



iPassConnect™/Check Point™ VPN-1® SecuRemote/SecureClient™ NGX Integration Guide

Corporate Headquarters

iPass Inc.

3800 Bridge Parkway

Redwood Shores, CA 94065 USA

<http://www.ipass.com>

T: +1 650.232.4100

F: +1 650.232.0227

**iPassConnect™/Check Point™ VPN-1® SecuRemote/SecureClient™ NGX
Integration Guide 3**

Introduction 3
 iPass Mobile Office 3
 Integration Definitions 3
 Auto-connect Integration 3
 Auto-launch Integration 3
 Auto-teardown 4
 Configuring Integration 4
 Auto-connect (a.k.a. “1-click”) 4
 Tunnel Action: 4
 Disconnect Action: 4
 Miscellaneous Action: 4
 Auto-launch (a.k.a. “1.5-click”) 4
 Tunnel Action: 5
 Disconnect Action: 5
 Miscellaneous Action: 5
 Demonstration and Testing 5
 Summary 6
 Reference 6
 Support from iPass 6

iPassConnect™/Check Point™ VPN-1® SecuRemote/SecureClient™ NGX Integration Guide

Introduction

This document outlines the integration capabilities of any version of the iPassConnect™ client software for Microsoft™ Windows® PCs and Check Point VPN-1 SecuRemote/SecureClient NGX client.

iPass Mobile Office

The iPass Mobile Office solution, together with virtual private network (VPN) products, allows mobile employees, day extenders and telecommuters to gain secure, reliable, high-speed access to their corporate network or the Internet from virtually anywhere in the world. iPass provides this service by transmitting user data over the Internet through our private network of providers to terminate at the company's local AAA server for authentication. In a fashion transparent to the user, the iPass system records each user session, passes logon credentials to the appropriate corporate authentication server, and performs settlement between the various service providers involved. The iPass solution is compatible with all industry leading VPNs and security solutions, allowing our customers to select the tunneling and security technology of their choice. The iPass solution is independent of the VPN solution and its architecture although iPass does offer integration at the client level.

This document is targeted for audiences consisting of corporate VPN administrators, sales engineers, systems engineers, and any potential or existing iPassConnect customer/partner.

DISCLAIMER: The configurations presented in this document have been successfully tested by iPass. This document is intended as an overview, and not as a definitive guide for deployment or configuration of Check Point or iPass products or services. Nothing herein should be construed as a guarantee of the effectiveness of any of these methods or an endorsement of any of these vendors' products. Rather, iPass provides this information merely as a reference to system administrators. Implementation decisions should be made in consultation with the vendors involved. A discussion of requirements or procedures for installing or using iPassConnect or the Check Point VPN client software is beyond the scope of this document. Please consult either the iPass web site or the Check Point web site for complete product documentation.

Integration Definitions

Auto-connect (a.k.a. 1-click) Integration

Auto-connect integration is defined as a user needing to enter only one set of credentials into the iPassConnect software and having both the Internet and the VPN connection established automatically. This means the iPass RoamServer authentication and the VPN authentication must either point to the same common user database or must have the identical active username and password resident in each respective user database to which they authenticate

Auto-launch (a.k.a. 1.5-click) Integration

Auto-launch integration is defined as iPassConnect automatically launching the VPN client once connected to the Internet. The user must then select one of several possible pre-configured VPN

connection entries and manually click **Connect**. Finally, to authenticate the VPN client, the user must enter in a second set of credentials.

The user has the option of not connecting with the VPN client, but if *auto-teardown* (see page 4) is enabled, the user can only remain connected to the Internet if the VPN is connected.

Auto-teardown

Auto-teardown is defined as having the Internet connection (established by iPassConnect) disconnected automatically if the integrated VPN client is ever disconnected. Auto-teardown also functions if the VPN client was not connected within a given amount of time (a “grace period”) after the iPassConnect Internet connection was established. This is typical in the Auto-launch model or, where a two-factor strong/token authentication method is used for the VPN connection. With auto-teardown enabled, a user must be logged onto and connected to the Internet and the VPN at the same time.

Companies wishing an enhanced security policy may optionally disallow split tunneling on the VPN gateway connected. It should be noted that disabling split tunneling adds extra overhead to the VPN encryption/decryption, and decreases VPN system performance, as all traffic to and from the client PC must travel over the encrypted tunnel. Companies may also optionally allow Internet access through a corporate proxy or firewall server/router.

Configuring Integration

iPassConnect 3.50 or higher uses SHIM to reduce the path dependencies for Check Point VPN client installation paths. The SHIM also has timeout and retries logic built-in to support possible restarts of Check Point services when certain CLI functions are performed in the background. R56 or higher is currently supported client version.

Auto-connect (a.k.a. “1-click”) Integration

To configure iPassConnect for auto-connect interoperability with Check Point Client, submit the following requests to iPass for your iPassConnect client profile modification:

Tunnel Actions:

```
Path = CheckPointVPNShim.exe  
Parameters = /Launch /timeout=120 /enablemonitor /h=<WinHandle>  
/u=<UserName> /p=<UserPassword> /profile=[myprofile]
```

Disconnect Actions:

```
Path = CheckPointVPNShim.exe  
Parameters = /Disconnect
```

Miscellaneous Actions:

```
Path = CheckPointVPNShim.exe
```

<UserName> and <UserPassword> are iPassConnect “macros” used to pass the information to another client and must be typed as is (including arrow brackets). This is defined as the user entering in only

Auto-launch (a.k.a. “1.5-click”) Integration

To configure iPassConnect for auto-connect interoperability with Check Point Client, submit the following requests to iPass for your iPassConnect client profile modification:

Tunnel Actions:

Path = CheckPointVPNShim.exe

Parameters = /Launch /profile=[myprofile] /h=<WinHandle> /enablemonitor
/timeout=120

Disconnect Actions:

Path = CheckPointVPNShim.exe

Parameters = /Disconnect

Miscellaneous Actions:

Path = CheckPointVPNShim.exe

Demonstration and Testing

iPass maintains a Solutions Lab in our Redwood Shores, CA, corporate headquarters, where we can demonstrate the interoperability and integration of iPass products with security solutions including:

- VPN applications
- Personal firewall software
- AAA servers
- Access Gateways

In addition, the Lab is configured to troubleshoot issues that our customers face in testing and deploying their connectivity solutions. If you are interested in knowing more about the Solutions Lab, please contact us at solutions_lab@ipass.com.

iPass has included Check Point in our testing suite for all new releases of iPass products, as well as in certification of broadband providers included in the iPass virtual network.

Summary

iPass offers a very robust and tight integration with the Check Point VPN Client in many options to tailor the needs of Check Point VPN customers. The end result is a seamless user interface in iPassConnect which can be configured to automatically launch and optionally completely control the Check Point VPN Client.

iPassConnect integration for earlier versions of the Check Point VPN Client is also available, with certain limitations. Please contact iPass Technical Support or your iPass account manager for more details.

Reference

More information regarding Check Point VPN Client options can be found on the on the Check Point Web site.

More information regarding iPassConnect integration with this and other Technology Partner software, please visit the iPass Technology Partner web site located at:

http://www.ipass.com/?Technology_Partner/Technology_Partners

Support from iPass

To obtain support from iPass regarding this and any other issue, please contact iPass Technical Support at:

<http://www.ipass.com/support>

About iPass

iPass Inc. (www.ipass.com) provides software-enabled enterprise connectivity services designed to give employees secure access to information and applications on the corporate network from virtually any location in the world. As a virtual network operator (VNO), iPass offers enterprise employees a range of Internet protocol-based connectivity technologies, including wired and wireless broadband service at airports, hotels and conference centers worldwide. The iPassConnect™ smart client can be easily deployed across multiple computing devices and operating systems within an enterprise. Once deployed, the iPass service gives the corporate IT department complete control over how network resources are accessed. Founded in 1996, iPass is headquartered in Redwood

Corporate Headquarters
iPass Inc.
3800 Bridge Parkway
Redwood Shores, CA 94065
United States
Tel: +1 650.232.4100
Fax: +1 650.232.4111
www.ipass.com

United Kingdom
iPass (U.K.) Limited
139 Piccadilly
London W1J 7NU
United Kingdom
Tel: +44 20.7317.4400 Fax: +44
20.7317.4450

Germany
iPass (U.K.) Limited
Stiglmaierplatz/Dachauer Straße 37
(5.OG)
80335 Munich
Germany
Tel: +49 89.54.55.8.120
Fax: +49 89.54.55.8.333

Singapore
iPass Asia Pte Ltd.
7 Temasek Boulevard
#23-02 Suntec Tower One
Singapore 038987
Tel: +65 6334.8783
Fax: +65 6337.033

Australia
iPass Holdings Pty Ltd. Level 1, 80
Waterloo Road Macquarie Park, NSW
2113 Australia Tel: +612 8876.8700 Fax:
+612 8876 8777

Hong Kong
iPass Asia Pte Ltd. 3802A, Lippo Centre
Tower Two 89 Queensway, Admiralty
Hong Kong Tel: +852.2918.8268 Fax:
+852.2918.8278

Japan iPass Inc. Ginko Kyokai Building,
15th Floor 1-3-1 Marunouchi Chiyoda-
ku, Tokyo 100-0005 Japan Tel: +81
3.3216.7266 Fax: +81 3.3216.7281