Integrity SecureClient Mobile

For additional technical information about Check Point products, consult Check Point's SecureKnowledge at:

https://secureknowledge.checkpoint.com

View the latest version of this document in the User Center at:

http://www.checkpoint.com/support/technical/documents/

Intelligent Security

August 2006

We Secure the Internet.

© 2003-2005 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

©2003-2005 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Application Intelligence, Check Point Express, the Check Point logo, AlertAdvisor, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia, Eventia Analyzer, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureXL Turbocard, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, and the Zone Labs logo, are trademarks or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726, 6,496,935 and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

THIRD PARTIES:

Entrust is a registered trademark of Entrust Technologies, Inc. in the United States and other countries. Entrust's logos and Entrust product and service names are also trademarks of Entrust Technologies, Inc. Entrust Technologies Limited is a wholly owned subsidiary of Entrust Technologies, Inc. FireWall-1 and SecuRemote incorporate certificate management technology from Entrust.

Verisign is a trademark of Verisign Inc.

The following statements refer to those portions of the software copyrighted by University of Michigan. Portions of the software copyright © 1992-1996 Regents of the University of Michigan. All rights reserved. Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided "as is" without express or implied warranty. Copyright © Sax Software (terminal emulation only).

The following statements refer to those portions of the software copyrighted by Carnegie Mellon University.

Copyright 1997 by Carnegie Mellon University. All Rights Reserved.

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The following statements refer to those portions of the software copyrighted by The Open Group.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE OPEN GROUP BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

The following statements refer to those portions of the software copyrighted by The OpenSSL Project. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following statements refer to those portions of the software copyrighted by Eric Young. THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. Copyright © **1998** The Open Group.

The following statements refer to those portions of the software copyrighted by Jean-loup Gailly and Mark Adler Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler. This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

The following statements refer to those portions of the software copyrighted by the Gnu Public License. This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version. This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

The following statements refer to those portions of the software copyrighted by Thai Open Source Software Center Ltd and Clark Cooper Copyright (c) 2001, 2002 Expat maintainers. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

GDChart is free for use in your applications and for chart generation. YOU MAY NOT re-distribute or represent the code as your own. Any re-distributions of the code MUST reference the author, and include any and all original documentation. Copyright. Bruce Verderaime. 1998, 1999, 2000, 2001. Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health. Portions copyright 1996, 1997, 1998, 1999, 2000, 2001, 2002 by Boutell.Com, Inc. Portions relating to GD2 format copyright 1999,

Check Point Software Technologies Ltd.

U.S. Headquarters: 800 Bridge Parkway, Redwood City, CA 94065, Tel: (650) 628-2000 Fax: (650) 654-4233, info@CheckPoint.com

International Headquarters: 3A Jabotinsky Street, Ramat Gan, 52520, Israel, Tel: 972-3-753 4555 Fax: 972-3-575 9256, http://www.checkpoint.com

2000, 2001, 2002 Philip Warner. Portions relating to PNG copyright 1999, 2000, 2001, 2002 Greg Roelofs. Portions relating to gdttf.c copyright 1999, 2000, 2001, 2002 John Ellson (ellson@graphviz.org). Portions relating to gdft.c copyright 2001, 2002 John Ellson (ellson@graphviz.org). Portions relating to JPEG and to color quantization copyright 2000, 2001, 2002, Doug Becker and copyright (C) 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001, 2002, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group. See the file README-JPEG.TXT for more information. Portions relating to WBMP copyright 2000, 2001, 2002 Maurice Szmurlo and Johan Van den Brande. Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation. This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived works" includes all programs that utilize the library. Credit must be given in user-accessible documentation. This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation. Although their code does not appear in gd 2.0.4, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

The curl license

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2004, Daniel Stenberg, <daniel@haxx.se>.All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose

with or without fee is hereby granted, provided that the above copyright

notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

The PHP License, version 3.0

Copyright (c) 1999 - 2004 The PHP Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.

4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"

5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes PHP, freely available from <http://www.php.net/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the PHP Group. The PHP Group can be contacted via Email at group@php.net.

For more information on the PHP Group and the PHP project, please see <http://www.php.net>. This product includes the Zend Engine, freely available at <http://www.zend.com>.

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Copyright (c) 2003, Itai Tzur <itzur@actcom.co.il>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistribution of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Neither the name of Itai Tzur nor the names of other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Copyright © 2003, 2004 NextHop Technologies, Inc. All rights reserved.

Confidential Copyright Notice

Except as stated herein, none of the material provided as a part of this document may be copied, reproduced, distrib-uted, republished, downloaded, displayed, posted or transmitted in any form or by any means, including, but not lim-ited to, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of NextHop Technologies, Inc. Permission is granted to display, copy, distribute and download the materials in this doc-ument for personal, non-commercial use only, provided you do not modify the materials and that you retain all copy-right and other proprietary notices contained in the materials unless otherwise stated. No material contained in this document may be "mirrored" on any server without written permission of NextHop. Any unauthorized use of any material contained in this document may violate copyright laws, trademark laws, the laws of privacy and publicity, and communications regulations and statutes. Permission terminates automatically if any of these terms or condi-tions are breached. Upon termination, any downloaded and printed materials must be immediately destroyed.

Trademark Notice

The trademarks, service marks, and logos (the "Trademarks") used and displayed in this document are registered and unregistered Trademarks of NextHop in the US and/or other countries. The names of actual companies and products mentioned herein may be Trademarks of their respective owners. Nothing in this document should be construed as granting, by implication, estoppel, or otherwise, any license or right to use any Trademark displayed in the document. The owners aggressively enforce their intellectual property rights to the fullest extent of the law. The Trademarks may not be used in any way, including in advertising or publicity pertaining to distribution of, or access to, materials in this document, including use, without prior, written permission. Use of Trademarks as a "hot" link to any website is prohibited unless establishment of such a link is approved in advance in writing. Any questions concerning the use of these Trademarks should be referred to NextHop at U.S. +1 734 222 1600.

U.S. Government Restricted Rights

The material in document is provided with "RESTRICTED RIGHTS." Software and accompanying documentation are provided to the U.S. government ("Government") in a transaction subject to the Federal Acquisition Regulations with Restricted Rights. The Government's rights to use, modify, reproduce, release, perform, display or disclose are restricted by paragraph (b)(3) of the Rights in Noncommercial Computer Software and Noncommercial Computer Soft-ware Documentation clause at DFAR 252.227-7014 (Jun 1995), and the other restrictions and terms in paragraph (g)(3)(i) of Rights in Data-General clause at FAR 52.227-14, Alternative III (Jun 87) and paragraph (c)(2) of the Commer-cial

Computer Software-Restricted Rights clause at FAR 52.227-19 (Jun 1987).

Use of the material in this document by the Government constitutes acknowledgment of NextHop's proprietary rights in them, or that of the original creator. The Contractor/ Licensor is NextHop located at 1911 Landings Drive, Mountain View, California 94043. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in applicable laws and regulations.

Disclaimer Warranty Disclaimer Warranty Disclaimer Warranty Disclaimer Warranty

THE MATERIAL IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTIES OF ANY KIND EITHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT POSSIBLE PURSUANT TO THE APPLICABLE LAW, NEXTHOP DISCLAIMS ALL WARRAN-TIES,

EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON INFRINGEMENT OR OTHER VIOLATION OF RIGHTS. NEITHER NEXTHOP NOR ANY OTHER PROVIDER OR DEVELOPER OF MATERIAL CONTAINED IN THIS DOCUMENT WARRANTS OR MAKES ANY REPRESEN-TATIONS REGARDING THE USE, VALIDITY, ACCURACY, OR RELIABILITY OF, OR THE RESULTS OF THE USE OF, OR OTHER-WISE RESPECTING, THE MATERIAL IN THIS DOCUMENT.

Limitation of Liability

UNDER NO CIRCUMSTANCES SHALL NEXTHOP BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSE-QUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOSS OF DATA OR PROFIT, ARISING OUT OF THE USE, OR THE

INABILITY TO USE, THE MATERIAL IN THIS DOCUMENT, EVEN IF NEXTHOP OR A NEXTHOP AUTHORIZED REPRESENTATIVE HAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IF YOUR USE OF MATERIAL FROM THIS DOCUMENT RESULTS IN

THE NEED FOR SERVICING, REPAIR OR CORRECTION OF EQUIPMENT OR DATA, YOU ASSUME ANY COSTS THEREOF. SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE

ABOVE LIMITATION OR EXCLUSION MAY NOT FULLY APPLY TO YOU.

Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

BIND: ISC Bind (Copyright (c) 2004 by Internet Systems Consortium, Inc. ("ISC"))

Copyright 1997-2001, Theo de Raadt: the OpenBSD 2.9 Release

Table of Contents

CHAPTER 1

Introduction

In This Chapter

Overview of Integrity SecureClient Mobile

Integrity SecureClient Mobile is a client for mobile devices that includes a VPN and a firewall. It replaces SecureClient for PocketPCs. The client works on various platforms and enables easy deployment and upgrade.

Integrity SecureClient Mobile's VPN is based on SSL (HTTPS) tunneling and enables handheld devices to securely access resources behind Check Point gateways.

Integrity SecureClient Mobile has the following two modes of operation:

- **Centrally Managed Mode**: The client connects to a gateway (module) configured for Integrity SecureClient Mobile and downloads a set of policies that were sent to the gateway from the SmartCenter server. The client then enforces th policies. For this mode to work, the gateway and the SmartCenter server must be upgraded to support the client. The upgrade is a patch that can be installed over R60 HF2 on both the gateway and the SmartCenter server. On the gateway, the patch adds support for the new protocol and policy. On the server, the patch extends the schema (database) with relevant additions.
- **SSL Network Extender Mode**: The client connects to a gateway configured only for SSL Network Extender. In this mode, the client does not download policies, but enforces a set of policies predefined upon client installation (for additional

information, refer to “Client Deployment” on page 43). The client works with any gateway configured for SSL Network Extender Network mode (available on Checkpoint VPN-1 Pro R55 HF8 versions and above, and on Connectra 1.0 versions and above). This is a backward compatibility mode that enables the running of a subset of the client features without upgrading the corporate infrastructure. For additional information on how to configure SSL Network Extender mode on a Check Point VPN-1 Pro gateway, refer to the *VPN User Guide*. For additional information on how to configure SSL Network Extender mode on a Connectra gateway, refer to the *Connectra Web Security Gateway* guide.

Integrity SecureClient Mobile is supported on the Windows Mobile 2003/SE/5.0 operating system.

Connectivity Features

When users access their organization from remote locations, it is essential that not only are the normal requirements of secure connectivity met, but also the following requirements of remote clients:

- **Connectivity**: The remote client must be able to access the organization from various locations, even if it is behind a NATing device, proxy or firewall. The range of applications available must include web, mail and file share applications, in addition to other more specialized applications required by the corporation.
- **Session Continuation**: Once authenticated, remote users begin a session. The session provides the context for which all requests are processed until the user logs out (disconnects), or the session ends due to a timeout. If the client's VPN tunnel is dropped due to various networking conditions, the client uses its session to reconnect the VPN tunnel without disturbing the overall user experience.
- **Secure Connectivity**: Secure connectivity is guaranteed by the combination of authentication, confidentiality and data integrity procedures employed for every connection.
- **Usability**: Seamless solutions for the connecting user.

Temporary Loss of IP

When an IP address is temporarily lost, Integrity SecureClient Mobile automatically reconnects to the gateway without user intervention. For example, this occurs if a user goes through a tunnel or enters an elevator.

Interface and IP Change

If there is a change to the interface or the IP address, Integrity SecureClient Mobile does not lose its connection to the gateway. This occurs, for example, if a user is connected using Wi-Fi and then switches to GPRS.

Automatic Connect

Integrity SecureClient Mobile can be configured to automatically connect to the last gateway to which it was connected when any of the following conditions are met:

- The device has a valid IP address.
- The device exits standby mode or after a softreset.
- After the condition that caused the device to automatically disconnect ceases to exist (for example, allow clear traffic during ActiveSync Disconnect when idle)

Configure this feature using the `neo_always_connected_retry` property found in TABLE 3-1 on page 33.

Authentication Schemes

There are three ways to authenticate the user and the connection device:

- Machine Certificates (PKCS#12)
- One Time Password (for example, RSA SecureID)
- User/Password combinations

A connectivity policy downloaded to the device enables the administrator to define the amount of user interaction required to carry out the authentication process.

Integrity SecureClient Mobile can be configured to save a user's credentials (password), which are used for authenticating with the gateway. As long as the password is cached, the user is not prompted to re-enter it when the client connects or re-authenticates.

Warning - When this feature is enabled, the password is stored locally on the PDA. This poses a security threat because the password can be retrieved if the PDA is lost, stolen or hacked.

Integrity SecureClient supports a secure authentication (SAA) OPSEC interface that allows third party-extensions to the standard authentication schemes.

For additional configuration information, refer to "Authentication Schemes" on page 26.

Initiate Dialup

Integrity SecureClient Mobile can be configured to initiate a dialup connection (for example, GPRS) for users with no valid IP address, if a dialup connection is configured on the device.

Configure this feature using the `neo_initiate_dialup` property found in TABLE 3-1 on page 33.

Re-authenticate Users

Depending on the user's authentication settings, the user may be prompted for authentication credentials five minutes before session timeout nce these credentials are accepted, the timeout interval is initialized. If the user does not provide credentials before the timeout begins, the user is disconnected from the server and must reconnect to the client manually.

Gateway History

Integrity SecureClient Mobile retains the details of the gateway to which it was previously connected. This enables users to more readily access the gateway without having to re-enter the gateway's information.

Allow Clear Traffic During ActiveSync and When Disconnected

Corporate users, who use Integrity SecureClient Mobile to access their corporate network from home or from the road with their mobile devices, may also wish to use Integrity SecureClient Mobile in the office where traffic encryption is not necessary.

Integrity SecureClient Mobile can be configured to allow clear traffic while in ActiveS (the PDA is “cradled” to the PC, which serves as a NAT device for the PDA to access the network).

Traffic may also need to be sent unencrypted ("in the clear") when the mobile device is located in a private network inside the encryption domain. For example, when a Wi-Fi base station is located inside the corporate network.

Topology Concepts

A topology is the collection of enabled VPN links in a system of gateways, their VPN domains, hosts located behind each gateway, and the remote clients external to each gateway.

Remote Access VPN

Remote access VPN refers to remote users accessing the network with client software, such as SecuRemote/SecureClient, SSL clients or third party IPSec clients. The VPN-1 gateway provides a *Remote Access Service* for remote clients.

Remote Access Community

A remote access community is a type of community created specifically for users that normally work from remote locations outside the corporate LAN.

Office Mode

Office mode enables a VPN-1 Pro gateway to assign an IP address to a remote client. This IP address is only used internally for secure encapsulated communication with the home network and is not visible in the public network. The IP address assignment takes place once the user connects and authenticates. The assignment lease is renewed so long as the user is connected. The address may be selected either from a general IP address pool, or from an IP address pool specified by the user group using a configuration file. This mode enables connections from within the corporate network to the remote access device and client-to-client connectivity (for example, P2P and VOIP protocols, back connections, and “push” technologies).

Visitor Mode (SSL Tunnel)

Visitor mode enables the tunneling of all client-to-gateway communication through a SSL/TLS connection on port 443. Visitor mode is designed to traverse firewalls and proxy servers.

Hub Mode (VPN Routing for Remote Access)

VPN routing for remote access clients is enabled through hub mode. In this mode, all traffic is directed through the connected gateway. The central hub acts as a router for the remote client. When traffic from remote access clients is directed through a hub, subsequent traffic can be filtered.

Security Policies

Integrity SecureClient Mobile has a built in IP firewall, which supports predefined security policies that are centrally managed. When a Integrity SecureClient Mobile user connects to the organization's gateway to establish a VPN, one of the following policies is downloaded to the device and enforced:

- **Allow All**: No policy is enforced, enabling all traffic to pass successfully.

- **Allow Outgoing and Encrypted**: All outbound connections are permitted and all inbound connections are permitted provided that they come from the encryption domain and pass through a VPN tunnel. This is the recommended setting.
- **Allow Outgoing Only**: All outbound connections are permitted and all inbound connections are blocked.
- **Allow Encrypted Only**: All connections are permitted provided that they originated from or are destined to the encryption domain and the connection passes through a VPN tunnel.

The type of policy enforced for Integrity SecureClient Mobile users can be defined by the administrator, or each user (if permitted by the administrator).

The administrator can also define a policy to allow/disallow ActiveSync (device to PC sync) communications.

Packaging

Integrity SecureClient Mobile comes packaged as self-installing CAB and MSI files. The CAB installation can be customized before it is distributed to users to include predefined topology, settings, and credentials, and a default firewall policy. During version upgrades, the installer preserves the existing client policies and credentials that are not predefined in the upgrade package. The administrator can enforce client upgrades using the `neo_upgrade_mode`, `neo_upgrade_version`, and `neo_upgrade_url` flags.

When the client is installed on the mobile device, another applet called Certificate Import Wizard is also installed. This applet enables the importing of PKCS#12 certificates to the device.

CHAPTER 2

Installation

This chapter describes how to install the Mobile Security SecureClient in an VPN-1 Pro environment.

In This Chapter

Integrity SecureClient Mobile Gateway Side Installation

Integrity SecureClient Mobile (ISCM) can be installed on individual gateways. For central management of these gateways, ISCM support can be installed on the SmartCenter server.

An Integrity SecureClient Mobile user can connect to a gateway that does not have ISCM support installed, or to a gateway with ISCM support installed but not enabled, through the SSL Network Extender settings.

Module Support

There are two methods for installing Integrity SecureClient Mobile (ISCM) support on gateways:

- R60 HFA_02
- R60 HFA_04 or later

In order to centrally manage the gateways, a management patch should be installed on the SmartCenter server, although this is not mandatory. If ISCM support is only installed on the gateways, then configuration must be applied to each gateway individually.

SmartCenter Server Support

To centrally manage the individual gateways, first install R60 HFA_02 with the management patch.

Downloading HFAs

If R60 HFA_02 is already installed, install the appropriate patch(es). If you do not have an HFA installed, download the R60 HFA_04 at:

http://www.checkpoint.com/downloads/latest/hfa.html

Before installing the management or gateway patch, first install R60 HFA_02.

Management Patch

To download the management patch:

1 At the command prompt on the SmartCenter server, type:
`fw1_HOTFIX_DAL_HF_HA02_151_591151NNN_NN`

2 When prompted, type **y** to continue with the installation.

3 After the installation is complete, reboot the machine.

4 At the command prompt on the SmartCenter server, run the following commands:

```
cpstop

cpdb scheme_adjust

cpstart
```

5 Select **Install policy.**

Gateway Patch

This patch is required only for R60 HFA_02.

To download the gateway patch (for each gateway):

1 At the command prompt, type:
`fw1_HOTFIX_DAL_HF_HA02_129_591129NNN_N`

2 When prompted, type **y** to continue with the installation.

3 After the installation is complete, reboot the machine.

Hardware and Software Requirements

Operating System

- Windows Mobile 2003/SE (Pocket PC Configuration)
- Windows Mobile 5.0 (Pocket PC Configuration)

Processor

- Intel ARM/StrongARM/XScale/PXA Series Processor family
- Texas Instrument OMAP Processor family

Client Side Installation

There are two ways to install Integrity SecureClient Mobile:

- Self-installing CAB Package: This file is installed directly on the mobile device.
- Self-installing MSI Package: This file is installed on the user's personal computer. During installation, the installer extracts a CAB file package from within the MSI package and installs it on a connected mobile device using ActiveSync services.

CAB Package

The `.cab` file is provided by the administrator and may be stored anywhere on the mobile device or an attached storage card. The installation can be automated using configuration tools such as Over The Air (OTA).

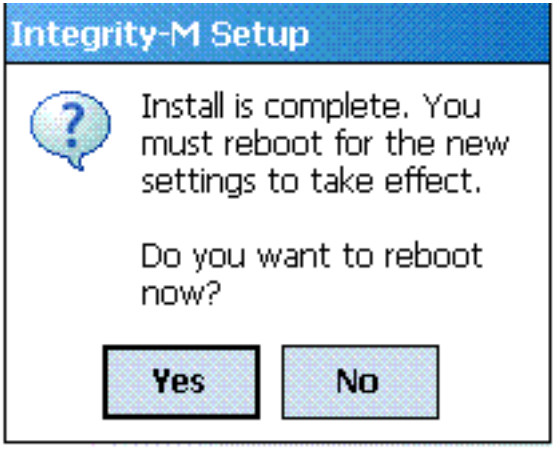
Installation

To install the CAB package:

1 From the **File Explorer** window, select the `.cab` file.

2 Mobile 5.0 users are prompted to select an installation location. Select **Device**, and then tap **Install**.

The **Integrity-M Setup** window opens.



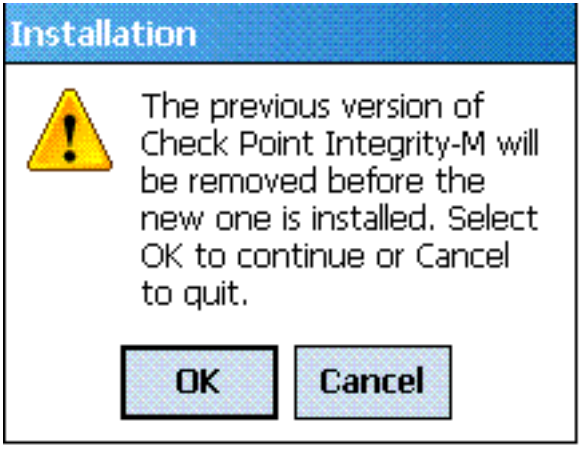
3 Tap **Yes** to reboot.

Upgrade

To upgrade the CAB package:

1 From the **File Explorer** window, select the `.cab` file.

The **Installation** window opens .



2 Tap **OK** to install the new version. Existing configuration settings are not lost during upgrade, they are transferred to the new version.

3 Mobile 5.0 users are prompted to select an installation location. Select **Device**, and then tap **Install**.

4 Tap **OK** to reboot.

Uninstall

To uninstall the CAB package:

1 Select **Start > Settings > System Tab > Remove Programs**.

2 Highlight **Check Point Integrity-M**, and then tap **Remove**.

MSI Package

The `.msi` file package is provided by the administrator and may be stored anywhere on the PC. The installation can be automated using tools such as Microsoft SMS Server.

Installation

To install the MSI package:

1 Run the `.msi` file provided by your administrator.

2 Follow the instructions in the wizard to complete the installation. During installation, the ActiveSync service prompts users to install the software on its device.

Upgrade

To upgrade the MSI package:

1 Run the `.msi` file provided by your administrator.

2 Follow the instructions in the wizard to complete the installation. During installation, the ActiveSync service prompts users to install the software on its device.

3 Click **OK** to install the new version. Existing configuration settings are not lost during upgrade, but transferred to the new version.

Uninstall

To uninstall the MSI package:

1 Click **Start > Settings > Control Panel > Add Remove Programs**.

2 Highlight **Integrity SecureClient Mobile**, and then click **Remove**.

3 Follow the instructions in the wizard to complete the uninstallation. If you want to remove the client from the device, see “Uninstall” on page 19 to follow the CAB Package uninstall procedure.

CHAPTER 3

Configuration

In This Chapter

Overview

In order for Integrity SecureClient Mobile clients to work in centrally managed mode, the following configuration is required:

- Configure a remote access community.
- Define a topology for remote access.
- Set global properties for Integrity SecureClient Mobile (neo properties).
- Establish connectivity settings.
- Define a security policy.

- Enable and configure support for Integrity SecureClient Mobile on each gateway that offers client connectivity.
- Enable load sharing and high availability features.

When an Integrity SecureClient Mobile gateway and an enabled SSL Network Extender property are configured with different settings, the SSL Network Extender settings are applied.

Configuring a Gateway to Support Integrity SecureClient Mobile

There are two ways to configure a gateway to enabl ISCM support:

1 **Enabling the `neo_enable` property**: This method is available only if a management patch is installed. This property is enabled on the SmartCenter server using GuiDBedit. Set this property to **true** to enable and **false** to disable support.

This property should be set on the SmartCenter server only after all patches have been installed.

To enable support using GuiDBedit:

a Go to **Network Object > network_objects**.

b Select a gateway and search for the `ssl_ne` set within the VPN set. If the `ssl_ne` properties (such as `neo_enable` and `ssl_enable`) are not displayed, set the value of `ssl_ne` to `ssl_network_extender`. These properties are then displayed.

c Within the set, change the value of `neo_enable` to **true**.

d Save the changes to install the policy.

2 **Adding a registry key**: This method must be performed on each gateway.

To enable support, run: `ckp_regedit -a SOFTWARE\\CheckPoint\\VPN1 neo_enable 1`.

Support starts once `cpstop` and `cpstart` are run.

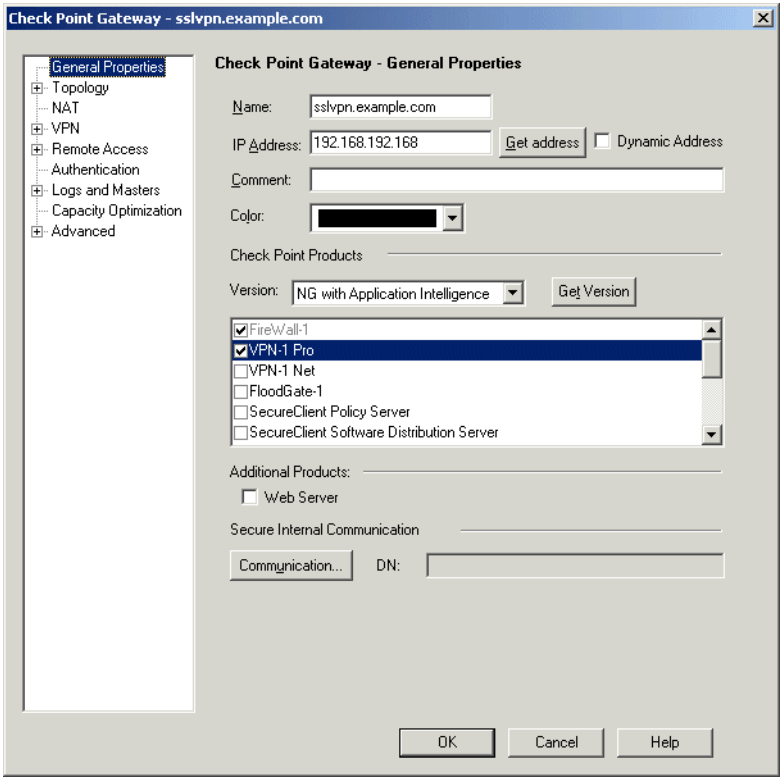
1 To disable support, run: `ckp_regedit -d SOFTWARE\\CheckPoint\\VPN1 neo_enable`.

Configuring the Gateway as a Member of a Remote Access Community

To configure a gateway as a member of a remo

1 On **SmartDashboard**, select the **Gateway Object** from the **Network Object** tab of the **Objects Tree**. The **General Properties** window opens.

FIGURE 3-1 General Properties Window



2 Verify that **VPN** is selected.

3 Select **VPN** from the menu on the left.

4 Verify that the gateway participates in the remote access community. If not, add the gateway to the remote access community.

5 From the **Gateway Properties** page, in the **Topology** tab, configure the VPN domain for Integrity SecureClient Mobile in the same way that it was configured for SecureClient.

Note - The VPN domain can be used to configure Integrity SecureClient Mobile to work in hub mode, where all traffic is directed through a central hub.

The "Set domain for Remote Access Community ..." button on the **Topology** tab can also be used to create a different encryption domain for remote access clients that connect to the gateway.

6 Configure visitor mode, as described in the *Resolving Connectivity Issues* chapter in the *VPN Guide*. Configuring visitor mode does not interfere with regular SecureClient user functionality, but permits SecureClient users to enable visitor mode.

Note - The Integrity SecureClient Mobile uses TCP 443 (SSL) to establish a secure connection with the VPN SecurePlatform and the Nokia platform, and for remote administration purposes. Another port may be assigned to the Integrity SecureClient Mobile, however, this is not recommended, as most proxies do not allow ports other than 80 and 443. Instead, it is recommended that you assign SecurePlatform, or the Nokia platform web user interface, to a port other than 443.

7 On SecurePlatform, perform one of the following procedures:

To change the webui port, run: `webui enable <port number>`. (For example, `webui enable 444`.)

To disable the webui port, run: `webui disable`.

8 To change a Voyager port on a Nokia platform, run:

`voyager –e x –S <port number>` (x represents the encryption level).

For more information, run: `voyager –h`

9 Select **Remote Access > Office Mode**.

10 Configure office mode, as described in the *Office Mode* chapter of the *VPN Guide*.

Note - Office mode support is mandatory on the gateway side.

11 Configure users and authentication.

Load Sharing Cluster Support

Integrity SecureClient Mobile provides load sharing cluster support.

To enable load sharing cluster support:

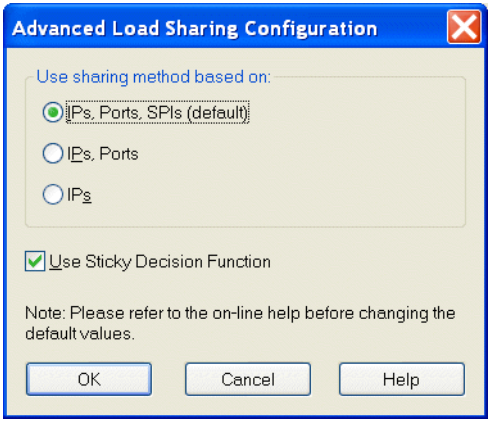
1 Double-click the **Gateway Cluster Object** from the **Network Object** tab of the **Objects Tree.** The **Gateway Cluster Properties** window opens.

Note - A load sharing cluster must be created before you can configure the sticky decision function.

2 Select **Cluster XL**. The **Cluster XL** tab opens.

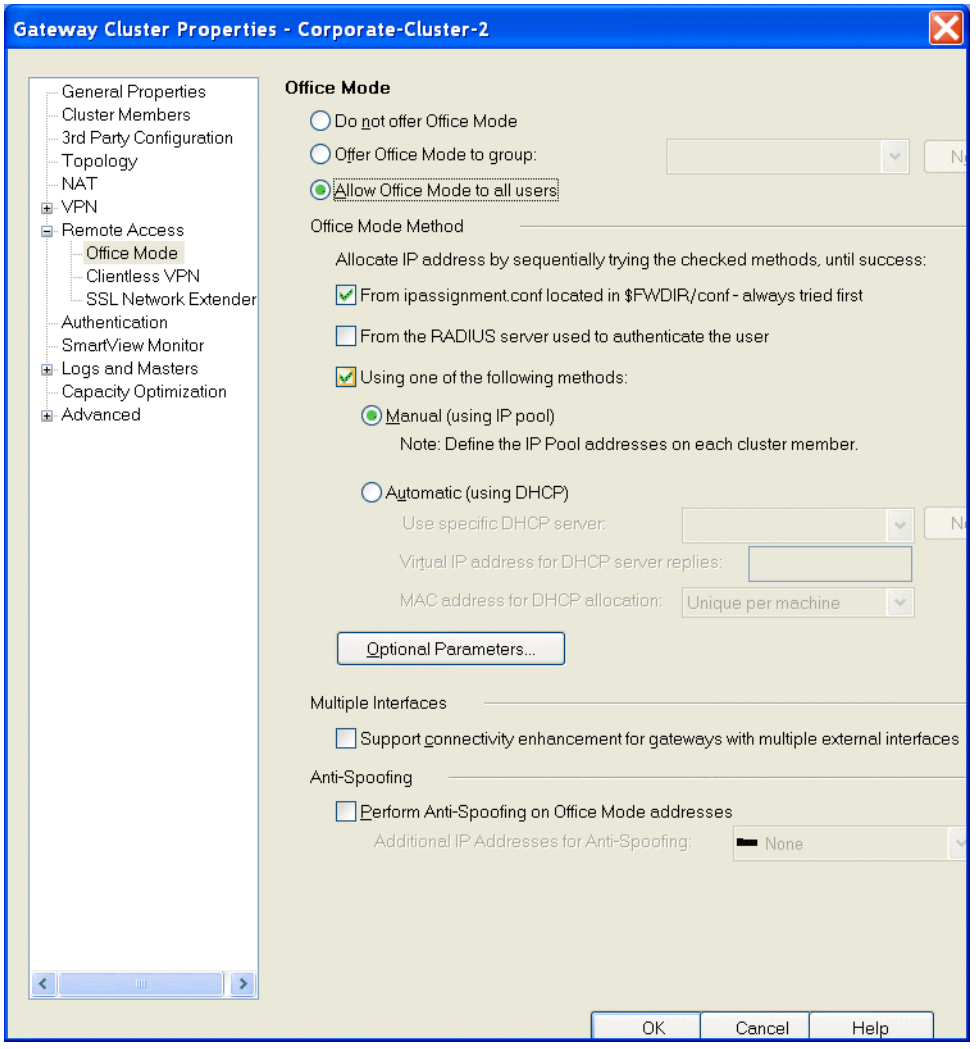
3 Click **Advanced**. The **Advanced Load Sharing Configuration** window opens.

FIGURE 3-2 Advanced Load Sharing Configuration window



4 Select **Use Sticky Decision Function**. Using this function, when the client connects to the cluster, all of its traffic passes through a single gateway. If the member gateway fails, the client reconnects to another cluster member and resumes its session.

5 Select **Gateway Cluster Object > Remote Access > Office Mode**. When defining office mode for use with load sharing clusters, only the **Manual (using IP pool)** method is supported. (Why is there another picture here?)Office Mode window



Authentication Schemes

There are four ways to identify and authenticate a remote user

- **Certificate**: The system authenticates the user through a certificate. Enrollment is not permitted.

- **Certificate with enrollment**: The system authenticates the user through a certificate. Enrollment is permitted. If the user does not have a certificate, enrollment is permitted using a registration key provided by the system administrator.
- **Legacy**: The system authenticates the user through their username and password as well as other challenge-response options (for example, SecurID).
- **Mixed**: The system attempts to authenticate the user through a certificate. If the user does not have a valid certificate, the system attempts to authenticate the user through one of the legacy methods.

Integrity SecureClient supports a secure authentication (SAA) OPSEC interface that allows third party-extensions to the standard authentication schemes.

For additional information, refer to *Client-Gateway Authentication Schemes* in the *VPN User Guide*.

Configuring the Authentication Method

This feature is configured using the `neo_user_auth_methods` property described in TABLE 3-2.

Re-authenticate Users

This feature is configured using the `neo_user_re_auth_timeout` property described in TABLE 3-2.

Configuring Encryption Methods

To determine whether the Integrity SecureClient Mobile client supports the RC4 or the 3DES encryption method, use the `neo_encryption_methods` property listed in TABLE 3-2. The following encryption methods are available:

- **3DES only**: (Default) The Integrity SecureClient Mobile client only supports 3DES.
- **3DES or RC4**: The Integrity SecureClient Mobile client supports both the RC4 and the 3DES encryption methods. (RC4 is a faster encryption method.)

Certificates

The SmartCenter server uses the same certificate for both SSL Network Extender and Integrity SecureClient Mobile clients when SSL Network Extender is enabled. If SSL Network Extender is disabled, add the `neo_gw_certificate` key to `SOFTWARE/CheckPoint/VPN1` to the registry on each gateway.

To add the certificate, run:

```
ckp_regedit -a SOFTWARE/CheckPoint/VPN1 neo_gw_certificate
“cert_nickname”
```

To remove the certificate, run:

```
ckp_regedit -d SOFTWARE/CheckPoint/VPN1 neo_gw_certificate
```

If SSL Network Extender is disabled, and no certificate for Integrity SecureClient Mobile clients is defined, a certificate issued by the internal CA is used.

Certificate Nickname

To view the certificate nickname

1 On **SmartDashboard**, open the **VPN** tab of the relevant network object.

2 In the **Certificates List** section, the nickname is listed next teach certificate.

Management of Internal CA Certificates

If the administrator has configured **Certificate with Enrollment** as the user authentication scheme, the user can create a certificate by using a registration key provided by the system administrator.

To create a user certificate for enrollment:

1 Follow the procedure described in “The Internal Certificate Authority (ICA) and the ICA Management Tool” in the *SmartCenter User Guide.*

Note - In this version, enrollment to an External CA is not supported.

2 Browse to the ICA Management Tool site, `https://<mngmt IP>:18265`, and select **Create Certificates**.

3 Enter the username, and click **Initiate** to send a registration keyto the user.

When the user connects using Integrity SecureClient Mobile without a certificate, the **Enrollment** window opens, and the user can create a certificate by entering the registration key they received from the system administrator..

Note - The system administrator can direct the user to the URL, `http://<IP>/registration.html`, to receive a registration key and create a certificate even if they do not wish to use the SSL Network Extender at that time.

Importing a Certificate

To import a certificate using Integrity SecureClient Mobile, the certificate must already be on the Pocket PC and located in the `My Documents` directory.

To import a certificate:

1 Select **Start > Programs > Connection > CertImport**.

2 Click the certificate to be imported.

3 Enter the certificate password.

4 Select **Import issuer to Root CA** to import the certificate of the CA that was issued for the imported certificate. Use this feature when user and server certificates are issued by the same CA, for example a Check Point internal CA.

5 To view the additional certificate, select **Start > Settings > System > Certificates > Root**.

6 To view the personal certificate, select **Start > Settings > System> Certificates > Personal**.

7 Click **OK**. A window opens indicating that the certificate was imported successfully.

8 Click **OK**.

Topology Update

Topology updates are downloaded to the client on a regular basis, as defined by the administrator. The topology also is automatically updated each time that a user connects to a gateway and when a user reconnects after an authentication timeout occurs. The client is therefore always aware of changes made to the network behind the gateway.

To determine the frequency with which updated site details are downloaded to the client

1 On **SmartDashboard**, select **Policy > Global Properties > Remote Access**.

2 In **Topology Update**, select **Update topology every ... hours**.

3 Enter the frequency (in hours) with which the policy should be updated.

Security Policy

A security policy is created by the system administrator in order to regulate incoming and outgoing traffic.

If a client connects and Integrity SecureClient Mobile is disabled, a default policy is enforced for first time users. If the client connected previously, the policy used during the last connection is enforced.

Use one of the following methods (listed in order of priority) to configure a security policy:

1 Using dbedit on the SmartCenter server. For additional information, refer to "Advanced Configuration" on page 33.

2 Modifying the TTM files on each gateway. For additional information, refer to "Transform Template Files (TTM)" on page 40.

3 Modifying the `startup.C` file in a package. For additional information, refer to "Client Deployment" on page 43.

When there are conflicting settings, that is one setting is configured differently in two locations, the settings configured in the highest priority location are applied. For example, if `neo_remember_user_password` is set to `true` in dbedit and `false` in the TTM file, Integrity SecureClient Mobile treats the property as `true`.

Configuring Security Policy When Management Patch is Installed

When the management patch is installed, the security policy is configured on the SmartCenter server using dbedit.

To configure the security policy using dbedit:

1 Select **Global Properties > properties > firewall_properties**.

2 In the **Field Name** column, find `mobile_remote_access_properties`. The Integrity SecureClient Mobile properties appear below this property.

3 Customize the properties to meet the requirements.

4 Save the changes and select install policy.

The changes are not enforced until install policy is run. The policy is delivered to all gateways. Refer to TABLE 3-1 for a list of the properties used to configure the security policy.

Configuring Security Policy Without Management Patch

If the management patch is not installed, the security policy is configured on each gateway using Transform Template (TTM) files. The TTM files `fw_client_1.ttm`, `vpn_client_1.ttm` and `neo_client_1.ttm` are located on each gateway in the `$FDIR/conf/` folder. For additional information, refer to "Transform Template Files (TTM)" on page 40.

Connecting to a Site

To connect to a site:

1 On the toolbar, tap **Connect**. The **Connect to a new Server** window opens.

2 In the **Server address or name** field, enter the gateway information. If you are using Visitor mode to connect to a port other than the default (TCP port 443as explained in "Visitor Mode (SSL Tunnel)" on page 13), enter "<gateway information>:<port>".

3 Tap **OK**. The first time you connect to a server, the credentials need to be verified.

4 When prompted, enter your credentials.

Note - If you connected to a gateway, then tap **Connect** on the toolbar to connect to the most recently connected gateway.

To connect to the most recently connected gateway:

1 On the toolbar, select **Tools > Connect**.

2 Select the server name or IP address of the gateway, or tap **Connect** on the toolbar to connect to the most recently connected gateway.

Configuring Display Settings

To configure display settings on the mobile device:

1 Select **Tools > Options...**.

2 Scroll down to **Display Settings**, and configure the following:

- **Show Today Item**: Select this option to display Integrity SecureClient Mobile in the **Today Item** menu.
- **Show Taskbar icon**: Select this option to display the Integrity SecureClient Mobile icon on the taskbar when the client is running.

- **Flash icon on encrypting**: Select this option to display the **i** in the icon on the taskbar, which flashes when information is sending or receiving.
- **Flash icon on firewall packet drop**: Select this option to display the lock in the icon on the taskbar, which flashes when packets are dropped.

Status Page

The status page has two views, basic details and more details.

Basic details view contains:

- **Status**: Displays whether the client is connected to a gateway.
- **Server ID**: Displays the gateway name or IP address of the current connection.
- **Firewall policy**: Displays whether the firewall policy is enabled or disabled.

More details view contains:

- **Status**: Displays whether the client is connected to a gateway.
- **Server ID**: Displays the gateway name or IP address of the current connection.
- **Office mode IP**: Displays the office mode IP address that was assigned by the gateway.
- **Duration**: Displays the duration of the current session.
- **Firewall policy**: Displays whether the firewall policy is enabled or disabled.
- **ActiveSync policy**: Displays whether the ActiveSync policy is enabled or disabled.

Advanced Configuration

The security policy is configured using the properties described in:

- TABLE 3-1 VPN Properties
- TABLE 3-2 Gateway Properties
- TABLE 3-3 Firewall Properties
- TABLE 3-4 General Properties

TABLE 3-1 VPN Properties

Property	Description	Valid Values (Default value in bold)
`neo_remember_user_password`	Remembers the user password (password caching). So long as the password is cached, the user should not be prompted to enter a password when the client connects, reconnects or re-authenticates.	**false**, true, client_decide
`neo_remember_user_password_timeout`	The password cache timeout (in minutes) since the user has entered their credentials. An authentication attempt after this timeout expires requires the user to re-enter their credentials.	-1 (infinite), 1 - MAX_INT, **1440**
`neo_clear_in_activesync`	Enables clear traffic during ActiveSync. When the device is cradled (for example, when ActiveSync is activated to a PC using Bluetooth), the client automatically disconnects and the firewall settings permit clear traffic to exit the device to the encryption domain. This is required when the connected PC is located inside the encryption domain and the encryption of data is not necessary. A message balloon appears when the client disconnects.	false, true, **client_decide**

TABLE 3-1 VPN Properties

Property	Description	Valid Values (Default value in bold)
neo_always_connected	Always connected. The client automatically connects to the last connected gateway: • When the device has a valid IP address. • When the device "wakes up" after it had low-power and after a soft-reset. • After the condition that caused the device to automatically disconnect ceases to exist (Allow clear traffic during ActiveSync, Disconnect when idle).	false, true, **client_decide**
neo_always_connected_retry	The always connected retry timeout (in minutes). If an automatic connection fails, the client tries to reconnect until the retry timeout is reached. The client also tries to reconnect after the IP address of the client changes, or if the user requests aconnection.	**1 (default)** -MAX_INT
neo_initiate_dialup	This flag instructs the client to automatically initiate an existing dialup connection (for example, GPRS). When the always connected flag is set to true, the user requests a connection, and there is no valid IP on the machine.	false, true, **client_decide**

TABLE 3-1 VPN Properties

Property	Description	Valid Values (Default value in bold)
neo_disconnect_when_idle	Disconnect when idle. Automatically disconnects the tunnel when there is no traffic sent over the tunnel over a defined time period. A message balloon appears when the client disconnects.	false, true, **client_decide**
neo_disconnect_when_idle_timeout	Disconnect when idle timeout (in minutes).	**1 (default)** -MAX_INT
neo_allow_clear_while_disconnected	Enables clear traffic to the encryption domain when the client is disconnected. The client prevents clear traffic to the encryption domain from exiting the machine at all times except if this flag is set to true. Note: In an IPSEC client, this functionality is achieved using the VPN chain in the firewall. In Integrity SecureClient Mobile, this functionality is achieved using the firewall rule setting.	false, true, **client_decide**
neo_user_approve_server_fp	Requests user approval of server Finger Print (FP) before the client enters its credentials. The server FP is part of the gateway certificate provided in the SSL interaction with the client. The following options are available: • **Once**: If the FP is seen for the first time by the client and not stored in the client database. • **Always**: Prompts the user to approve the FP for every connection. • **Never**: Always accepts the FP.	once, always, never, **client_decide**

TABLE 3-1 VPN Properties

Property	Description	Valid Values (Default value in bold)
`neo_allow_site_creation`	Enables the client to connect to a new gateway. When this flag is set to false, the client can only connect using the list of gateways configured in the client setup package.	false, true, **client_decide**
`neo_block_conns_on_erase_passwords`	Blocks a connection upon the removal of passwords. If set to true, when the user clears the **Remember Password** option in the **Settings** window, or selects the **Erase Passwords** menu option, the tunnel is automatically disconnected. A message balloon appears when the client disconnects.	false, true, **client_decide**
`neo_disconnect_when_in_enc_domain`	If the client is connected to a site, and an interface appears with an IP address located within one of the VPN encryption domains, the client disconnects. A message balloon appears when the client disconnects.	false, true, **client_decide**

TABLE 3-2 Gateway Properties

Property	Description	Valid Values (Default value in bold)
neo_enable	A gateway property which activates neo support.	**false**, true
neo_user_auth_methods	Client authentication methods.	certificate, certificate with enrollment, **legacy**, mixed
neo_encryption_methods	Client encryption methods.	**3DES only**, 3DES or RC4
neo_upgrade_mode	Client upgrade mode.	no upgrade, **ask user**, force upgrade
neo_upgrade_version	The client required version.	a number in hexadecimal format
neo_upgrade_url	Client download URL.	
neo_keep_alive_timeout	The frequency with which the client sends keep-alive packets (in seconds).	10-MAX_INT, **20 (default)**
neo_package_id	The gateway allows only clients with these package IDs to connect (comma separated list).	
neo_user_re_auth_timeout	The session validity timeout (in minutes).	10~1440, **480 (default)**
neo_saa_guilibs	The DLL name or full path that is loaded for authentication with the server.	
neo_saa_url	The relative URL for SAA authentication.	

TABLE 3-3 Firewall Properties

Property	Description	Valid Values (Default value in bold)
neo_enable_firewall_policy	Enables the firewall policy (disabled if not installed).	false, true, **client_decide**
neo_firewall_policy	The supported firewall policies: • Allow-all • Outgoing only • Outgoing and encrypted • Encrypted only • Block all (never disabled)	allow_all, outgoing_only, **outgoing_and_encrypted**, encrypted_only, block_all
neo_enable_activesync	Enables ActiveSync (disabled if firewall is not installed).	false, true, **client_decide**
neo_enable_ip_forwarding	Enables IP forwarding (when firewall is enabled).	**false**, true, client_decide
neo_enable_automatic_policy_update	Automatically update the policy when it expires.	false, **true**, client_decide
neo_policy_expire	The policy expiration timeout (in minutes).	-1 (infinite); 10-MAX_INT, **525600**
neo_automatic_policy_update_frequency	frequency with which the client updates policy files (in minutes).	5-MAX_INT, **120**

TABLE 3-3 Firewall Properties

Property	Description	Valid Values (Default value in bold)
neo_request_policy_update	If set to true, the client prompts the user to update the policy upon policy expiration (automatic_policy_update_frequency). If the client is disconnected, the client attempts to update the policy after a connection is made.	false, **true**, client_ decide
neo_route_all_traffic_through_gateway	Routes all traffic through a gateway (in hub mode). This flag sets the default route in the IP routing table to the connected gateway, which results in all traffic leaving the machine (except for specific routes) to be encrypted and possibly re-routed from the gateway to the outside Internet. It allows for the inspection of all client data received that is examined by the connected gateway.	**false**, true, client_ decide
neo_implicit_disconnect_timeout	The retry to establish a tunnel until the timeout elapses (in minutes).	1-MAX_INT, **2 (default)**

TABLE 3-4 General Properties

Property	Description	Valid Values (Default value in bold)
neo_run_client_on_device_startup	Runs the client on device startup.	false, **true**, client_decide
neo_enable_kill	Specifies whether the user can stop the client. If this option is set to false, the quit option does not appear in the client menu.	false, true, **client_decide**
neo_allow_client_debug_logs	Enables the client troubleshooting window.	false, true, **client_decide**
neo_allow_client_db_export	Enables the client to export its local database to a clear text file is used to create a customized installation package.	**false**, true, client_decide
neo_show_today_item	Displays the today item.	false, true, **client_decide**
neo_show_taskbar_item	Displays the taskbar icon.	false, true, **client_decide**
neo_flash_icon_on_encrypting	Displays the flash icon, which monitors VPN tunnel activity (traffic).	false, true, **client_decide**
neo_flash_icon_on_fw_packet_drop	Displays the flash icon, which monitors firewall packet dropping activity.	false, true, **client_decide**

Transform Template Files (TTM)

The security policy is defined on each gateway individually using the TTM files when the management patch is not installed on the SmartCenter server. TTM files are found on each gateway in the `$FDIR/conf/` folder.

There are three types of TTM files:

- `vpn_client_1.ttm` (Refer to TABLE 3-1 for details.)
- `fw_client_1.ttm` (Refer to TABLE 3-3 for details.)
- `neo_client_1.ttm` (Refer to TABLE 3-4 for details.)

To configure the security policy using TTM files:

1 Open a TTM file using any text editor.

2 Set the default value for the property you are changingexample:

```
   :neo_request_policy_update ( :gateway ( :default (true)))
or
   :neo_request_policy_update (
           :gateway (
                   :map (
                           :false (false)
                           :true (true)
                           :client_decide (client_decide)
                   )
                   :default (true)
           )
   )
```

3 Change the default setting, `true`, to create a new default setting for the security policy.

4 Save the file and select install policy.

Setting Policy Expiration

The following property is used to set the policy expiration timeout for all policies, except the firewall policy: `:expiry ( :gateway ( :default (100)))`.

The following property is used to set the firewall policy expiration timeout: `:expiry ( :gateway (neo_policy_expire :default (100)))`.

CHAPTER 4

Client Deployment

In This Chapter

Client Deployment Overview

Integrity SecureClient Mobile is packaged as a self-installing CAB (cabinet) or MSI (Microsoft Installer) file package. Users can install either package without specifying configuration details. This ensures the proper configuration of Integrity SecureClient Mobile software.

A CAB file package contains compressed files, which are mainly used to distribute software. The CAB file package is installed directly on the mobile device and has a `.cab` file extension.

An MSI file package, created by Windows Installer, is used for a silent (unattended) installation. It contains a record of all the keystrokes required to install Integrity SecureClient Mobileincludes a `.cab` file. The MSI package is installed on the user's personal computer and has a `.msi` file extension. During installation, the CAB file package is extracted from the MSI package and installed on a connected mobile device using ActiveSync services.

Package Customization

The administrator obtains the Integrity SecureClient Mobile distribution package from the Check Point Download Center. The distribution package is located in a `.zip` file, which contains the client components, such as the CAB and MSI packages, and the unpacked client (application) files.

The unpacked client files are the same as those in the CAB package. The administrator can customize and package these files into a new CAB or MSI file package before distributing it to users. The customized package can include predefined topology andcredentials, a default firewall policy and other settings.

During version upgrades, the installer retains the existing client policies and credentials that were not predefined in the upgrade package. The administrator can client upgrade using the `neo_upgrade_mode`, `neo_upgrade_version`, and `neo_upgrade_url` flags.

When the client is installed on the mobile device, another applet, called Certificate Import Wizard, is also installed. This applet enables you to import PKCS#12 certificates to the device.

The CAB and MSI packages can be edited by the administrator to customize the settings for Integrity SecureClient Mobile. The administrator can edit the package :

- Adding a file to the CAB package, for example, a user certificate file or a Secure Authentication (SAA) plug-in. For additional information, refer to "Adding a File to a CAB Package" on page 44.
- Deleting a file from the CAB package, for example, the `Cert_import` utility may not be needed for some configurations. For additional information, refer to "Deleting a File from a CAB Package" on page 45.
- Preconfiguring the client database parameters. For additional information, refer to "Exporting the Client Configuration" on page 46.
- Defining the client installation version. For additional information, refer to "Defining the Client Installation Version" on page 46.

Adding a File to a CAB Package

To add a file to a CAB package:

1 Obtain the Integrity Secure Client Mobile distribution `.zip` file from the Check Point Download Center site or from the CD.

2 Save the distribution `.zip` file to your local machine and extract its contents. One of the files is the `Integrity-M_Setup_<build number>.zip` file.

3 Extract `Integrity-M_Setup_<build number>.zip` to a folder (for example, `ISCM`). This creates a number of subfolders.

4 Copy and paste the file(s) to be included in the package to the `conf` folder (one of the extracted subfolders created in step 3).

5 In the `ISCM` folder, open the `Integrity-M_Setup_<build number>.inf` file using a text editor.

6 In the `Integrity-M_Setup_<build number>.inf` file, add the name(s) of the file(s) to be included in the package to the following sections:
   - In the `[conf]` section, add the name(s) of the file(s) starting on the line immediately after `startup.C`.
   - In the `[SourceDisksFiles]` section, add the name(s) of the file(s) starting on the line immediately after `startup.C`. Every file in this section ends with an equal sign and a number, for example, `startup.C=7`. Add an equal sign and a number to the end of each file name that is added. The number represents the folder the file is placed in and corresponds to the `[SourceDisksNames]` section numbers.

7 Save the file.

8 Continue to "Creating a CAB Package" on page 47.

Deleting a File from a CAB Package

To delete a file from a CAB package:

1 Obtain the Integrity SecureClent Mobile distribution `.zip` file from the Check Point Download Center site or from the CD.

2 Save the distribution `.zip` file to your local machine and extract its contents. One of the files is the `Integrity-M_Setup_<build number>.zip` file.

3 Extract `Integrity-M_Setup_<build number>.zip` to a folder (for example, `ISCM`). This creates a number of subfolders.

4 In the ISCM folder, open the `Integrity-M_Setup_<build number>.inf` file using a text editor.

5 In the `Integrity-M_Setup_<build number>.inf` file, delete references to the file(s) to be deleted in the following sections:
   - In the `[conf]` section, delete the name(s) of the unwanted file(s).
   - In the `[SourceDisksFiles]` section, delete the name(s) of the unwanted file(s).

6 Save the file.

7 Continue to "Creating a CAB Package" on page 47.

Exporting the Client Configuration

The administrator can provide all users with customized settings that are configured on an Integrity SecureClient Mobile client.

To export the client configuration, xports the client database file to the `startup.C` file, which is then added a CAB or an MSI package that is distributed to clients. When the customized package is installed on the device, the `startup.C` file is imported to the client database.

To export the client configuration:

1 Install the client on a handheld device.

2 Configure a client with the required configuration, for example, configure the client's firewall options and connection to the gateways. You can now export the database with the current client configuration settings.

3 To export the database, locate the `database.C` file on the client, and in the `global properties` section of `database.C`, change the value of the property `neo_allow_client_db_export` to `true`.

4 Copy the `database.C file` to the `client` folder.

5 Restart the client.

6 In Integrity SecureClient Mobile, select **Tools > Help > Export db**. This exports the current settings to the `startup.C` file, which contains the nonconfidential data in the database.

7 Replace the `startup.C` file that is located in the `conf` folder of the preconfigured package. This file may be edited manually using a text editorin order to add or remove flags.

Note - Exporting `startup.C` will also export the global property `neo_allow_client_db_export` with the value set to **true**. To restrict users from exporting the client configuration, edit the `startup.C` and remove the property or set it to **false**.

Defining the Client Installation Version

The default client installation version is the client build number defined by Check Point.

To change the client installation version:

1 Obtain the Integrity Secure Client Mobile distribution `.zip` file from the Check Point Download Center site or from the CD.

2 Save the distribution `.zip` file to your local machine and extract its contents. One of the files is the `Integrity-M_Setup_<build number>.zip` file.

3 Extract `Integrity-M_Setup_<build number>.zip` to a folder (for example, `ISCM`). This creates a number of subfolders.

4 In the ISCM folder, open the `Integrity-M_Setup_<build number>.inf` file using a text editor.

5 Change the following attribute to the desired build number:

```
NEO_VERSION_NUMBER= <build number>
```

6 Save the file.

7 Continue to "Creating a CAB Package" on page 47.

Creating a CAB Package

A CAB package is created from the application files using the Cabwiz utility. Cabwiz can be downloaded and installed from the Microsoft Pocket PC 2003 SDK.

To create a CAB package:

1 To obtain the Cabwiz utility

- Download the Microsoft Pocket PC 2003 SDK from here.
- Install the SDK on your PC. After the SDK is installed, the Cabwiz utility is normally located at: `C:\Program Files\Windows CE Tools\wce420\POCKET PC 2003\Tools`.

2 Edit the package by exporting the client configuration and removing and/or adding files (for additional information, refer to "Adding a File to a CAB Package" on page 44, "Deleting a File from a CAB Package" on page 45 and "Exporting the Client Configuration" on page 46).

3 Copy the `Cabwiz.exe` and the `Cabwiz.ddf` files to the `ISCM` folder created when extracting the `Integrity-M_Setup_<build number>.zip` file (this file was originally extracted from the Integrity SecureClient Mobile distribution `.zip` file).

4 Copy the `makecab.exe` from the Windows system directory (by default: `C:\WINDOWS\system32`) to the `ISCM` folder.

5 Run the `Cabwiz Integrity-M_Setup_<build number>.inf` file. The created CAB package has a `.cab` extension.

Creating an MSI Package

The user provided MSI package includes a Windows installer, which is added to the MSI package using the Microsoft ORCA tool and installs the `.cab` file.

To create an MSI package:

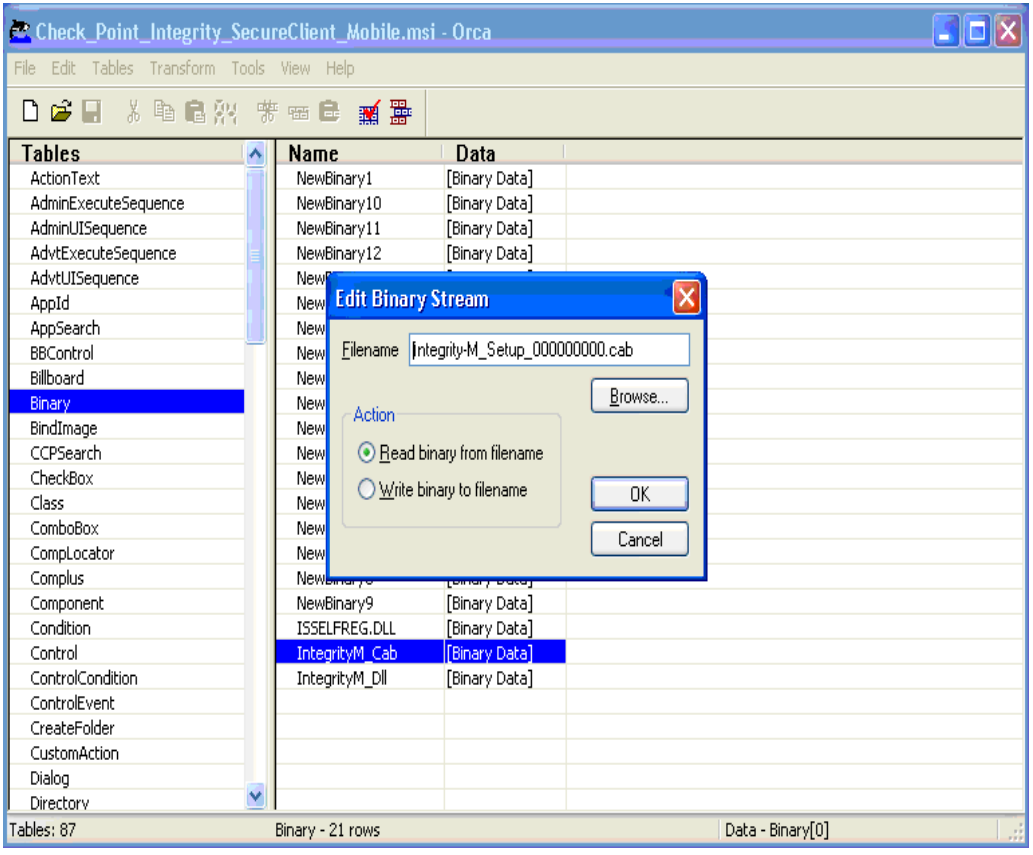
1 Obtain the Integrity Secure Client Mobile distribution `.zip` file from the Check Point Download Center site or from the CD.

2 Save the distribution `.zip` file to your local machine and extract its contents. One of the files is the Integrity SecureClient Mobile MSI file.

3 Download the Microsoft Windows Installer SDK that includes ORCA from http://support.microsoft.com/kb/255905/EN-US/.

4 Using the ORCA tool, open the Integrity SecureClient Mobile `.msi` file. The **Integrity SecureClient Mobile MSI** window in Orca is displayed.

5 Select **Binary** from the **Tables** list.



6 In the right pane, on the **IntegrityM_Cab** row, double-click **Binary Data** in the **Data** column. The **Edit Binary Stream** window opens.

7 Browse to the Integrity SecureClient Mobile CAB package and select **OK**.

8 Save the file and exit. The created MSI package has a `.msi` extension.

Configuring the SAA Plugin

Enabling the SAA plugin enables the ability to implement additonal authentication schemes (for example SoftID.) The plugin also allows customizing the login page.

To enable the SAA plugin using GuiDBedit:

1 Set the property `neo_saa_guilibs` to the SAA plugin name, for example `SAAPlugin.dll`.

2 Save the change and exit GuiDBEdit.

3 Install the updated policy.

Once the SAA plugin is enabled on the gateway, the client can be configured in one of two ways:

1 Manually

2 Using a predefined package

Configuring the SAA Plugin on the Client Manually

On the device:

1 Copy the SAA plugin into the following folder:

```
\Program Files\CheckPoint\Integrity-M
```

2 Connect to the gateway. During the connection process, the defined SAA plugin pop-up appears.

In the event you receive the following error message, "Configuration Error: Failed to load SAA plugin," use the client login page (username-password) to connect. Once connected, quit and relaunch the client again.

Using a Predefined Package

This configuration is for situations where all the users use the SAA plugin to connect. In the event that only only certain users are required to use the plugin, set the `neo_saa_guilibs` property to an empty string after you complete the creation of the customized package. As a result, only the users using the customized package will be using the SAA plugin.

1 Follow the steps described in “Configuring the SAA Plugin on the Client Manually” on page 49.

2 Establish a connection with each gateway that will be included in the package. This will store each gateway into the clients database.

3 Export the client configuration. To export the database, see “Exporting the Client Configuration” on page 46.

4 Use the exported `startup.c` to create the customized CAB file (include the SAA plugin in the CAB too). To create a CAB file, see “Creating a CAB Package” on page 47.

Client Hardware and Software Requirements

Operating System

- Windows Mobile 2003/SE (Pocket PC Configuration)
- Windows Mobile 5.0 (Pocket PC Configuration)

Processor

- Intel ARM/StrongARM/XScale/PXA Series Processor family
- Texas Instruments OMAP Processor family

CHAPTER 5

Troubleshooting

In This Chapter

Enabling Log Files

Log files are files that records client activity, which are useful when troubleshooting various issues.

To enable log files:

- From the Integrity SecureClient Mobile GUI, select **Tools > Help > Troubleshooting**.

5 Log files may be enabled for **Client**, the **VNA Kernel** (Virtual Network Adapter) and the **FW Kernel**.

Routing Table

The routing table is used by the TCP/IP stack to route IP packets on the device.

IP Configuration

The IP configuration page displays the IP addresses of the various interfaces.

Error Messages

TABLE 5-1 provides a list of error messages, their possible cause and a solution.

TABLE 5-1 Error Messages Troubleshooting

Error Message	Possible Cause	Solution
Cannot find the server (server name). Please check the server name and try again.	There is an error resolving the server name.	Check the server name and verify that the IP address is valid.
Error while negotiating with the server (server name). Please try again.	Error in client-server negotiation.	Try to connect again.
You are not permitted to access the server.	The user is not authorized.	Check that the user certificate is installed and is valid.
Your device is not connected to any network.	The network is not available for connection.	Connect the device to a network.
Your device is not connected to any network. Dialup connection is not available.	The network is not available for connection and dialup cannot be initiated. The settings may not be configured properly.	Check that your dialup settings are configured properly.
Access denied. Wrong username or password.	Wrong credentials supplied.	Ensure that the credentials are current and retry. If the credentials are cached, use the **clear passwords** button.
User is not permitted to have an office mode IP address.	The user attempting to connect is not configured to have an office mode IP address and therefore the connection failed.	Ensure that the user is configured to receive an office mode IP address.

TABLE 5-1 Error Messages Troubleshooting

Error Message	Possible Cause	Solution
The certificate provided is invalid. Please provide the username and password.	Invalid certificate provided.	Either install a new user certificate or connect with a username and password.
Connection to the server (server name) was lost.	There is no connection to the server, and the client disconnected.	Try to reconnect.
Security warning! Server fingerprint has changed during connection. Contact your administrator.	Server validation failed and therefore the connection failed.	Contact your administrator.

Additional Resources

For additional resources on setting up Integrity SecureClient Mobile, refer to:

How to add your own root certificate via CAB file.

How to add root certificates to Windows Mobile 2003 Smartphone and to Windows Mobile 2002 Smartphone.

Windows Mobile 5.0 Security Model FAQ.

ActiveSync 4.x Troubleshooting Guide.

Index

V