

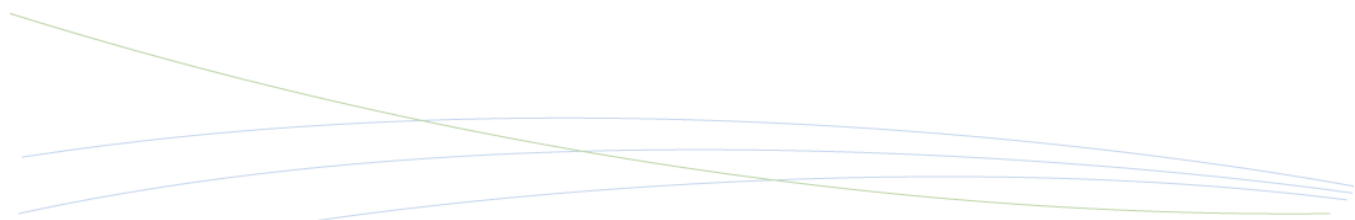


- What's New in  
Connectivity Secure Shell™ 2008

While every attempt has been made to ensure the accuracy and completeness of the information in this document, some typographical or technical errors may exist. Hummingbird, the Open Text Connectivity Solutions Group cannot accept responsibility for customers' losses resulting from the use of this document. The information contained in this document is subject to change without notice.

This document contains proprietary information that is protected by copyright. This document, in whole or in part, may not be photocopied, reproduced, or translated into another language without prior written consent from Hummingbird.

**This edition published June 2007**

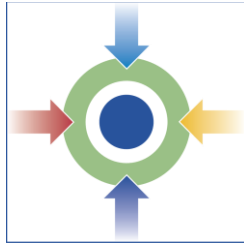


# Contents

<b>Contents</b>	<b>3</b>
<b>Hummingbird Connectivity™ 2008</b>	<b>4</b>
<b>Feature Summary</b>	<b>5</b>
<b>Feature Details</b>	<b>6</b>
Windows Vista Certification	6
SSH Command Line	6
Microsoft Windows Kerberos Support	7
X509 Authentication Support	8
Integrated SOCKS Support	9
Additional Browser Support	13
SOCKS Dynamic Port Forwarding	13
Event Monitoring Server	14

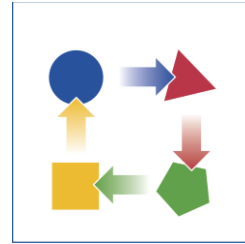
# Hummingbird Connectivity™ 2008

Hummingbird Connectivity is a suite of technology solutions that help organizations meet the challenges of integrating heterogeneous systems while providing cost effectiveness. Our customers have been instrumental in our development efforts, over the years and together we have achieved success. Hummingbird Connectivity continues to deliver unparalleled product functionality and substantive return on investment.



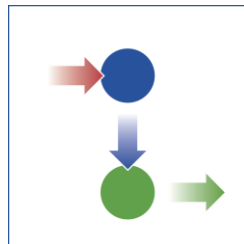
## Consolidation

Many organizations with numerous connectivity software vendors have been able to consolidate their needs into one single solution with Hummingbird Connectivity, helping them realize significant savings on their overall IT budgets



## Migration

Regardless of your current connectivity solution, Hummingbird Connectivity offers you a smooth migration path with minimal business disruption and immediate return on investment.



## Security

Hummingbird Connectivity features a robust and complete security set across all of its components, in order to help organizations meet their security and compliance objectives.



## Productivity

Employees are companies' most important assets. Hummingbird Connectivity provides users with unique ways of increasing their productivity while reducing the complexity associated with implementation and delivery.

## Feature Summary

Features	Summary
Windows Vista Certification	The Hummingbird Connectivity 2008 products have received the “Certified for Windows Vista” Logo and were vigorously and exhaustively tested by a Microsoft-authorized third-party laboratory under their finalization.
SSH command line	The SSH2 command line allows the user to run remote commands on the host, and to retrieve the output on the windows client machine. It supports a range of parameters including tunnel profiles.
Microsoft® Windows® Kerberos Support For Authentication	The Connectivity Secure Shell™ client now supports the Windows SSPI interface to acquire a security context which can be used to establish a Kerberos authentication in much the same manner as in an external Kerberos provider case (with MIT Kerberos or Connectivity Kerberos™ for instance).
X509 Certificate Authentication for SSH	Connectivity Secure Shell now offers support for draft v2 of the SSH public key authentication based on a user X.509 certificate.
Integrated SOCKS Support	SOCKS is a networking proxy protocol that enables hosts on one side of a SOCKS server to gain full access to hosts on the other side of the SOCKS server without requiring direct IP-reachability. SOCKS is often used as a network firewall. This new feature allows users to configure tunnel settings to use a Socks server.
SOCKS Dynamic Port Forwarding	Dynamic port forwarding allows a sockisfied application (one that supports using a socks proxy) to use a Connectivity Secure Shell tunnel as a VPN to forward connections dynamically, to different hosts, from the tunnel endpoint.
Additional Browser Support	In addition to Internet Explorer, Connectivity Secure Shell and other products that use the Hummingbird Deployment Wizard™ can now be deployed on Firefox®, Opera® and 3rd party java compatible browsers.
Event Monitoring Server	The Event Monitoring Server is an IIS-based service that monitors events generated by Hummingbird Connectivity™ client applications (e.g. HostExplorer®, Connectivity Secure Shell™, Hummingbird FTP™, Exceed® etc.). It logs client-specific actions like HostExplorer connecting to a host or Connectivity Secure Shell starting a tunnel into an event database and offer various administrative views to analyze that information.

## Feature Details

### Windows Vista Certification

The following Hummingbird Connectivity solutions have received the “Certified for Windows Vista” certification and are available on both 32-bit and 64-bit platforms:

- Exceed PowerSuite™ 2008
- Exceed 2008
- HostExplorer 2008
- NFS Maestro Solo™ 2008
- NFS Maestro Client™ 2008
- NFS Maestro Server™ 2008 Enterprise Edition
- Connectivity Secure Shell 2008
- Connectivity SecureTerm® 2008



### SSH Command Line

The SSH command line is a new utility introduced in Connectivity Secure Shell 2008 in order to provide administrators with the ability to execute remote actions over SSH from the windows command prompt.

The SSH command line is the ideal power tool for administrators, allowing them to perform many tasks, including the following:

- Running interactive standalone or piped commands against a remote host (for instance directory listing)
- Launching X11 clients from the command line (Exceed needs to be installed for the X11 client to be displayed)
- Running remote scripts securely
- Automating tasks through the creation of command files that invoke the SSH command

Figure 1 — The SSH Command Line options

```
C:\WINDOWS\system32\cmd.exe
C:\Program Files\Hummingbird\Connectivity\12.80\Security>ssh2
Usage:
ssh2 [-l user] [-p password] [-i pubkey] [-x] [-F file] [-v] [-d #] [-df file] [-q] [-p #] [-U file] [-c text] [-t] [-o] [-C] [-dt #] [-XD #] [-qpf #] [-h]
host is the remote server - use ? to be prompted, * to skip
cmdin is a remote command to be executed
-l user login name to be authenticated
-p password
-i pubkey passphrase for public key
-x enables (default) / -disables X11 forwarding
-F file specifies a .SSH profile
-v enables verbose mode
-d # trace level - from 0 to 3 (default = 2)
-df file specifies the trace (debug) file
-q displays the version string
-q quiet mode: no output
-p # port number (default 22) on the remote server
-U file filename containing the password
-c text remote command
-t allocate a pty - if not set, then no command output
-o display output from remote command
-C enable/disable (default) compression
-dt # delay time (seconds) to wait for idle channel
-XD # specifies the display # to use for X11 Forwarding
-qpf # specifies dynamic port forwarding on port # -accepts any connection
-lpf # specifies dynamic port forwarding on port # -local connections only
-h displays this help
Note: quote parameters containing embedded spaces.
C:\Program Files\Hummingbird\Connectivity\12.80\Security>
```

The SSH command line offers many options including

- Specifying a Secure Shell tunnel profile to be used
- Manually configuring the SSH connection through the command line switches
- Prompting the user at various steps of the connection
- Executing a remote command
- Launching an X11 client automatically: the display variable will be automatically set and the X server will be launched if needed (only with Exceed)

## Microsoft Windows Kerberos Support

Kerberos is a trusted third-party authentication service. Kerberos was originally created by the engineers of MIT's Project Athena. It evolved from version 4 to version 5, which is now on a standard track with the IETF (Internet Engineering Task Force).

Kerberos offers many benefits:

- It is a standards-based strong authentication system.
- It is supported by various operating systems (Windows and UNIX<sub>R</sub> for instance).
- It prevents transmission of passwords over the network.
- It offers single sign-on capabilities (1 password a day).
- It provides mutual authentication between the client and the server.

Hummingbird Connectivity products have been supporting Kerberos for a long time. Initial Kerberos support was provided through the MIT Kerberos client.

Hummingbird Connectivity 9.0 introduced Connectivity Kerberos™, our branded version of the MIT Kerberos client.

With Connectivity 2008, we are adding native Windows Kerberos support. Microsoft adopted Kerberos with the release of Windows Server 2000, when Kerberos became the default mechanism for authentication in the Windows world.

Support for Windows Kerberos allows Connectivity Secure Shell to natively use the Active Directory Kerberos authentication.



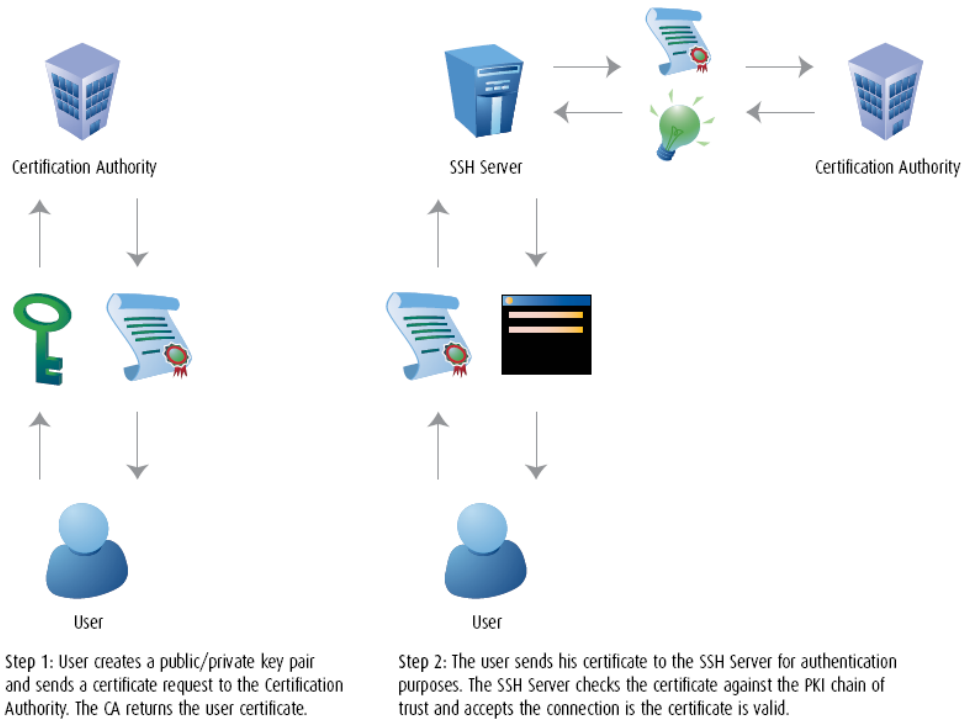
Figure 2 — The Kerberos authentication setting dialog in Connectivity Secure Shell 2008

## X509 Authentication Support

Public and private keys authentication has been available for a long time in the SSH protocol. Although this authentication mechanism is considered to be robust, it does not provide a strong method to verify that the key used during the authentication really does belong to the host claiming ownership.

X509 authentication can solve this problem by offering third-party trust through PKI in order to assert ownership of keys. Using X509 certificate instead of a normal public key allows the destination host to validate the identity of the user before using the public key from the certificate for authentication.

Figure 3 — Overview of the X509 user certificate authentication method



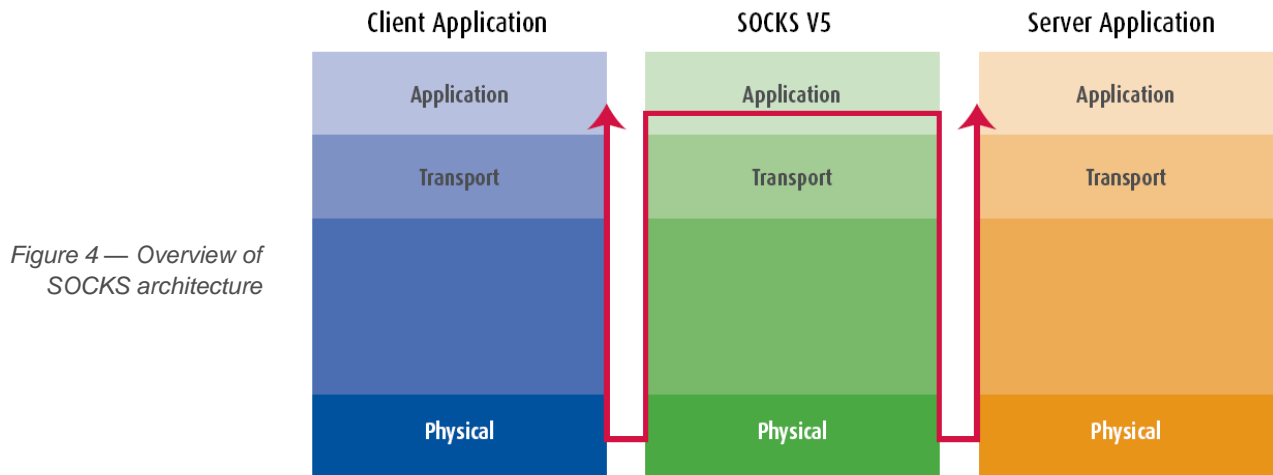
Unlike some of the proprietary SSH X509 authentication solutions, Hummingbird offers an implementation of X509 authentication that is fully compliant with the corresponding IETF draft. The power and flexibility of the Hummingbird Keys and Certificate Manager allow users to create their own self-signed certificate, issue a certificate request to a certification authority, or import an existing certificate in a variety of formats.

X509 certificate authentication can be combined with any of the other authentication mechanisms available in Connectivity Secure Shell, such as password, keyboard interactive, public/private keys, Kerberos, and Kerberos key exchange.

## Integrated SOCKS Support

SOCKS is a networking proxy protocol that enables hosts on one side of a SOCKS server to gain full access to hosts on the other side of the SOCKS server without requiring direct IP-reachability.

SOCKS is often used as a network firewall, redirecting connection requests from hosts on opposite sides of a SOCKS server. The SOCKS server authenticates and authorizes requests, establishes a proxy connection, and relays data between hosts.



SOCKS is an intermediate layer between the application layer and the transport layer.

There are two versions of the SOCKS protocol — SOCKSv4 and SOCKSv5, respectively.

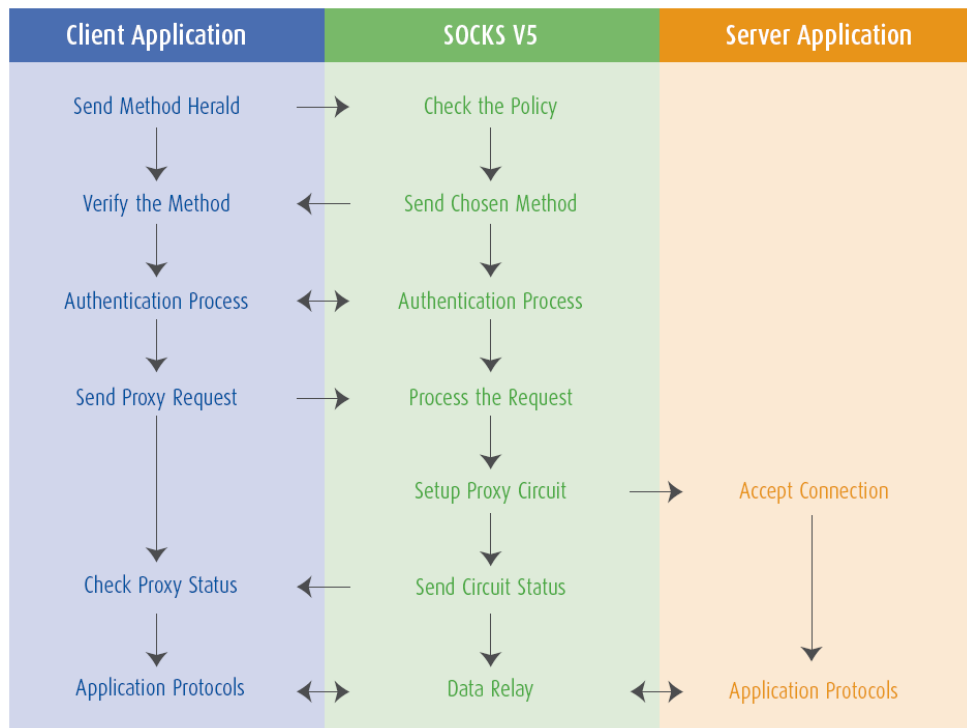
The SOCKSv4 protocol performs the following three functions:

- Makes connection requests
- Sets up proxy circuits
- Relays application data

The SOCKS version 5 protocol resolves several issues that SOCKS version 4 protocol did not fully address or omit:

- Strong authentication
- Authentication method negotiation
- Address resolution proxy
- Proxy for UDP-based applications

Figure 5 — The SOCKSv5 control flow diagram



Hummingbird has always been at the forefront of Windows SOCKS client. For more than 10 years, Hummingbird SOCKS Client has been available for free from the Web. It also was integrated into certain versions of Microsoft Internet Explorer.

Connectivity Secure Shell 2008 builds on our experience with SOCKS by offering an integrated SOCKS client within the terminal.

Connectivity Secure Shell SOCKS client offers complete SOCKS support.

- SOCKS version 4 and 5 support
- Configurable port
- Ability to force local DNS lookup
- Support for username/password authentication
- Support for Kerberos authentication and encryption
  - Connectivity Kerberos client or MIT Kerberos client
  - Windows Kerberos ticket support

Figure 6 — HostExplorer SOCKS configuration dialog

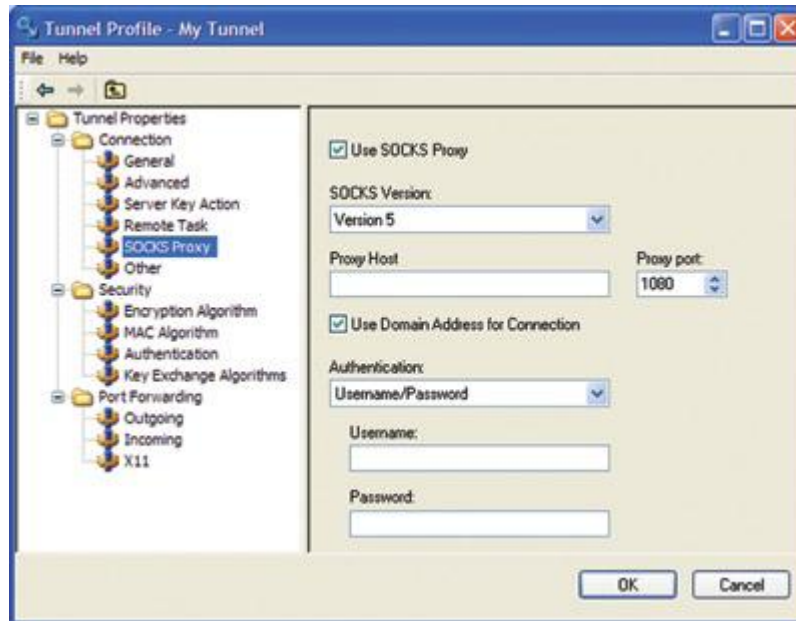
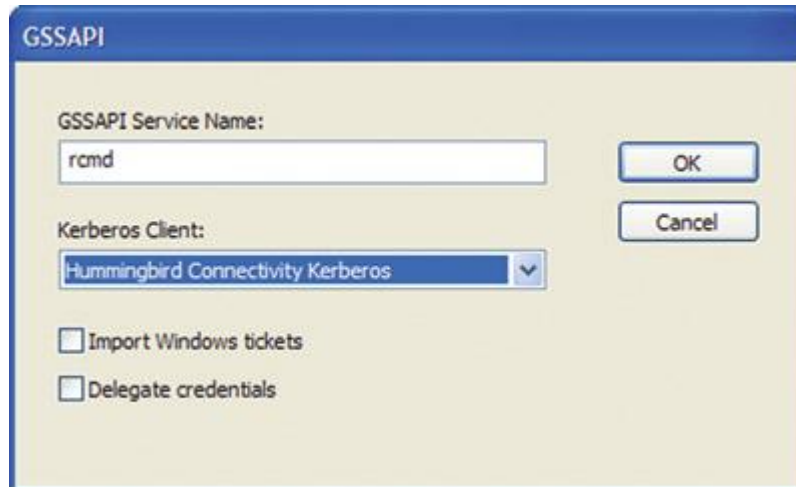


Figure 7 — SOCKS Kerberos authentication configuration dialog



## Additional Browser Support

For the past five versions, Hummingbird FTP for Windows Explorer, HostExplorer, Connectivity Secure Shell, and Connectivity SecureTerm had the ability to be deployed to Internet Explorer using the Hummingbird Deployment Wizard technology. Hummingbird Connectivity 2008 expands browser support to Firefox, Opera, and third-party Java-compatible browsers.

## SOCKS Dynamic Port Forwarding

Port forwarding is one of the most powerful capabilities of the SSH protocol. It allows third party applications data, which would normally be sent unencrypted over the network, to be secured through the SSH client. A good example of port forwarding is that of e-mails. Normally, e-mail client applications exchange data directly with e-mail servers. With an SSH client installed, the e-mail client can be reconfigured to route its data to the SSH client. The SSH client receives the incoming data, and once encrypted sends it to the SSH Server. Upon reception, the SSH server decrypts the data and forwards it to its original destination: the e-mail server.

Port forwarding could be the perfect solution to many problems if not for the inconvenience of changing the configuration of the client application as well as defining one port forwarding rule for each application that needs to be forwarded. On top of that, each application require a different port to communicate with the SSH client. SOCKS Dynamic Port Forwarding offers an elegant solution to this problem. Client applications that support SOCKS, can be instructed to use the SSH client as a SOCKS Server, therefore minimizing the disruption of the client application configuration. The SSH client, which becomes a local SOCKS server, only require one forwarding rule to be set up regardless of the number of applications that access it. Finally, all applications use the same port number (1080: the SOCKS port) to communicate with the SSH client.

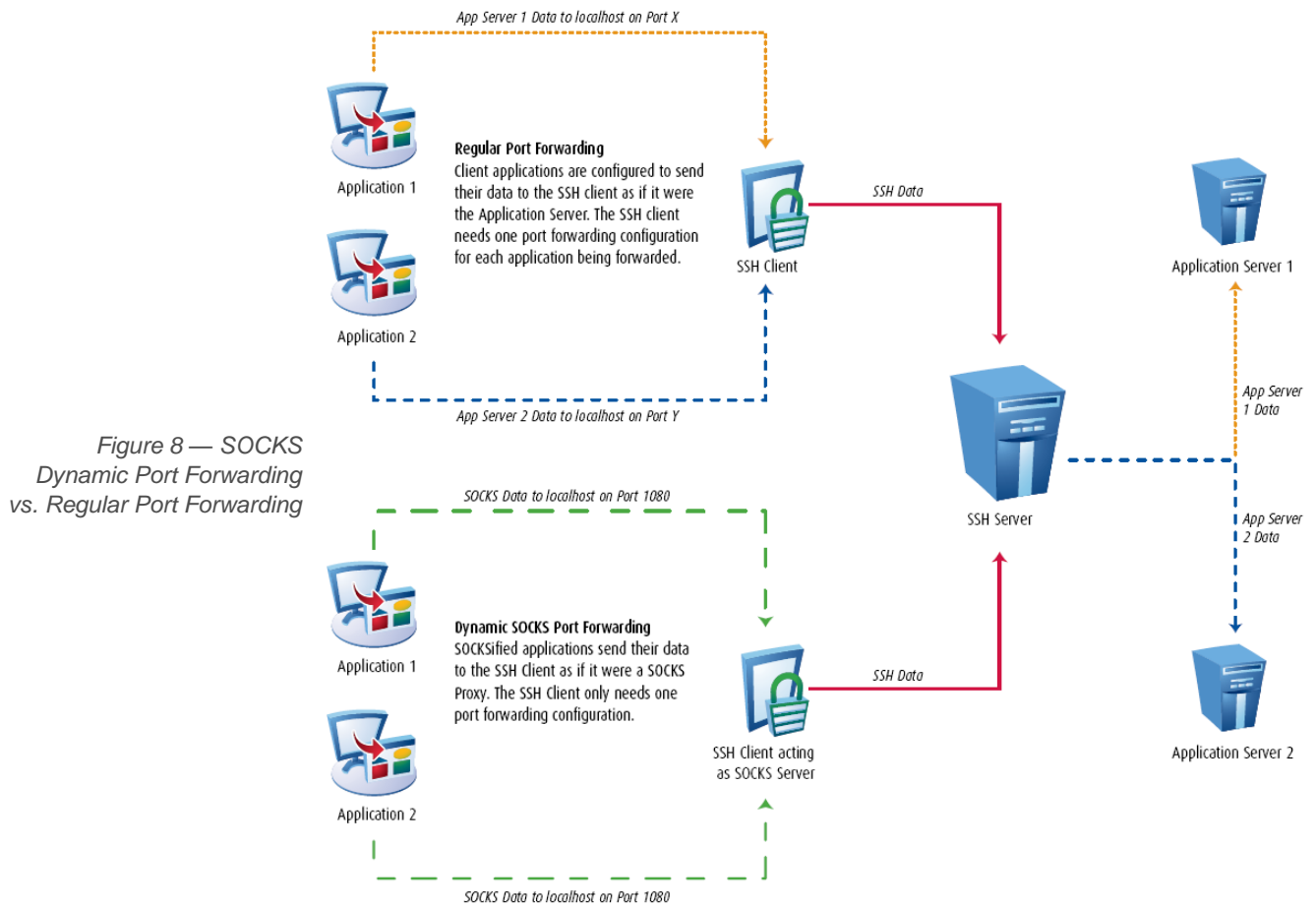


Figure 8 — SOCKS Dynamic Port Forwarding vs. Regular Port Forwarding

## Event Monitoring Server

For the past three versions, Hummingbird products have come with a built-in license metering functionality. With Hummingbird Connectivity 2008, we are taking metering one step further by introducing the Event Monitoring Server.

The Event Monitoring Server (EMS) is a robust and scalable facility designed to help administrators gather information about their Hummingbird infrastructure. EMS comes as a client/server architecture:

- The EMS Client is installed with every Hummingbird software package. Its role is to report installation and activity information to the EMS Server.

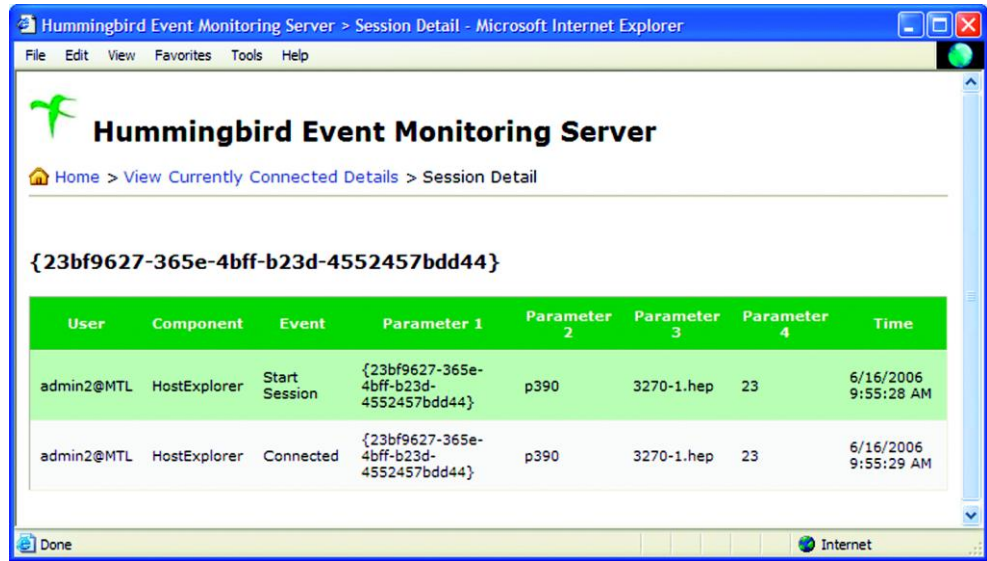
- The EMS Server comes as an ASP.NET application that runs on Microsoft Internet Information Server. Its role is to collect information from the EMS clients, store it in a relational database (SQL Server or MySQL), and to offer several administrative views to display that information.



Figure 9 — The EMS Server main page

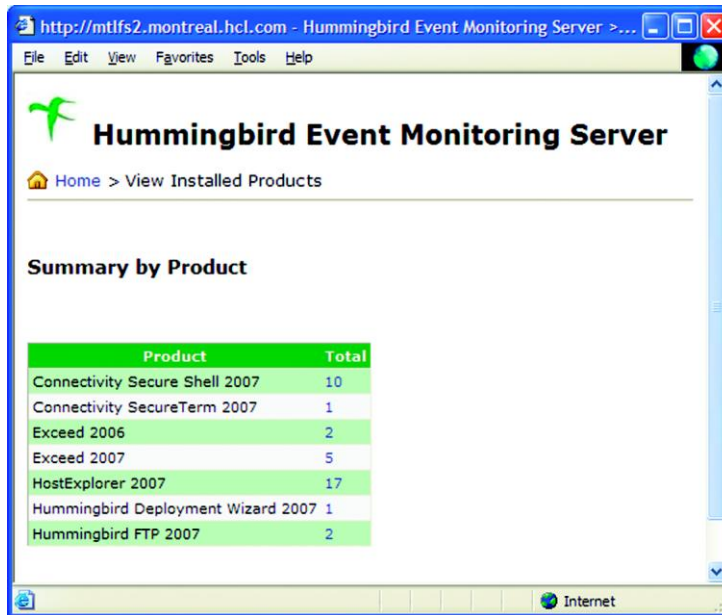
The EMS Server main screen provides administrator with the total number of active users and active sessions running. Administrators have the ability to drill down and isolate a specific user or machine in order to determine its activity.

Figure 10 — The EMS Server Session Detail.



Administrators also have the ability to see how many product licenses are installed on their network. Here again, the EMS Server offers the ability to drill down and identify the machines on which the products have been installed.

Figure 116 — Administrators have the ability to see how many licenses of the Hummingbird Connectivity software have been installed.







---

Sales & Support		Corporate Head Office
Canada 38 Leek Crescent, Richmond Hill, L4B 4N8 Phone: 905-762-6400 Fax: 905-762-6407 Toll Free: 1-877-359-4866	<a href="http://www.hummingbird.com">www.hummingbird.com</a> <a href="mailto:getinfo@hummingbird.com">getinfo@hummingbird.com</a> <a href="mailto:support@hummingbird.com">support@hummingbird.com</a> North America Support 1 800-486-0095 Worldwide Support 1-905-762-6400	<a href="http://www.opentext.com">www.opentext.com</a> <a href="mailto:sales@opentext.com">sales@opentext.com</a> North America Sales 1-800-499-6544 International Sales +800-4996-5440

If you are a Hummingbird partner or customer, visit [www.hummingbird.com](http://www.hummingbird.com) or [online.opentext.com](http://online.opentext.com) for more information about this and other Open Text solutions.

Open Text is a publicly traded company on the NASDAQ (OTEX) and the TSX (OTC).

Copyright © 2008 Hummingbird Ltd. All other trademarks or registered trademarks are the property of their respective owners. All rights reserved. Hummingbird, the Open Text Connectivity Solutions Group. Printed in Canada. WP-03-00-EN-146.02/08