



Citi Architecture and Technology Engineering

HDS - Remote Access Control Center (RACC)

CSBE-12020-SG

Solutions Guide

Version 1.0

Version Control

Version	Date	Author	Reviewed	Comments
0.1	18-Oct-2011	Kevin Hobaugh	CSBE	Peer Review
0.2	20-Oct-2011	Kevin Hobaugh	Global SAN Stakeholders	RFC
1.0	21-Nov-2011	Kevin Hobaugh	Global SAN Stakeholders	Production Release

Legal Notice

Information contained herein is for Internal Use and may be used only for business purposes authorized by Citigroup.

CITI, CITIBANK, CITICORP, CITIGROUP and the Umbrella Device are trademarks and service marks of Citicorp and are used and registered throughout the world. Citibank, Citicorp, Citigroup and their subsidiaries also claim rights in certain other trademarks and service marks contained in these pages.

Contact

Please address any comments or questions regarding the information contained in this document via email to the “*GT PSE Storage Platforms and Services” distribution list or alternatively to gdse@citi.com.

Latest Versions

It is recommended that the latest version of the document be used from the [CATE - Storage Engineering](#) website. Newer versions may include certification on additional platforms, or comments on issues discovered after deployment.

Table of Contents

1. INTRODUCTION.....	4
1.1. REMOTE ACCESS CONTROL CENTER (RACC) SERVER	4
1.2. ARCHITECTURE (HOW IT WORKS).....	5
2. PREREQUISITES.....	7
2.1. SITE INFORMATION	7
2.2. RACC SERVER REQUIREMENTS.....	7
2.3. SOFTWARE.....	7
2.4. FIREWALL RULES.....	7
2.4.1. CEP (INTERNAL FIREWALL).....	8
2.4.2. W2K8 LOCAL FIREWALL (INSTRUCTIONS LATER IN DOCUMENT)	8
2.5. VMWARE ESX SUPPORT STATEMENT	8
3. HI TRACK RACC INSTALLATION STEPS.....	8
3.1. IIS INSTALLATION.....	8
3.1.1. <i>Configure IIS</i>	9
3.2. RACC INSTALLATION	10
3.2.1. <i>F5 Network Installation</i>	10
3.3. HI TRACK RACC INSTALLATION	13
3.4. RUNNING RACC ON WINDOWS SERVER 2008 64-BIT	18
3.5. ENABLE REMOTE CONNECTIVITY SERVICES	18
3.6. ENABLE WINDOWS 2008 FIREWALL	19
3.7. UNINSTALL CASSINI WEB SERVER.....	21
3.8. CONFIGURE IIS HTTPS RATHER THAN HTTP	21
3.9. USER ACCESS RIGHTS.....	22
3.10. INSTALL SSH CLIENT AND/OR PUTTY (IF NOT ALREADY INSTALLED) ..	22
3.11. CONFIGURE HDS LOCAL USER ACCOUNT.....	22
4. HI TRACK RACC CONFIGURATION	23
4.1. USER ADMINISTRATION	23
4.2. NODE ID AND HDS SIGNAL SERVERS	24
4.3. ADD HDS SUPPORTED HARDWARE	25
4.4. W2K8 LOCAL FIREWALL RULES.....	26
4.5. RDP SETTINGS FOR LOCAL VENDOR ACCOUNT (OPTIONAL)	27
4.6. GRANTING HDS REMOTE ACCESS	30
5. APPENDIX A: REFERENCES AND RELATED DOCUMENTS.....	31
6. APPENDIX B: USE OF PROXY SERVER	31
7. APPENDIX C: REVISION HISTORY.....	31

1. Introduction

The Hi-Track RACC product provides a secure, IP-based remote access solution giving Citigroup control and visibility of remote support access. **The RACC solution provides remote support capability only.**

Call home alert notifications and heartbeats will continue to be serviced by Hi-Track using SMTP from the individual storage devices.

Simplicity – The RACC solution consolidates access points for HDS support by providing a uniform, standards-based architecture for remote access across HDS product lines. The benefits include:

- The elimination of modems and modem lines
- CitiVPN/DiaVPN connections
- Management of safeword tokens
- Storage Operations ability to control authorization of access for remote support events
- Consolidated logging of remote access for audit review

Improved Availability – Because the RACC solution is built and supported by HDS, problems can be resolved faster because a single vendor will now own all the pieces. Also because fewer components are involved the risk of remote access malfunction from mis-configuration of a component is reduced.

Security – The RACC solution fulfills CISS requirements for authentication, authorization and auditing.

- Digital security – RACC security includes SSL data encryption, entity authentication (private digital certificates), and remote access user authentication verified through HDS network security.
- Secure remote access session tunnels – RACC establishes a secure IP based remote session between the RACC server and HDS.

1.1. Remote Access Control Center (RACC) server

A Citi-supplied, dedicated Windows 2008 R2 64-bit server acts as the single point of entry and exit for all IP-based HDS remote support activity. The RACC is an SSL HTTP handler between the RACC server and HDS.

The RACC server will reside on the Citi Global Distributed Network (GDN). The RACC server queries HDS every few minutes to detect if any outstanding SSL Tunnel connection requests. Via this secure SSL Tunnel, an HDS support specialist can connect to the RACC server. From there he can connect to the HDS devices to provide support.

NOTE: The SSL Tunnel is initiated from Citi outbound to the HDS Hi-Track SSL Tunnel Appliance.

1.2. Architecture (How it works)

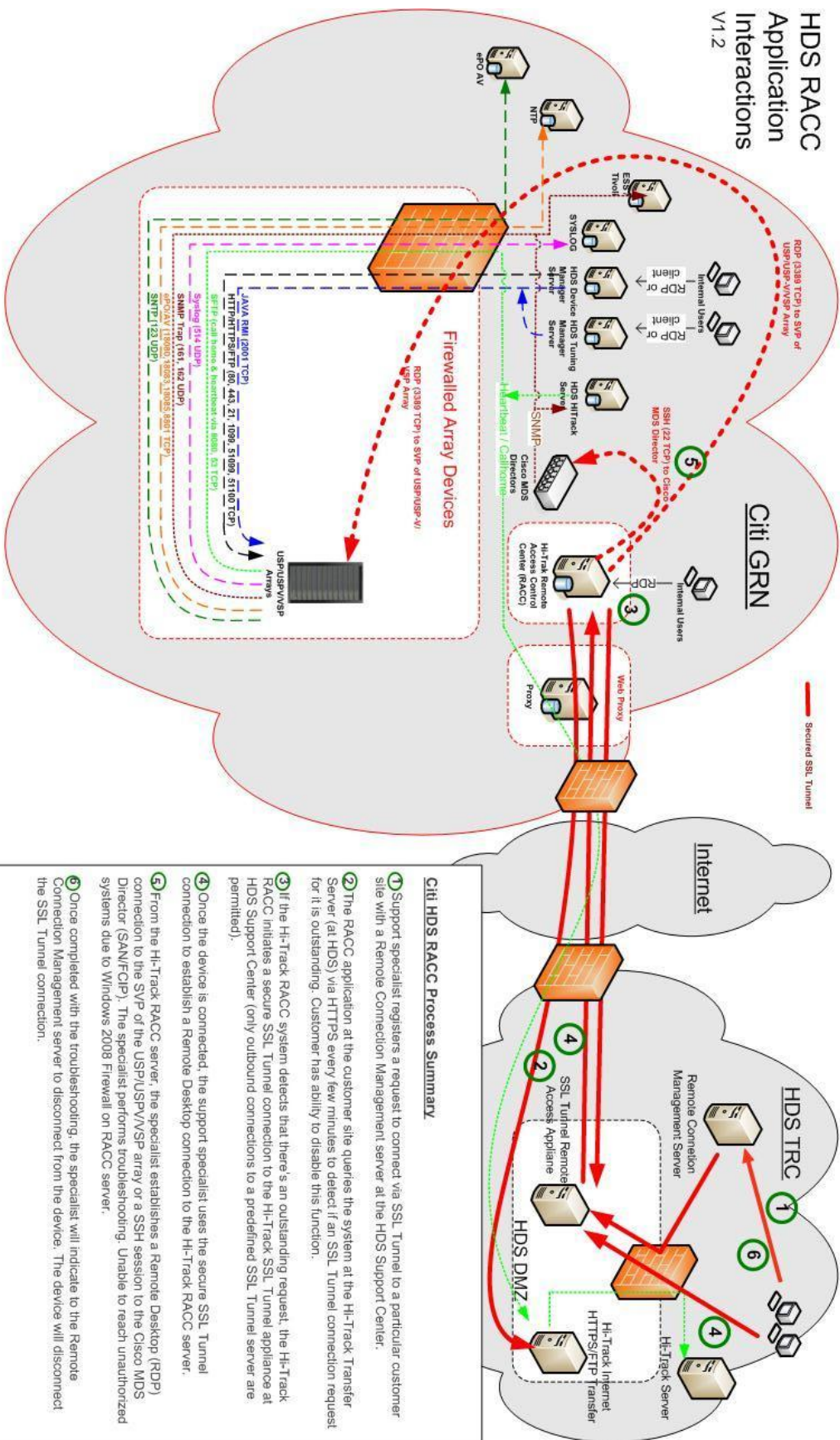
Hi-Track RACC enables HDS support personnel to request and establish a VPN connection from the computer running the Hi-Track RACC application inside Citi's network environment. Using the HTTPS protocol (secure HTTP), the RACC application periodically polls HDS servers to see if a connection is requested.

When HDS support personnel want to establish a remote support session, they browse to an internal HDS website called the Remote Access Web (RAW) server where they can request a connection from a specific site. When they request such a connection, the publicly accessible HDS servers wait for that site to poll. When it does, they respond with a command to establish a secure SSL Tunnel connection.

Once that SSL tunnel is established, the RACC application notifies the internal RAW server that the remote site has connected. The support person is then notified that the connection has been established and is provided with the IP address of the remote system hosting the RACC application.

With the SSL tunnel established, and the IP address of the remote system, the initiating support person may launch a Remote Desktop session back to the RACC server. From there, they may Remote Desktop or use SSH to connect to HDS devices for remote support. A Windows firewall is in place to only allow HDS to connect their storage devices. They are unable to "Leapfrog" to any other systems. Below is a diagram of the RACC environment.

**HDS RACC
Application
Interactions
V1.2**



2. Prerequisites

2.1. Site Information

- Site ID
- Storage products and serial numbers
- Citi Proxy Server IP address (obtain from *CATE Network – Perimeter)
- Storage and Cisco switch IP addresses

2.2. RACC Server Requirements

- Each region will have two HDS RACC servers (at different locations within the region) Every HDS RACC Server instance will have access to ALL HDS arrays globally (Distributed & MF). This is for redundancy and for "follow the sun" support
- Windows Server 2008 x64bit Standard Edition SP2 (without Hyper-V)
 - Server should be a member of the regional active directory domain
- Dual CPU (3.45 GHz recommended)
- 4GB Memory (8GB recommended)
- 60GB Hard Drive
- RACC server should reside on the Global Data Network (GDN) with access to HDS supported devices residing behind a firewall (CEP)
- Windows 2008 Firewall should be enabled. Turned off by default of Group Policy
- RACC is supported on VMWare
- SAN team (AD groups) should have local administrator privileges

2.3. Software

- Microsoft IIS (**CITI_Win_2K8_x64_IISBase_7_02**)
- .Net Framework 3.5
- Remote Desktop (RDP)
- SSH or Putty

2.4. Firewall Rules

There are two kinds of firewall rules to be set for RACC to work correctly. Since, the HDS storage devices and Cisco switches are behind a Citi Firewall (CEP) there a couple firewall rules to request for the CEP.

In addition, to prevent the HDS support personnel from "leapfrogging" off the RACC server onto a Citi device, the **Windows 2008 Firewall with Advanced Security** functionality is being configured on the Windows 2008 RACC Server. These rules will lockdown the HDS support personnel to ONLY certain ports. Third the RACC software

itself has a “Manage Outbound Connections” configuration. This is where the HDS storage and switching devices IP addresses are configured. These IP addresses are the only IP addresses accessible from the RACC server. Only Citi storage administrators have access to web client to configure RACC.

2.4.1. CEP (Internal Firewall)

- **RDP** port 3389 (from RACC server to HDS Array in DMZ)
- **SSH** port 23 (from RACC server to HDS supported Cisco devices)

2.4.2. W2K8 Local firewall (instructions later in document)

- **Webproxy** port 8080
- **SSH** port 23
- **RDP** port 3389
- **SMTP** mail server port 25
- **Routing and Remote Access** port 1723
- **EPO/McAfee** updates (ports x,y,z)

2.5. VMware ESX Support Statement

HDS supports Hi-Track RACC on a VMware ESX Server.

GDSE does not recommend installing RACC on ESX servers which reside on SAN attached storage. Reasoning: If the SAN storage or the SAN were to go down, then RACC would not function and HDS would be unable to connect remotely to provide support. For this reason, GDSE recommends that RACC be installed on ESX running on NAS storage where available.

3. Hi Track RACC Installation Steps

- Install IIS
- Install Hi-Track RACC v1.2
 - Install F5 Network
 - Install Hi-Track RACC
- Configure RACC

3.1. IIS Installation

Install the IIS TPM package (**CITI_Win_2K8_x64_IISBase_7_02** or latest package) on each RACC Server. Configure The IIS default installation will require configuration to allow RACC to use IIS instead of its integrated web server.

3.1.1. Configure IIS

This procedure permits RACC to be hosted on a web server that supports HTTPS and can include customer provided certificates to allow the customer flexibility in the installation.

NOTE: Administrator rights on the host server will be needed to follow these steps.

1. Configure applicationHost.config file

Browse to “C:\Windows\System32\inetsrv\config” (you will need administrator rights here)

Open applicationHost.config

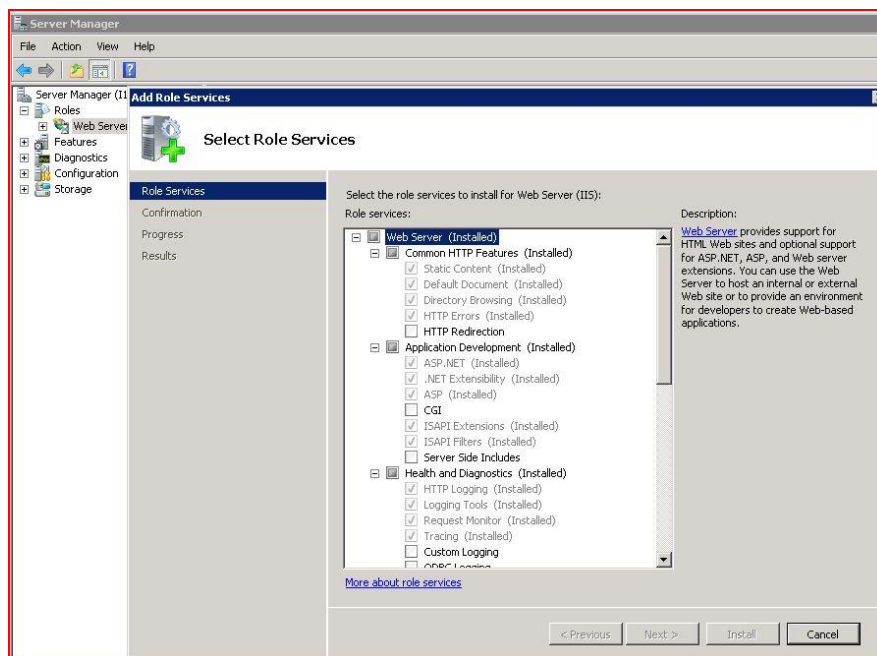
2. For **Modules** and **Handlers** sections only, change the **overrideModeDefault** attribute to “Allow”

```
<section name="handlers" overrideModeDefault="Allow" />
```

```
<section name="modules" allowDefinition="MachineToApplication" overrideModeDefault="Allow" />
```

3. Verify the ASP.NET service is installed

- Open server manager : *Start -> All Programs -> Administrative Tools -> Server Manager*
- In Web Server (IIS) Role, right click on Web Server (IIS), click on **Add Role Services**



- If ASP.NET service is not installed, select it from the list and install it

3.2. RACC Installation

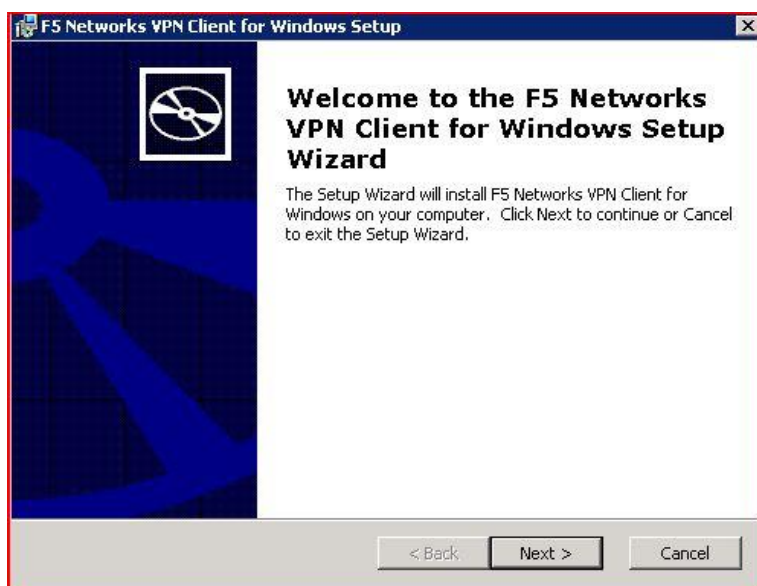
Install TPM package for HDS RACC v1.2 (**CITI_WIN_2K8_x64_HDSRACC_44492_01**).
Note: The package does not install the software. It copies the install files to **c:\HDSRACC** for Operations/Integrations (with HDS CE assistance) to perform a manual install.

3.2.1. F5 Network Installation

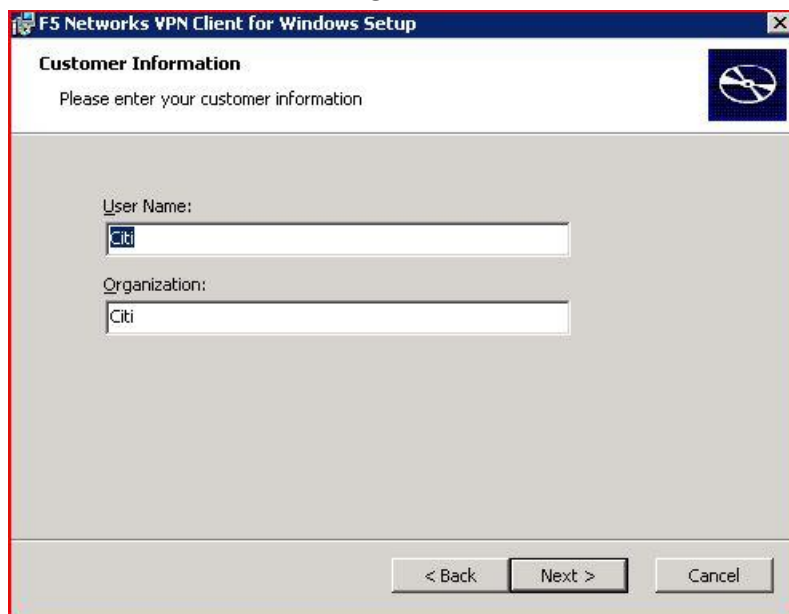
1. Install the **F5 Network software** (run: “**Setup.exe**” from c:\HDSRACC)
2. Select **Install F5 components**



3. Click **Next** to continue.

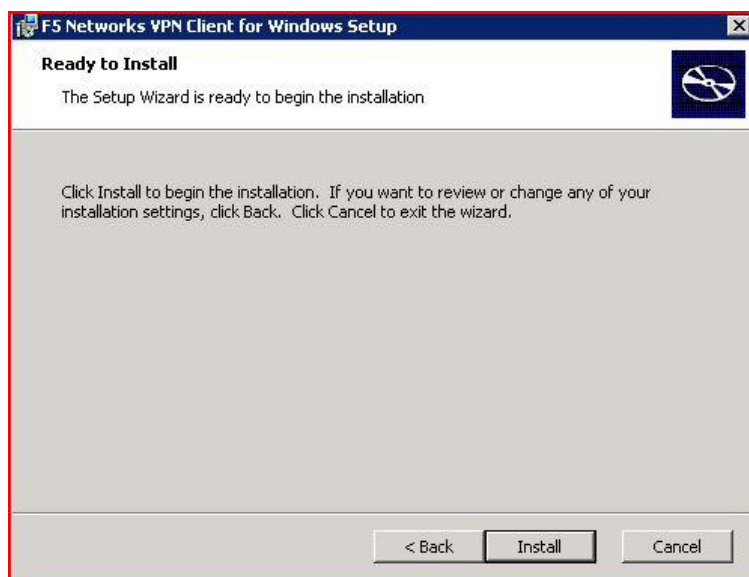


4. Enter **User Name** and **Organization**



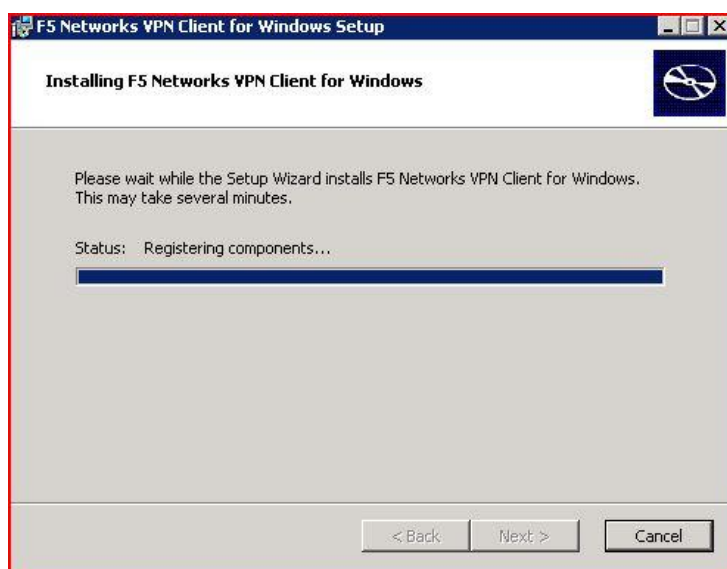
The screenshot shows the 'F5 Networks VPN Client for Windows Setup' window. The title bar includes the F5 logo and the text 'F5 Networks VPN Client for Windows Setup'. The window has a standard Windows XP-style title bar with minimize, maximize, and close buttons. The main content area is titled 'Customer Information' and contains the instruction 'Please enter your customer information'. Below this, there are two text input fields. The first field is labeled 'User Name:' and contains the text 'Citi'. The second field is labeled 'Organization:' and also contains the text 'Citi'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted, indicating it is the next step in the wizard.

5. Click **Install**



The screenshot shows the 'F5 Networks VPN Client for Windows Setup' window. The title bar includes the F5 logo and the text 'F5 Networks VPN Client for Windows Setup'. The window has a standard Windows XP-style title bar with minimize, maximize, and close buttons. The main content area is titled 'Ready to Install' and contains the instruction 'The Setup Wizard is ready to begin the installation'. Below this, there is a paragraph of text: 'Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.' At the bottom of the window, there are three buttons: '< Back', 'Install', and 'Cancel'. The 'Install' button is highlighted, indicating it is the next step in the wizard.

The installation will begin after you select Install button.



6. Click **Finish** to complete the install.



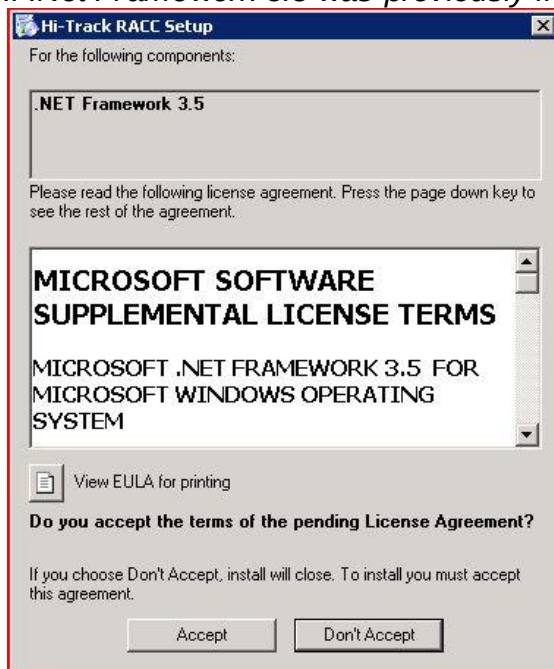
3.3. Hi Track RACC Installation

1. Select Install Hi-Track RACC application



2. .Net Framework 3.5 EULA. Click **Accept**.

If .Net Framework 3.5 was previously installed, you will not get this dialog box.

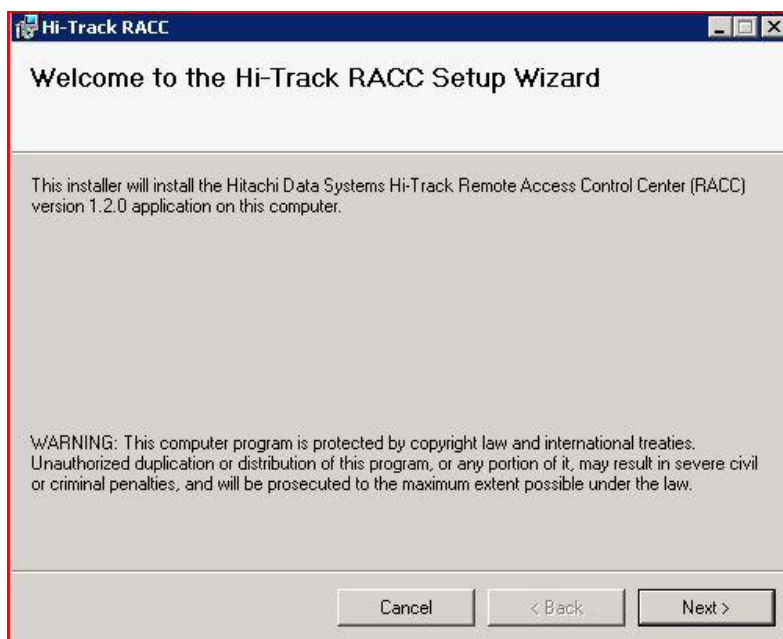


Microsoft .Net Framework 3.5 gets installed

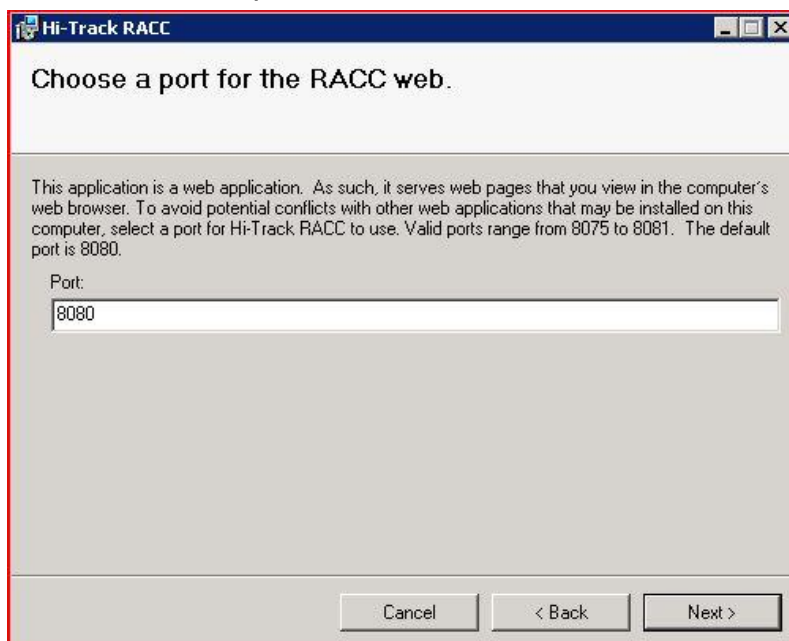
3. Click **Install** (Cassini Web Server will be uninstalled later)



4. Click **Next**



5. Leave default port **8080**



The image shows a Windows-style dialog box titled "Hi-Track RACC". The main heading is "Choose a port for the RACC web.". Below this, a paragraph of text explains that the application is a web application and provides instructions on selecting a port between 8075 and 8081, with 8080 as the default. A text input field labeled "Port:" contains the value "8080". At the bottom, there are three buttons: "Cancel", "< Back", and "Next >".

Hi-Track RACC

Choose a port for the RACC web.

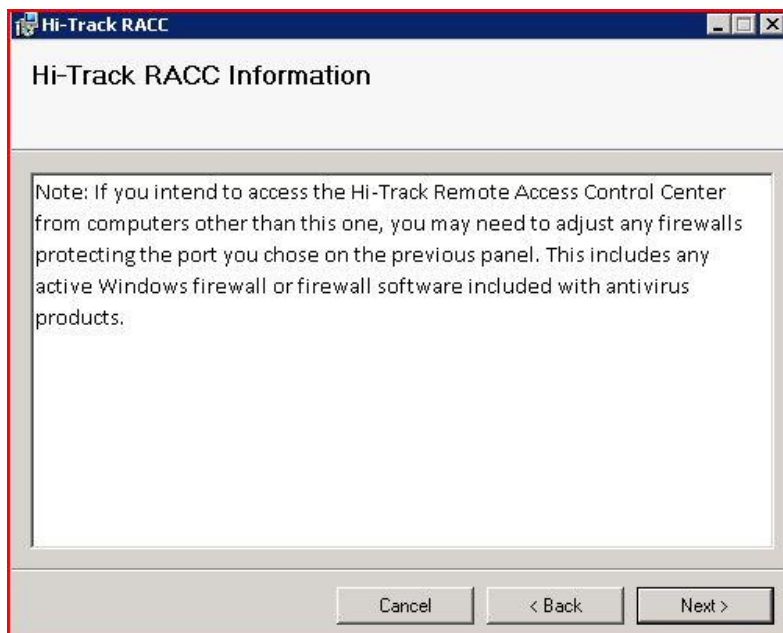
This application is a web application. As such, it serves web pages that you view in the computer's web browser. To avoid potential conflicts with other web applications that may be installed on this computer, select a port for Hi-Track RACC to use. Valid ports range from 8075 to 8081. The default port is 8080.

Port:

8080

Cancel < Back Next >

6. Click **Next**



The image shows a Windows-style dialog box titled "Hi-Track RACC". The main heading is "Hi-Track RACC Information". Below this, a text area contains a note about adjusting firewalls. At the bottom, there are three buttons: "Cancel", "< Back", and "Next >".

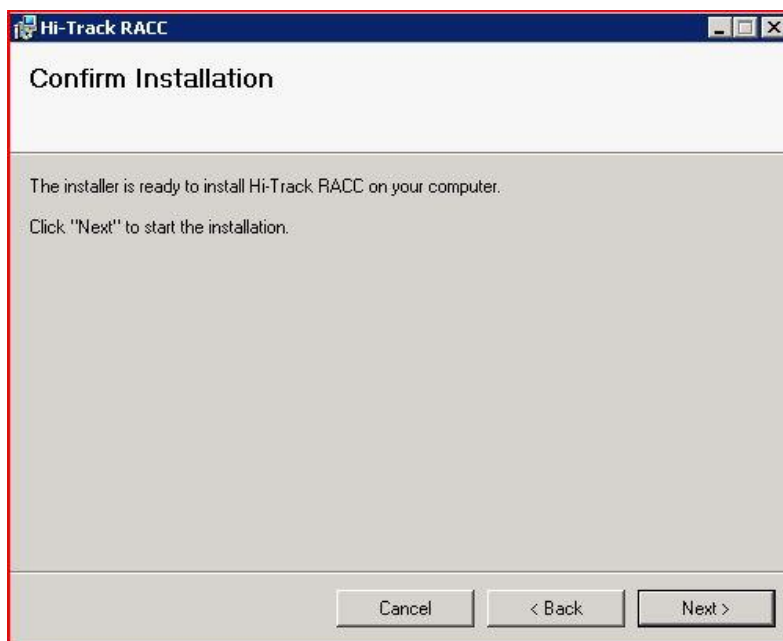
Hi-Track RACC

Hi-Track RACC Information

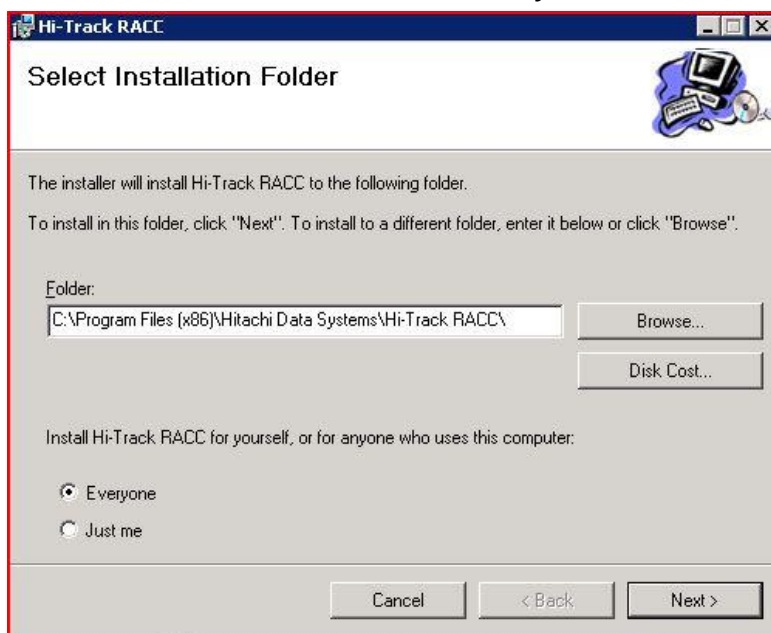
Note: If you intend to access the Hi-Track Remote Access Control Center from computers other than this one, you may need to adjust any firewalls protecting the port you chose on the previous panel. This includes any active Windows firewall or firewall software included with antivirus products.

Cancel < Back Next >

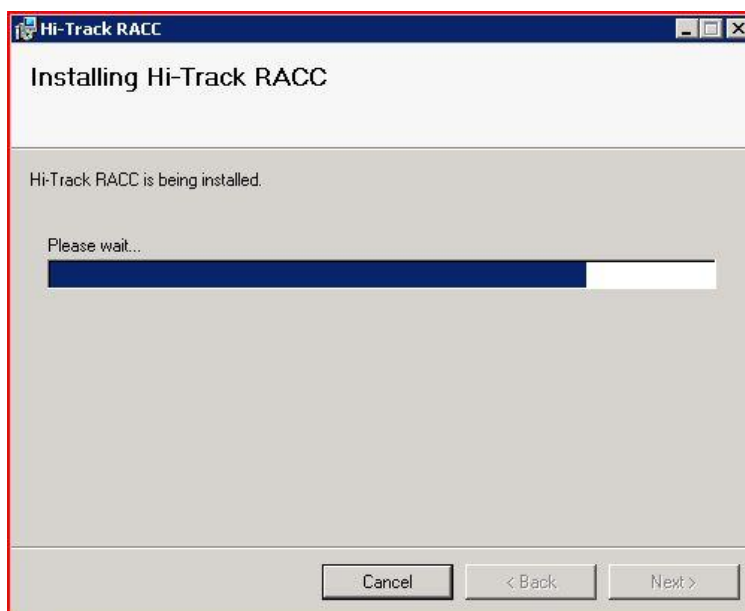
7. Confirm Installation, click **Next**



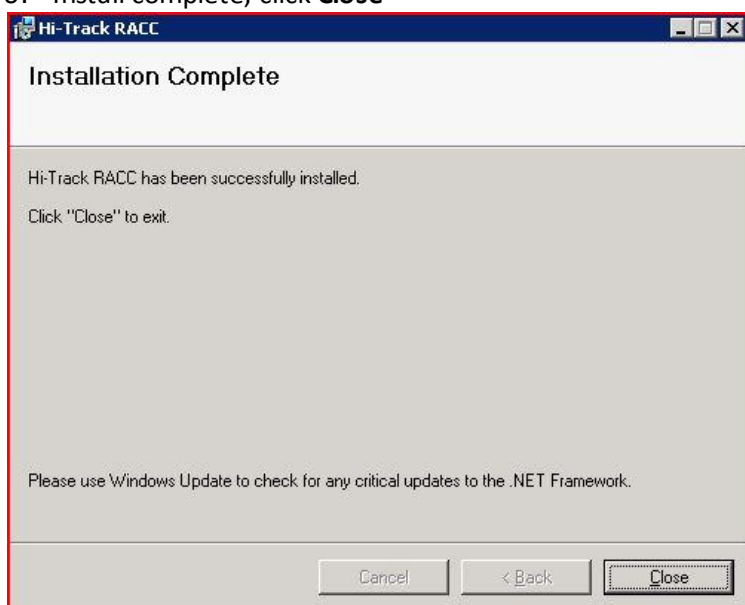
8. Select the drive, leave the directory default and click **Next**



RACC installing....



9. Install complete, click **Close**



10. Exit install by clicking **Exit**.



3.4. Running RACC on Windows Server 2008 64-bit

In order to use the built in Windows Advanced Firewall, it requires us to run on Windows 2008 which is a 64 bit version. RACC is a 32 bit application. To run the RACC application on Windows Server 2008 64-bit server, the RACC application requires the 32 bit corflags to be set. CATE Storage and Backup Engineering modified the corflags to force the RACC service to run in 32-bit mode and included the updated RACC executable in the installation package. The following instructions explain how to replace the installed HiTrackRACC.exe with the modified version.

1. Stop the HDS RACC service "**Hi-Track Remote Access Control Center**".
2. In directory "*Drive:\Program Files (x86)\Hitachi Data Systems\Hi-Track RACC\Bin*", rename the Application file **HiTrackRACC.exe** to **HiTrackRACC_old.exe**.
3. Copy the 32bit version of **HiTrackRACC.exe**
From: *Drive:\HDSRACC\RACC1.2_SetupImage\Racc_exe-Corflags set*
To: "*Drive:\Program Files (x86)\Hitachi Data Systems\Hi-Track RACC\Bin*".
4. Start the HDS RACC service "**Hi-Track Remote Access Control Center**".

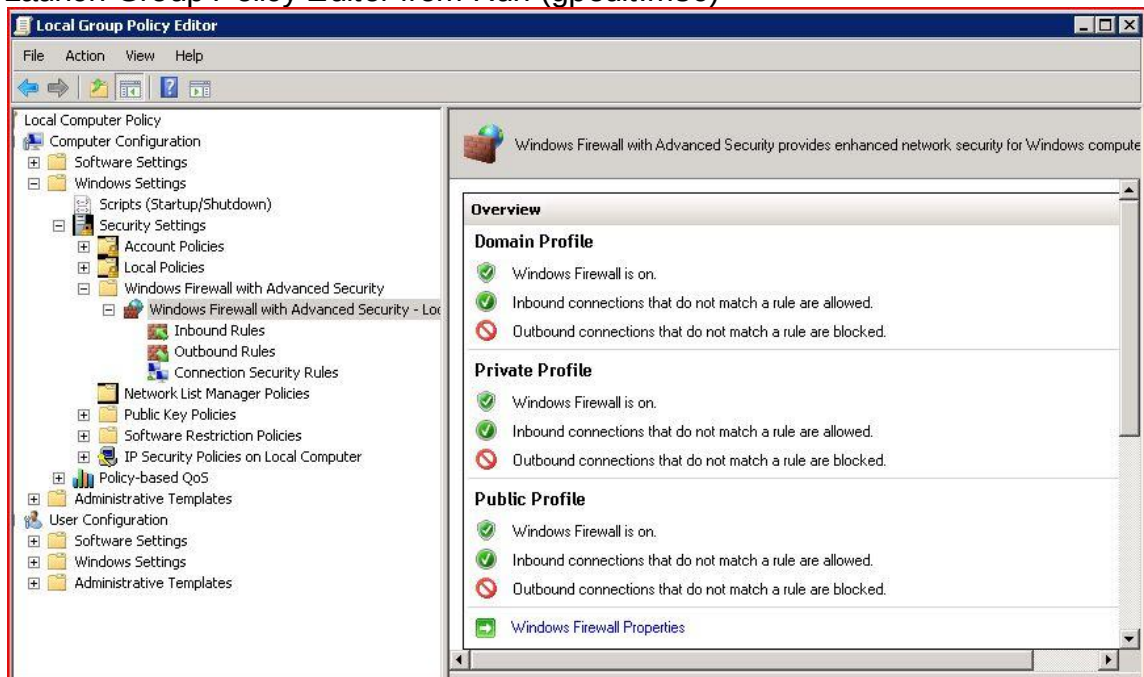
3.5. Enable Remote Connectivity Services

1. Telephony --> Automatic, Start
2. Remote Access Connection Manager-- > Automatic, Start
3. Remote Access Auto Connection Manager--> Automatic, Start

3.6. Enable Windows 2008 Firewall

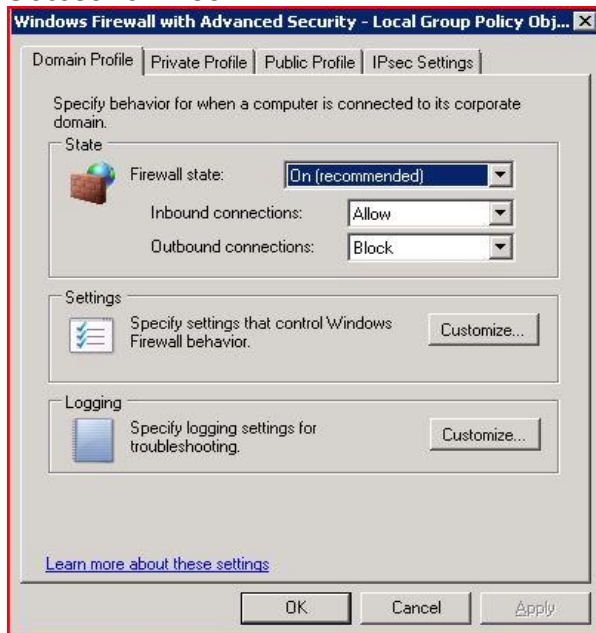
The Windows 2008 Firewall will allow Storage Operations to configure the firewall on the Citi SOE server to prohibit HDS support personnel from “leapfrogging” off the RACC server to another Citi owned servers. By default the Citi SOE Server build has a Group Policy that disables the W2K8 Firewall. Follow these steps to disable the group policy, thus enabling the firewall (inbound = allow, outbound = block).

1. Launch Group Policy Editor from Run (gpedit.msc)



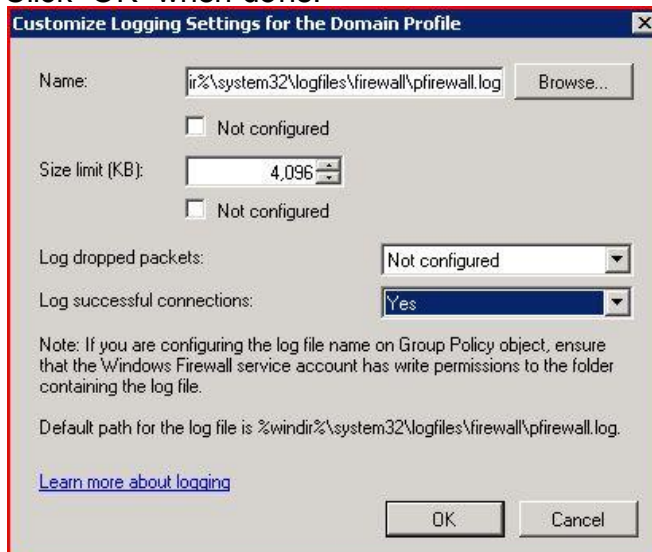
2. Expand: Computer Configuration \ Windows settings \ security settings \ Windows Firewall w/Advanced Security \ Windows Firewall with Advanced Security – Local Group Policy Obj.
3. Click on “Windows Firewall Properties” at bottom right of screen.

- Set the Domain \ Private \ Public Profiles to Firewall State: ON, Inbound: Allow, Outbound: Block.



- Set Logging for Firewall. Click Customize, and set as follows. Do this for Domain / Private / Public Profiles.

Uncheck the "Not Configured" boxes. Leave default settings
 Select "Yes" for "Log successful connections:"
 Click "OK" when done.



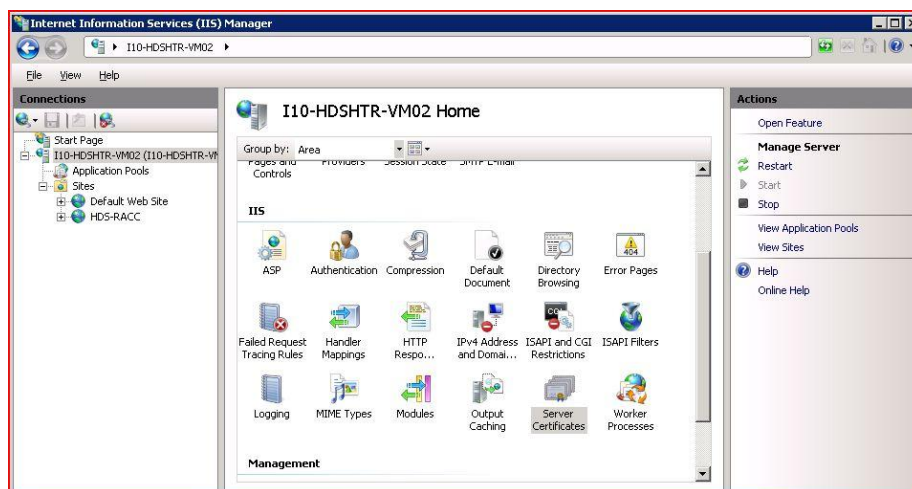
3.7. Uninstall Cassini Web Server

Hi Track RACC installs the “Cassini Web Server” by default. Since Microsoft IIS is the preferred web server and was installed earlier, the Cassini Web Server is not needed. This section explains how to uninstall the different pieces of Cassini.

1. Browse to *Start -> Control Panel -> Programs and Features*
2. Uninstall the following two programs
 - UltiDev Cassini Web Server Explorer
 - UltiDev Cassini Web Server for ASP .NET 2.0 (it closes ASP.Net and will restart it after uninstall is complete)

3.8. Configure IIS HTTPS rather than HTTP

1. Open IIS Manager: *Start -> Administrative Tools -> Internet Information Services (IIS) Manager*
2. Manage certificates
 - Navigate to the web server and double click **server certificates** in the **Features** view



- Use the options in the **Action** pane to import an existing certificate or **create a self-signed** one as appropriate
 - Click “**Create a Self-Signed Certificate**”
 - Name the certificate “**HDS-RACC**”
- 3. Add New Site
 - Right click on **Sites** and select **Add Web Site...** to open the Add Web Site Wizard

- Assign a name to the site (IE: HDS-RACC)
- Enter directory **C:\Program Files (x86)\Hitachi Data Systems\Hi-Track RACC**
- Set the **Binding Type** to **https**, leave the **IP address** and the **Port** fields in their default values or change them as appropriate
- For the **SSL Certificate**, select the certificate you created above **HDS-RACC**.
- Click “**OK**” to add the site.

3.9. User Access Rights

For the RACC software to work properly, the “USERS” group account requires “Write” access to the RACC directory.

1. Browse to **C :\Program Files (x86)\Hitachi Data Systems**
2. Open folder properties, select the security tab, and give write permission to USERS account

3.10. Install SSH Client and/or Putty (if not already installed)

3.11. Configure HDS Local User Account

HDS Support personnel will require a local user account on the RACC server. When HDS connects via RACC they will login to the RACC server. From the RACC server, they will connect to the HDS supported device.

1. Create a local account (example: **hdssupport**) as a local user with membership in the “**Remote Access**” user group.

4. Hi Track RACC Configuration

RACC needs to be configured with Users, Node ID for communication back to HDS Support Servers and HDS managed devices.

Login to the RACC web portal: <https://localhost:443> Use the default administrator ID until all the SOE User ID's are added into RACC. Currently, RACC doesn't support LDAP/s or Active Directory (Local RACC accounts only).

Note: *Default Administrator ID and Password will be provided separately or by HDS.*

4.1. User Administration

Local RACC users can be assigned to one of the following groups. HDS Support personnel DO NOT have ID's for RACC. They are not allowed, nor do they need access to the RACC software. Only Storage personnel should be able to login to the RACC system.

- **Viewers** group: Do not have permissions sufficient to change anything in the application. They can only view the current status, current configuration, or view log files. However they cannot view the User Mgmt page or see a list of defined users.
- **Users** group: Can also view status and configuration information, but they can also enable and disable polling (including terminating an open connection).
- **Administrators** group: Can specify configuration information or perform User Mgmt functions such as adding users or changing passwords.

Click on the “**Users**” tab to add users and to select their group assignment.

Current Users

User	Group	Actions
Administrator	Administrators	change password

Add a New User

Username

Password

Confirm password

Group

4.2. Node ID and HDS Signal Servers

Click on the “**Configuration**” tab to configure:

- Node ID
- Signal Servers
- Connection Points
- Proxy Server.

Note: These settings may be different for your Region. Contact HDS for assistance.

Hi-Track Remote Access Configuration

Node ID

Signal servers

Connection points

Web Proxy Information (if required)

Use proxy server: ☒

Address:

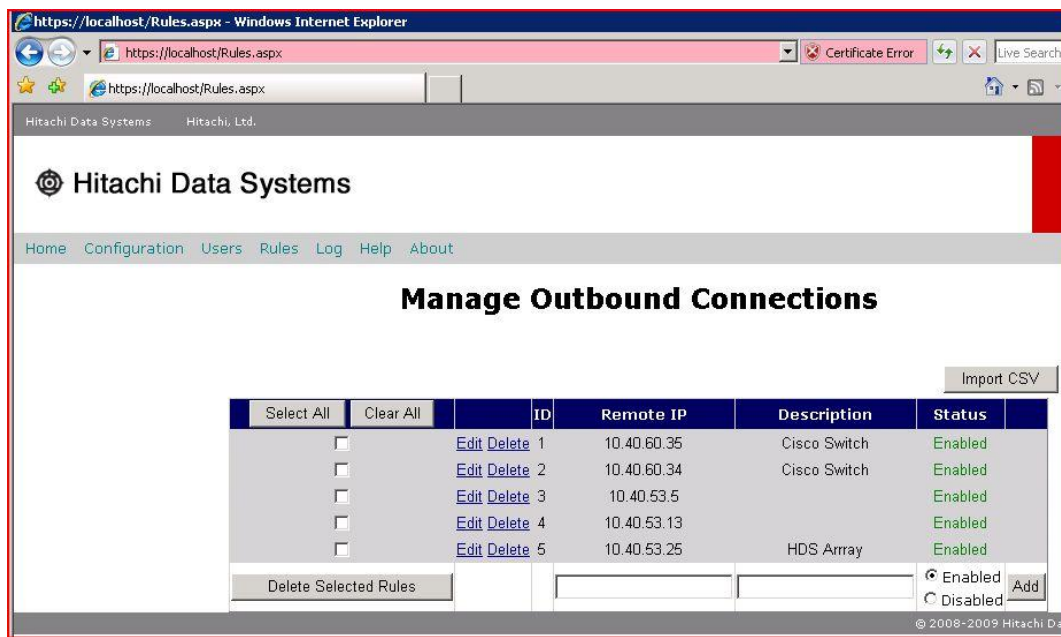
Port:

Username: (if required)

Password:

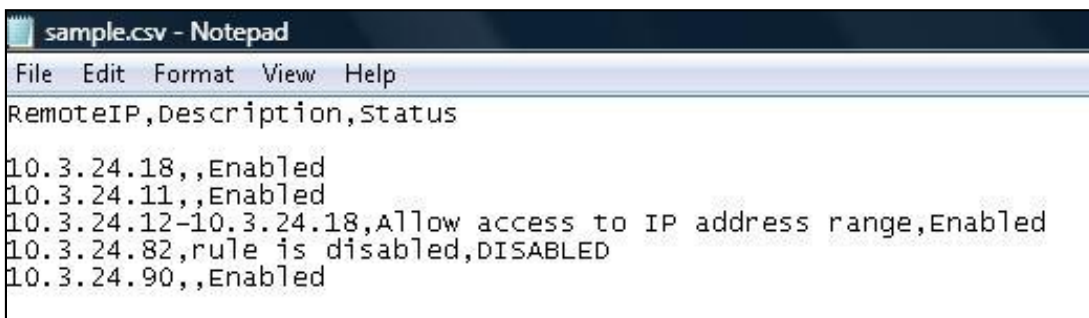
4.3. Add HDS Supported Hardware

From the RACC web interface, click on “**Rules**” to add HDS supported hardware. There should be an entry for each SVP and Cisco switch that will need to be supported by HDS.



In addition to creating "allow-connection" rules using the **Manage Outbound Connections** Table (above), users can **import them from a CSV file** by clicking on the Import CSV button. It is important to note that the Hi-Track RACC application does not perform any format validation on the supplied CSV file. Therefore, it is the end-user's responsibility to ensure that the content of a CSV file is well-formatted.

The following image represents an example of a well-formatted CSV file. The first line is the header identifying the three components of a rule while the second line is blank. The rest of the file consists of outbound rules to be added.



In addition, the definitions in the RACC configuration also need to be added to the rules list in RACC to prevent polling timeouts.

Hitachi Data Systems

Home Configuration Users Rules Log Help About

Hi-Track Remote Access Configuration

Node ID: R051419

Signal servers: ushtinet01.hds.com, ushtinet02.hds.com

Connection points: ushttrmt01.hds.com, ushttrmt02.hds.com, ushttrmt03.hds.com

The Signal Server and Connection Point IP addresses need to be entered into **Manage Outbound Connections** Table.

Manage Outbound Connections						
						Import CSV
Select All	Clear All		ID	Remote IP	Description	Status
☐		Edit Delete	1	207.126.240.71	ushtinet02.hds.com	Enable
☐		Edit Delete	2	207.126.254.52	ushtinet01.hds.com	Enable
☐		Edit Delete	3	207.126.254.64	ushttrmt03.hds.com	Enable
☐		Edit Delete	4	207.126.240.89	ushttrmt02.hds.com	Enable
☐		Edit Delete	5	207.126.248.27	ushttrmt01.hds.com	Enable

4.4. W2K8 Local Firewall Rules

The local Windows 2008 Firewall with Advanced Security will lock this server down. Certain ports are required to be opened to allow for RACC network traffic back to the HDS support servers, RDP (Remote Desktop), SMTP mail and others.

Add these rules and any others that might be required. You'll notice it will have the rules for the HDS hardware added previously from the RACC configuration steps.

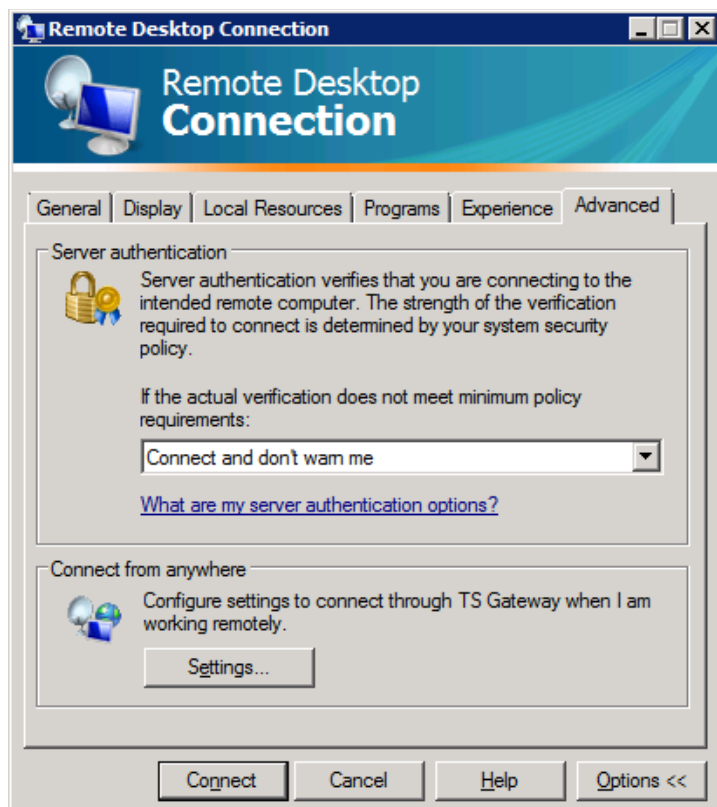
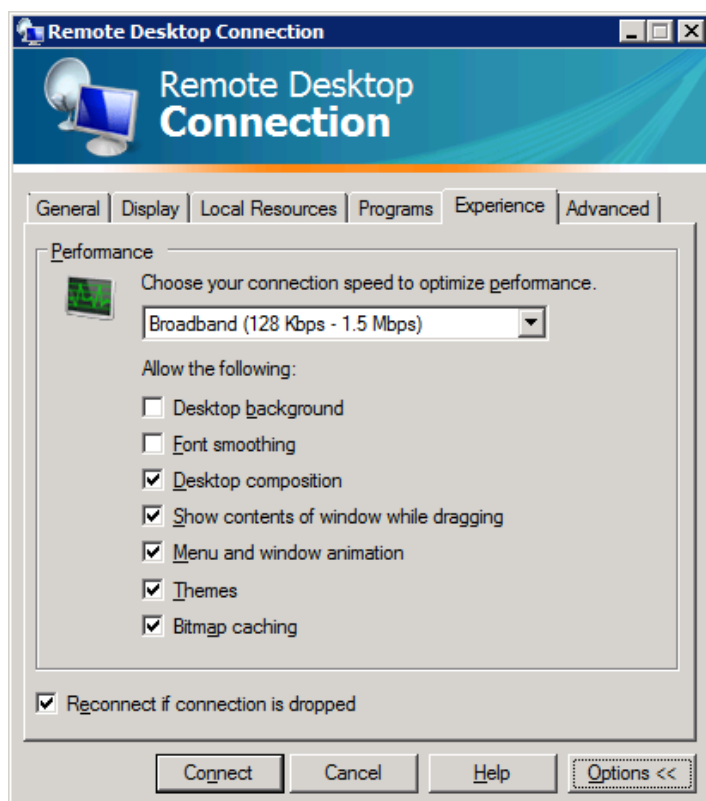
1. Browse to: Start -> Administrative Tools -> **Windows 2008 Firewall with Advanced Security**

2. **Webproxy** (port 8080 TCP) for domain,public,private (Outbound)
3. **SSH** (port 23 TCP) for domain,public,private (Outbound)
4. **RDP** (port 3389 TCP) for domain,public,private (Outbound)
5. **SMTP** mail server (port 25 TCP) for Dom/Pub/Priv (Outbound)
6. **Routing and Remote Access(PPTP-Out)** (port 1723 TCP) for Dom/Pub/Priv (Outbound)
7. **EPO/McAfee** updates (ports x,y,z) for domain,public,private (Outbound)

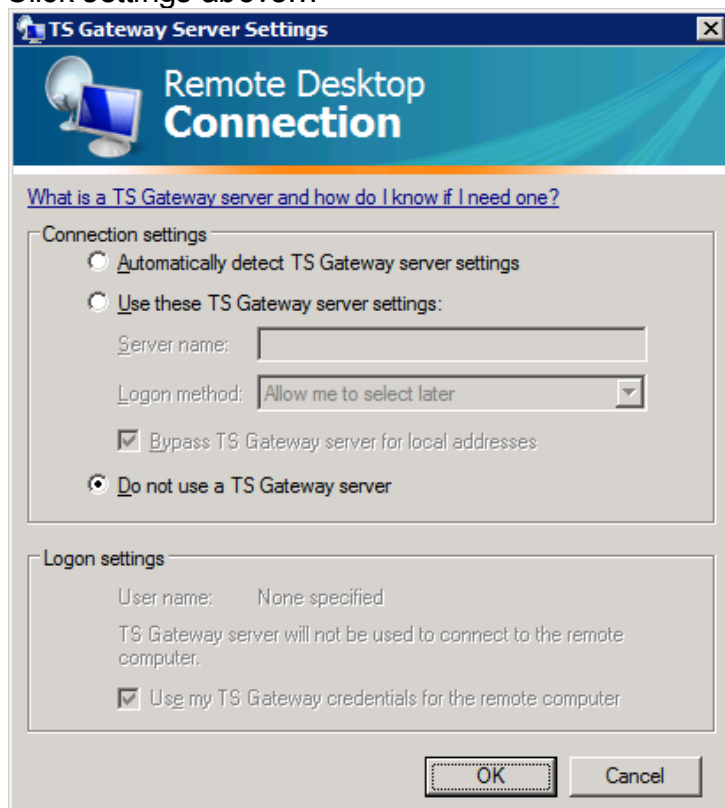


4.5. RDP Settings for Local Vendor Account (Optional)

These settings are optional, but do improve performance for the HDS remote connection. HDS will need to make these modifications when they login with their local account.



Click settings above...



The screenshot shows the 'TS Gateway Server Settings' dialog box. The title bar reads 'TS Gateway Server Settings'. The main header area has a blue background with a computer icon and the text 'Remote Desktop Connection'. Below this, there is a link: 'What is a TS Gateway server and how do I know if I need one?'. The 'Connection settings' section contains four radio buttons: 'Automatically detect TS Gateway server settings', 'Use these TS Gateway server settings:', 'Bypass TS Gateway server for local addresses' (checked), and 'Do not use a TS Gateway server' (selected). The 'Use these TS Gateway server settings:' option has a text field for 'Server name:' and a dropdown for 'Logon method:' with 'Allow me to select later' selected. The 'Logon settings' section shows 'User name:' as 'None specified', a message 'TS Gateway server will not be used to connect to the remote computer.', and a checked checkbox 'Use my TS Gateway credentials for the remote computer'. At the bottom are 'OK' and 'Cancel' buttons.

TS Gateway Server Settings

Remote Desktop Connection

[What is a TS Gateway server and how do I know if I need one?](#)

Connection settings

☐ Automatically detect TS Gateway server settings

☐ Use these TS Gateway server settings:

Server name:

Logon method:

☒ Bypass TS Gateway server for local addresses

☒ Do not use a TS Gateway server

Logon settings

User name: None specified

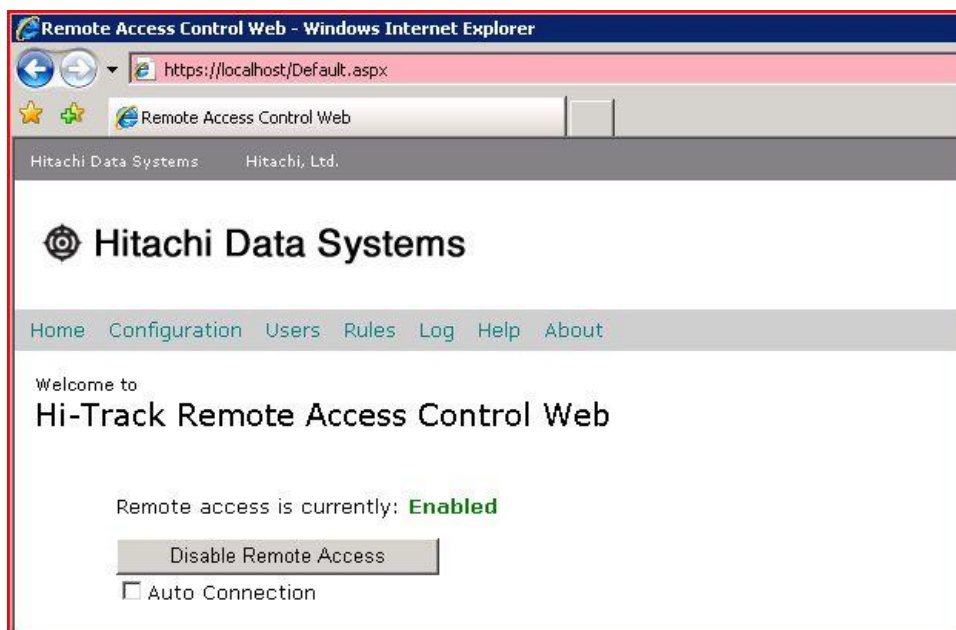
TS Gateway server will not be used to connect to the remote computer.

☒ Use my TS Gateway credentials for the remote computer

OK Cancel

4.6. Granting HDS Remote Access

Just like our other vendors, HDS is “Always Allowed” to connect to the RACC Server to provide remote support of their storage devices. To “Always Allow” HDS Support personnel to connect to their arrays, the “**Auto Connection**” check box should be checked and leave RACC always “**Enabled**” for remote access. This is configured from the “**Home**” tab.



5. Appendix A: References and Related Documents

Document	Location
HDS RACC – Release Notes	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/tagmastore.aspx
GDSE HDS website	https://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/tagmastore.aspx
GDSE Cisco MDS Switch website	http://catecollaboration.citigroup.net/domains/platstor/gdse/products/techstdshmpgs/ciscomds.aspx
Cate Storage and Backup Engineering Website	http://catecollaboration.citigroup.net/domains/platstor/gdse/products/default.aspx

6. Appendix B: Use of Proxy Server

The Hi Track RACC Server solution supports the use of a proxy server for routing outbound Internet traffic from the RACC servers to HDS. During installation, the RACC system is configured with the Citi Proxy address. The proxy server will then direct traffic from the RACC Server through the external firewall. All communication between RACC and HDS is initiated by the RACC Server at the Citi site over SSL via our Citi Proxy server.

7. Appendix C: Revision History

1.0 - Date: 11-Apr-2012

- Initial release of HDS Hi Track Remote Access Control Center (RACC)