



Radius Integration Guide Version 9

Document version 9402 -1.0-18/10/2006

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 the performance thereof is under warranty provided by Kaspersky Labs. 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

Copyright 2000 Elitecore Technologies Ltd. All rights reserved. Cyberoam, Cyberoam logo are trademark of Elitecore Technologies Ltd. Information supplies by Elitecore Technologies Ltd. Is believed to be accurate and reliable at the time of printing, but Elitecore Technologies assumes no responsibility for any errors that may appear in this documents. Elitecore Technologies reserves the right, without notice, to make changes in product design or specifications. Information is subject to change without notice

CORPORATE HEADQUARTERS

Elitecore Technologies Ltd.
904 Silicon Tower,
Off. C.G. Road,
Ahmedabad – 380015, INDIA
Phone: +91-79-26405600
Fax: +91-79-26407640
Web site: www.elitecore.com , www.cyberoam.com

Guide Sets

Guide	Describes
User Guide	
Console Guide	Console Management
Windows Client Guide	Installation & configuration of Cyberoam Windows Client
Linux Client Guide	Installation & configuration of Cyberoam Linux Client
HTTP Client Guide	Installation & configuration of Cyberoam HTTP Client
Analytical Tool Guide	Using the Analytical tool for diagnosing and troubleshooting common problems
LDAP Integration Guide	Configuration for integrating LDAP with Cyberoam for external authentication
ADS Integration Guide	Configuration for integrating ADS with Cyberoam for external authentication
PDC Integration Guide	Configuration for integrating PDC with Cyberoam for authentication
RADIUS Integration Guide	Configuration for integrating RADIUS with Cyberoam for external authentication
High Availability Configuration Guide	Configuration of High Availability (HA)
Data transfer Management Guide	Configuration and Management of user based data transfer policy
Multi Link Manager User Guide	Configuration of Multiple Gateways, load balancing and failover
VPN Management	Implementing and managing VPN
Cyberoam IDP Implementation Guide	Configuring, implementing and managing Intrusion Detection and Prevention
Cyberoam Anti Virus Implementation Guide	Configuring and implementing anti virus solution
Cyberoam Anti Spam Implementation Guide	Configuring and implementing anti spam solution

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: +91-79-26405600
Fax: +91-79-26407640
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

Overview

Welcome to the Cyberoam's - RADIUS Integration Guide.

Cyberoam is an Identity-based UTM Appliance. Cyberoam's solution is purpose-built to meet the security needs of corporates, government organizations, and educational institutions.

Cyberoam's perfect blend of best-of-breed solutions includes User based Firewall, Content filtering, Anti Virus, Anti Spam, Intrusion Detection and Prevention (IDP), and VPN.

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.

Once you have installed and placed Cyberoam, you can monitor user activity in your Network based on the default policy.

As Cyberoam monitors and logs user activity based on IP address, all the reports are generated based on IP address. To monitor and log user activities based on User names or logon names, you have to configure Cyberoam for integrating user information and authentication process. Integration will identify access request based on User names and generate reports based on Usernames.

When the user attempts to access, Cyberoam requests a user name and password and authenticates the user's credentials before giving access. User level authentication can be performed using the local user database on the Cyberoam, an External ADS server, Windows Domain Controller, RADIUS, or LDAP server.

To set up user database

1. Integrate ADS, Domain Controller, RADIUS or LDAP if external authentication is required.

If your Network uses Active Directory Services, configure Cyberoam to communicate your ADS. Refer to ADS Integration Guide for more details.

If your Network uses Windows Domain Controller, configure for Cyberoam to communicate with Windows Domain Controller. Refer to PDC Integration Guide for more details.

If your Network uses LDAP, configure for Cyberoam to communicate with LDAP server. Refer to LDAP Integration Guide for more details.

If your Network uses RADIUS server, configure for Cyberoam to communicate with RADIUS server. Refer to RADIUS Integration Guide for more details.

2. Configure for local authentication.

3. Register user

RADIUS server

RADIUS stands for Remote Authentication Dial In User Service and is a protocol for allowing network devices to authenticate users against a central database. In addition to user information, RADIUS can store technical information used by network devices such as protocols supported, IP addresses, telephone numbers, routing information, and so on. Together this information constitutes a user profile that is stored in a file or database on the RADIUS server.

RADIUS servers provide authentication, authorization, and accounting functions but Cyberoam uses only the authentication function of the RADIUS server.

Configuring Cyberoam to use RADIUS server

Before you can use RADIUS authentication, you must have a functioning RADIUS server on the network.

Select **User** → **Authentication Settings** to open configuration page

Screen – RADIUS Integration

Screen Elements	Description
Configure Authentication & Integration parameters	
Integrate with	Select RADIUS as an authentication server If the user does not exist in Cyberoam but is already in RADIUS, Cyberoam automatically adds users into the default group on first logon.
Default Group	Allows to select default group for all users Click <i>Default Group</i> list to select
Update button	Updates and saves the configuration
Add button	Allows to add RADIUS server details Refer Add RADIUS Server for details

Table – RADIUS Integration screen elements

Add RADIUS Server

RADIUS Server Details

Radius Server Configuration

Server Name*	<input type="text"/>
Server Ip*	<input type="text"/>
Authentication Port*	<input type="text" value="1812"/>
Shared Secret*	<input type="text"/>
Integration Type*	<input type="radio"/> Loose integration with cyberoam <input checked="" type="radio"/> Tight integration with cyberoam
Group Name Attribute *	<input type="text"/>

Screen – RADIUS Server configuration

Screen Elements	Description
RADIUS Server Configuration	
Server Name	Specify name of the RADIUS Server
Server IP	Specify RADIUS Server IP Address
Port	Specify Port number over which RADIUS Server communicates Default port is 1812
Shared Secret	Specify shared secret, which is to be used to encrypt information passed to Cyberoam
Integration Type	Integration type is used in setting the user group membership Select Tight integration with cyberoam if want to use vendor specific attribute for setting the user group membership and specify Group name attribute
Test Connection button	Allows to check the connectivity of Cyberoam with RADIUS server Click to check
Add button	Saves the server configuration
Cancel button	Cancels the current operation

Table – RADIUS Server configuration screen elements

Server Connectivity check

Connection to RADIUS is enabled automatically during setup, but as RADIUS server is used for authenticating users it is necessary to check whether Cyberoam is able to connect to RADIUS or not.

Connectivity can be checked:

1. At the time of adding RADIUS server details

Refer to Add RADIUS server for details on checking connectivity at the time of adding RADIUS server details.

2. After adding RADIUS server details

Select **User → Authentication Settings** and click RADIUS Server IP, which is to be tested for connection. Click Test Connection button.