 KB

To increase default file size scanning restriction to 51200 KB, specify 0.

For CR15i models, default file size restriction scanning is 1024 KB.

SMTP/S Oversize Mail Action | Specify the action to be taken to handle oversized files. By selecting one of the options you may either:
- Accept – all the oversize mails are forwarded to the
| POP3/IMAP Mails Greater Than Size | Specify maximum file size (in KB) for scanning. Files exceeding this size received through POP/IMAP will not be scanned. 
Default - 1024 KB  
To increase the default file size restriction to 10240 KB for restriction, specify 0.  
For CR15i models, default file size restriction for scanning is 1024 KB. |
| Add Signature To All Emails | Specify the signature to be added to all the outgoing Emails.  
Only text signatures are allowed. |
| SMTPS Scanning CA | Select the CA for scanning SMTP traffic over SSL from the available options.  
**Available Options:**  
- Cyberoam_SSL_CA  
- CyberoamSelfSignedCA  
- List of custom CAs if added  
Default - Cyberoam_SSL_CA |
| Allow Invalid Certificate | If enabled, SMTP over SSL connections will be allowed with invalid certificate from the Mail Server. Disable to reject such connections.  
Default - Enable |

**Table – Email Configuration screen elements**
SMTP/S Scanning Rules

SMTP/S Scanning Rules allows to define policies to take appropriate action based on the protocols. It allows you to create separate action policies in case an infection is detected for SMTP, SMTP over SSL, POP3, FTP, and HTTP traffic respectively.

SMTP policy is applied when the virus is detected in SMTP/S traffic. Depending on the action specified in the policy, Email is quarantined, cured, or deleted, thus preventing the virus from being circulated.

As soon as you subscribe for Gateway Anti Virus, the default SMTP policy is applied to all the inbound and outbound Email traffic. This default policy is a general policy and not a fit-for-all policy, and hence might not fit into your network requirement. Define multiple policies instead of one global policy, as per your requirement. Fine tuning the policies means reducing the virus attacks.

SMTP/S Scan policy defines:
- whether to quarantine the message or not
- what action is to be taken if the mail is infected
- whether to block the message containing the specified file type
- whether sender, receiver and Administrator are to be notified or not
- Default Rules – As soon as you subscribe Gateway Anti Virus, default SMTP policy is applicable to all the inbound and outbound Email traffic. You can modify default policy to fit in your network requirement but cannot delete.

Manage SMTP/S Scanning Rules

To manage SMTP/S Scanning Rules, go to Anti Virus > Email > SMTP/S Scanning Rules.

<table>
<thead>
<tr>
<th>Screen Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Name</td>
<td>Displays the name of SMTP Scanning Rule.</td>
</tr>
<tr>
<td>Sender</td>
<td>Displays the username of the Sender.</td>
</tr>
<tr>
<td>Recipient</td>
<td>Displays the username of the Recipient.</td>
</tr>
<tr>
<td>Scanning</td>
<td>Displays whether SMTP scanning is Enabled or Disabled.</td>
</tr>
<tr>
<td>Quarantine (Not for CR15i models)</td>
<td>Displays whether Quarantine Enabled or Disabled.</td>
</tr>
<tr>
<td>Blocked File Type</td>
<td>Displays File Types that are blocked.</td>
</tr>
<tr>
<td>Receiver Action</td>
<td>Displays the specified Receiver Action for Infected, Suspicious and Protected Attachments.</td>
</tr>
<tr>
<td>Notify Admin</td>
<td>Displays Notification Message to Admin for Infected, Suspicious and Protected Attachments.</td>
</tr>
</tbody>
</table>

Table – Manage SMTP/S Scanning Rules screen elements
SMTP/S Scanning Rule Parameters

To add or edit an SMTP/S Scanning Rule(s), go to **Anti Virus > Email > SMTP/S Scanning Rules**. Click the Add Button to add a new rule or click Edit Icon to modify the details of the rule.

### Screen – Add SMTP/S Scanning Rule

<table>
<thead>
<tr>
<th>Screen Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Provide a name to identify the SMTP/S Scanning Rule.</td>
</tr>
<tr>
<td>Sender</td>
<td>Select the sender name from the list of users. Select “Any” if the rule is to be applied on all the senders.</td>
</tr>
<tr>
<td>Recipient</td>
<td>Select the recipient name from the list of users. Select “Any” if the rule is to be applied on all the recipients.</td>
</tr>
</tbody>
</table>

You can also add a new Email Address by clicking on the “Add Email Address” link.
You can also add a new Email address by clicking on the “Add Email Address” link.

**Scanning**

Specify whether the policy should be enabled for use or not.

If enabled, the policy will be used for virus scanning and blocking the attachments of specified file types.

**Action**

Enable the Action(s) to be taken on the Email(s), from the available options:

Available Options:
- Quarantine – If enabled, the mails are not delivered to the recipient, but are copied to the Quarantine file list. You can review mail sender/receiver details from the quarantined file list.

**Note**

Quarantine option is not available in Cyberoam CR15i models.

- Notify Sender – If enabled, sends a notification to the sender that the mail was infected. If enabled, the sender receives a notification about the infected mail.

**Block File Types**

Select file types to be blocked that are included in the attachment, to remove files that are a potential threat and to prevent virus attacks.

More than one file type can be selected using ctrl/shift keys.

The list of file types is preconfigured with a list of default file extensions. Refer to Default File Types to view the list of file extensions which will be blocked.

Selected Blocked file types will not be scanned.

Instead of creating individual policies to block the messages with different file types, you can simply create a single policy and select “ALL” in block file types to block messages with any type of file attachment.

Using Block File Types, you can also stop users from sending/receiving the messages with attachments.

Available Options:
- **All** – Select “ALL” in block file types to block messages with any type of file attachment.
- **None** – Select ‘None’ in block file types to allow messages with all types of file attachments.
- Messages can also be blocked if it includes the selected type of file attachments. The type of file attachments to be blocked can be selected from the list available on the Web Admin Console.

**Action When message is detected as Infected, Suspicious, or Protected Attachment**
### Receiver Action

Select the action to be taken on the message that is detected to be Infected, Suspicious or includes a Protected Attachment.

**Available Options:**
- **Don’t Deliver** – The Receiver will not receive the message and will also not receive notification(s) regarding the infected mail(s).
- **Remove and Deliver** – The Infected part of the mail is removed before delivering the mail. The Receiver will also receive a notification stating that the mail was infected and the infected portion from the mail is removed. Not applicable for Blocked Attachments (Block File Type).
- **Deliver Original** – Receiver receives the original mail and the notification along with the mail stating that mail was infected and not cured or removed.

**Note**
Appliance protected attachments are not scanned but the receiver will be notified if not specified otherwise.

### Notify Administrator

Select the action to notify the Administrator for the message detected to be Infected, Suspicious or includes a Protected Attachment.

**Available Options:**
- **Don’t Deliver** – Administrator will not be notified about the infected mail.
- **Send Original** – Receiver receives the original mail and the administrator receives the notification mail stating that mail was infected and was delivered without removing infection or is not quarantined.
- **Remove Attachment** – Recipient receives message without attachment and the Administrator receives the notification that the mail attachment was infected and removed before delivering mail.

**Note**
Appliance will not scan the protected attachment but receiver will be notified if not specified otherwise.

---

**Table – Add SMTP/S Scanning Rule screen elements**


**POP/IMAP Scanning Rules**

The Administrator can define policies to take appropriate action based on the protocols that is, define separate action rule on how to handle SMTP, POP3, FTP and HTTP traffic if infection is detected.

POP3 policy is applied to the POP3 traffic only that is,... When the message containing virus is detected, depending on POP3 policy, the Appliance deletes message from the POP3 server or simply sends the notification to the receiver stating that mail was not delivered because it was infected. POP3 configuration allows you to enable or disable the deletion of the infected message from the POP3 server.

IMAP policy is applied to the IMAP traffic only. When message containing virus is detected, the infected message is replaced with a message notifying the receiver that mail was not delivered because it was infected.

SMTP rule is not applicable to POP3 and IMAP traffic.

**Sample Message (send to the receiver)**

Subject: **VIRUS FOUND MAIL REJECTED**

Virus infected attachment(s) have been removed from this mail.
Virus Name(s): "Virus name list"
Attachment Name(s): "File names list" [From > sender name] [Date]
Address Group

Scanning rule is configured for the address. To make configuration easier and simpler, the Administrator can group the addresses that will be treated as same or require the same scanning policy rather than configuring individual rule for each address or adding individual addresses in each rule. The policy applied to the address group is applicable to all the group members. Hence, when a group is used in a number of rules, it becomes much easier to add or remove addresses from the group rather than updating an individual rule and just with the one update the Administrator can re-assign the rules.

Address Group is grouping of:
- Email Address or Domain
- IP Address
- RBL (Real time black hole List) (applicable only for spam mails)

An IP address can be a member of multiple groups.
RBL is a list of IP Addresses whose owners are responsible for spamming or hijacking for Spam Relay. These IP Addresses might also be used for spreading virus. The Appliance checks each RBL for the connecting IP Address and action configured in the policy is taken if IP Address is found in any of the RBL list. Administrator can directly use the two default RBL groups shipped with the Appliance or update them as per the requirement:
- Premium RBL Services
- Standard RBL Services

The Address Group page displays list of all the default and custom groups and provides option to add a new group, update the parameters, import addresses in the existing group, or delete the group. You can filter the list based on address group name.

Manage Address Groups

To manage Address Groups, go to **Anti Virus > Email > Address Group.**

<table>
<thead>
<tr>
<th>Screen Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays the name of the Address Group.</td>
</tr>
<tr>
<td>Type</td>
<td>Displays the type of Group: RBL, IP Address and Email Address/Domain.</td>
</tr>
<tr>
<td>Description</td>
<td>Displays Address Group Description.</td>
</tr>
<tr>
<td>Import Icon</td>
<td>Click <img src="link" alt="icon" /> to import the Address Groups.</td>
</tr>
</tbody>
</table>

**Table – Manage Address Groups screen elements**
Address Group Parameters

To add or edit an Address Group, go to Anti Virus > Email > Address Group. Click the Add button to add a new group or Edit Icon to modify the details.

Screen – Add Address Group

<table>
<thead>
<tr>
<th>Screen Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name to identify the Address Group.</td>
</tr>
<tr>
<td>Group Type</td>
<td>Select the Group Type.</td>
</tr>
</tbody>
</table>

**Available Options:**

- **RBL** – IP Addresses of certain owners that are suspected of spam proliferation or are hijacked for spam relay are included in an RBL list. The Appliance will check each RBL for the connecting IP Address. If the IP Address matches to the one on the list then the specified action in the policy is taken. Specify the Domain Name to be added as RBLs to the Address Group.

- **IP Address** – Specify IPv4 Address to be added to the Address Group.

- **Email Address/Domain** – Import or manually specify Email Address or Domain Name to be added to the Address Group.
  - **Import** – Select to browse and import a CSV file or a text file to add the Email Address/Domain to address group.
  - **Manual** – Select to manually add Email Address/Domain to address group.
Use the Add button to add value to the list and ✗ to delete value from the list.

| Description | Provide description for Address Group. |

**Table – Add Address Group screen elements**

**Importing Email Addresses/Domains into an existing Address Group**

Instead of adding addresses again in the Appliance, the address details can be directly uploaded in case you have them saved in the form of a file on your system. If the file has multiple addresses then each address must be on the new line. File with comma-separated address will on uploading, give an error.

![Add Address Group screen elements](image)

**Screen – Import Address Group**

Click the Import button under Manage column against the Address Group in which you want to import addresses. Use Browse to select CSV or text file.
HTTP/S

Use this Configuration to
- Define file size threshold
- Define HTTP Scanning Rule
- Delete HTTP Scanning Rule
- Update scanning order

Apart from mails, virus can also infect your network through HTTP downloads. Define HTTP Scanning Rules to protect you against this.

The Administrator can be configured for real time or batch mode scanning of HTTP traffic.

You can configure the maximum file size that can be buffered to the memory for scanning. This will also prevent the unintentional download of virus file hidden in the fragmented files.

Depending on the scanning policy set at the time of deployment through the Network Configuration Wizard, the Appliance will scan HTTP and HTTPS traffic. HTTP and HTTPS scanning can be enabled or disabled from the Firewall Rule section. By default, the Appliance will not scan HTTP traffic. HTTP scanning is to be enabled from the Firewall Rule section. You can also define the rule to bypass HTTP scanning of the traffic from a specific source and destination. If virus scanning is enabled and a virus is detected, the receiver will receive a notifying message. Similarly, you can define a rule to bypass HTTPS scanning based on the web and file type categories.

Sample message

Cyberoam Anti virus Alert

The URL you are trying to access has been blocked as it contains the virus 'Constructor.BAT.BVGHH.11'

URL : vx.netux.org/dl/vir/Constructor.BAT.BVGHH.11.zip?x=13&y=17

- Configuration
- HTTP Scanning Rules
- HTTPS Scanning Exceptions

Configuration

Use the Configuration page to configure general restrictions for scanning and restricting all the HTTP/HTTPS traffic.

To configure restrictions on HTTP traffic, go to Anti Virus > HTTP/S > Configuration.
### Screen – Configure Parameters

<table>
<thead>
<tr>
<th>Screen Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP / HTTPS Configurations</strong></td>
<td></td>
</tr>
<tr>
<td>Scan Mode</td>
<td>Specify the scanning mode. The Appliance can be configured for Real Time or Batch mode scanning of HTTP/S traffic. For Batch mode, virus scanning will only start after the complete file is downloaded. This may take some time in case the file size is large. To avoid this delay, configure scan in Real Time mode if you have to download bulky files.</td>
</tr>
<tr>
<td>File Size Threshold</td>
<td>Specify the File Size Threshold (in KB). Files that exceed this configured threshold will not be scanned. Acceptable range – 1 to 25600 KB Default – 1024 KB</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>For 15i Appliances Acceptable range – 1 – 4096 KB</td>
</tr>
<tr>
<td>Audio &amp; Video File Scanning</td>
<td>Enable Audio &amp; Video File Scanning for scanning of Audio/Video streams that are being downloaded. Default – Disabled</td>
</tr>
<tr>
<td><strong>HTTPS Configurations</strong></td>
<td></td>
</tr>
<tr>
<td>HTTPS Scanning CA</td>
<td>CyberoamSelfSignedC</td>
</tr>
<tr>
<td>Deny Unknown Protocol</td>
<td>Enable</td>
</tr>
<tr>
<td>Allow Invalid Certificate</td>
<td>Enable</td>
</tr>
</tbody>
</table>
| HTTPS Scanning CA | Select the type of HTTPS Scanning CA from the available options:  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Available Options:</strong></td>
</tr>
<tr>
<td></td>
<td>• Cyberoam_SSL_CA</td>
</tr>
<tr>
<td></td>
<td>• CyberoamSelfSignedCA</td>
</tr>
<tr>
<td></td>
<td>• List of custom CA’s if added</td>
</tr>
<tr>
<td></td>
<td>Default – Cyberoam_SSL_CA</td>
</tr>
<tr>
<td>Deny Unknown Protocol</td>
<td>Enable to deny traffic not following the HTTPS protocol. This can be categorized as invalid traffic through HTTPS port.</td>
</tr>
</tbody>
</table>
| Allow Invalid Certificate | If you enable HTTPS scanning, you need to import the Appliance SSL Proxy certificate in Internet Explorer, Mozilla Firefox or any other browsers for decryption on SSL Inspection otherwise the browser will always give a warning page when you try to access any secure site. An “Invalid Certificate error“ warning appears when the site is using an invalid SSL certificate. The Appliance blocks all such sites.  
|                   | Enable if you want to allow access to such sites.                |
HTTP Scanning Rules

The HTTP Scanning Rules page displays the list of all the scanning rules. It also provides options to add a new rule, update the parameters of the existing rules, or delete a rule.

To manage HTTP Scanning Rules, go to **Anti Virus → HTTP/S → HTTP Scanning Rules**.

<table>
<thead>
<tr>
<th>Screen – Manage HTTP Scanning Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Screen Elements</strong></td>
</tr>
<tr>
<td>Rule Name</td>
</tr>
<tr>
<td>Source IP Address</td>
</tr>
<tr>
<td>Destination IP Address</td>
</tr>
<tr>
<td>URL Regex</td>
</tr>
<tr>
<td>Action</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table – Manage HTTP Scanning Rules Screen elements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HTTP Scanning Rule Parameters</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Screen – Add HTTP Scanning Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Screen Elements</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Source IP Address</td>
</tr>
<tr>
<td>Destination IP Address</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>URL Regex</td>
</tr>
<tr>
<td>Action</td>
</tr>
</tbody>
</table>

**Table – Add HTTP Scanning Rule screen elements**
HTTPS Scanning Exceptions

The Appliance allows to bypass HTTPS scanning for specified web categories. The Administrator needs to create an exception rule and include all the web categories which are to be bypassed from HTTPS scanning.

To bypass HTTPS scanning for web and file type categories, go to Anti Virus > HTTP/S > HTTPS Scanning Exceptions.

---

**Screen – Manage HTTPS Scanning Exceptions**

<table>
<thead>
<tr>
<th>Screen Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Displays a name for the Rule.</td>
</tr>
<tr>
<td>Bypass</td>
<td>Displays the list of categories under the HTTPS Scanning Exception rule.</td>
</tr>
</tbody>
</table>

**Table – Manage HTTPS Scanning Exceptions Screen Elements**

You can edit any entity by clicking either the hyperlink or the Edit icon under the Manage column.

HTTPS Scanning Exceptions Rule Parameters

---

**Screen – Add HTTPS Scanning Exception**
<table>
<thead>
<tr>
<th>Screen Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Specify a name for the bypass rule.</td>
</tr>
<tr>
<td>Bypass</td>
<td>Select the web category to be bypassed for HTTPS scanning. Select the Add Web Category option to add a new Web Category. You can directly add a new web category from this page or from Web Filter &gt; Category &gt; Category.</td>
</tr>
</tbody>
</table>

Table – Add HTTPS Scanning Exceptions Screen Elements
FTP

The Administrator can define policies to take appropriate action(s) based on the protocols. Separate policy can be defined on how to handle SMTP, POP3, FTP, and HTTP traffic if infection is detected.

When the Appliance detects a virus and removes the infected file from an FTP download or from an Email message.

To configure FTP file size, go to **Anti Virus > FTP > FTP**.

```
Files Greater Than Size* | 1024 KB should not be scanned

Apply
```

**Screen – Configure FTP File Size**

You can configure the maximum file size (in KB) for scanning. The Emails greater than the specified size will not be scanned.

Acceptable Range - 1 to 20480 KB
Default – 1024 KB
Quarantine

Quarantine Digest is an Email that contains a list of quarantined messages filtered by the Appliance and held in the User Quarantine Area. If configured, the user receives Quarantine Digest as per the configured frequency. The Digest also provides a link to the User/My Account section from where user can access quarantined messages and take the required action.

Note

Quarantine option is not available for Cyberoam CR15i models.

View the list of Quarantined Mails

To view list of quarantined mails, go to **Anti Virus > Quarantine > Quarantine**

Use the “Filter Result” section to search for mails from the list of Quarantined Mails.

The Filter result displays a list of all the Quarantined Emails based on the filter criteria. The Administrator can release the quarantined mails to the recipient’s inbox by clicking Release icon against the mail.

Total Utilization displays percentage of Quarantine Area used by quarantined spam and virus infected messages. The Appliance reserves 5GB for Quarantine Area. Once the Quarantine Repository is full, older Emails are purged.

Screen – View Quarantine Mails

<table>
<thead>
<tr>
<th>Screen Elements</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter Result</td>
<td></td>
</tr>
<tr>
<td>Start Date</td>
<td>Select the starting date from Calendar by clicking on the icon.</td>
</tr>
<tr>
<td>End Date</td>
<td>Select the ending date from Calendar by clicking on the icon.</td>
</tr>
<tr>
<td>Sender</td>
<td>Specify a name for the Sender.</td>
</tr>
<tr>
<td>Receiver</td>
<td>Specify a name for the Receiver.</td>
</tr>
<tr>
<td>Subject</td>
<td>Specify a Subject.</td>
</tr>
<tr>
<td>Filter</td>
<td>Click “Filter” to filter.</td>
</tr>
<tr>
<td>Clear</td>
<td>Click “Clear” to reset the details of Filter Result.</td>
</tr>
<tr>
<td>Sender</td>
<td>Sender of the Mail.</td>
</tr>
<tr>
<td>Recipient</td>
<td>Recipient of the Mail</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Subject</td>
<td>Mail Subject</td>
</tr>
<tr>
<td>Time Stamp</td>
<td>Timestamp when the mail was received</td>
</tr>
</tbody>
</table>

Table – View Quarantine Mails screen elements

Releasing Quarantine Mails

Either the Administrator or an authorized User can release the quarantined mails. The Administrator can release the quarantined mails from the Quarantine Area while an authorized user can release from his My Account. Released quarantined mails are delivered to the intended recipient’s inbox.

The Administrator can access Quarantine Area from **Anti Spam > Quarantine > Quarantine Area**, while user can logon to My Account and access Quarantine Area from Quarantine Mails > Spam > Quarantine Emails.

If Quarantine Digest is configured, user will receive Digest of the quarantined mails as per the configured frequency.