Host Gateway Server

Installation and Deployment Guide

For Version 3.x

Revised 10/28/2010

Table of Contents

Table of Figures

Table of Tables

Introduction

Host Gateway Server, a Microsoft .NET Framework-based application from KMSYS Worldwide, Inc., provides encrypted and authenticated connections for client applications that utilize Unisys UTS Terminal protocol. It allows enterprises to provide secure connections to and from the Unisys mainframes without the expense, complexity and user training issues of a typical VPN solution.

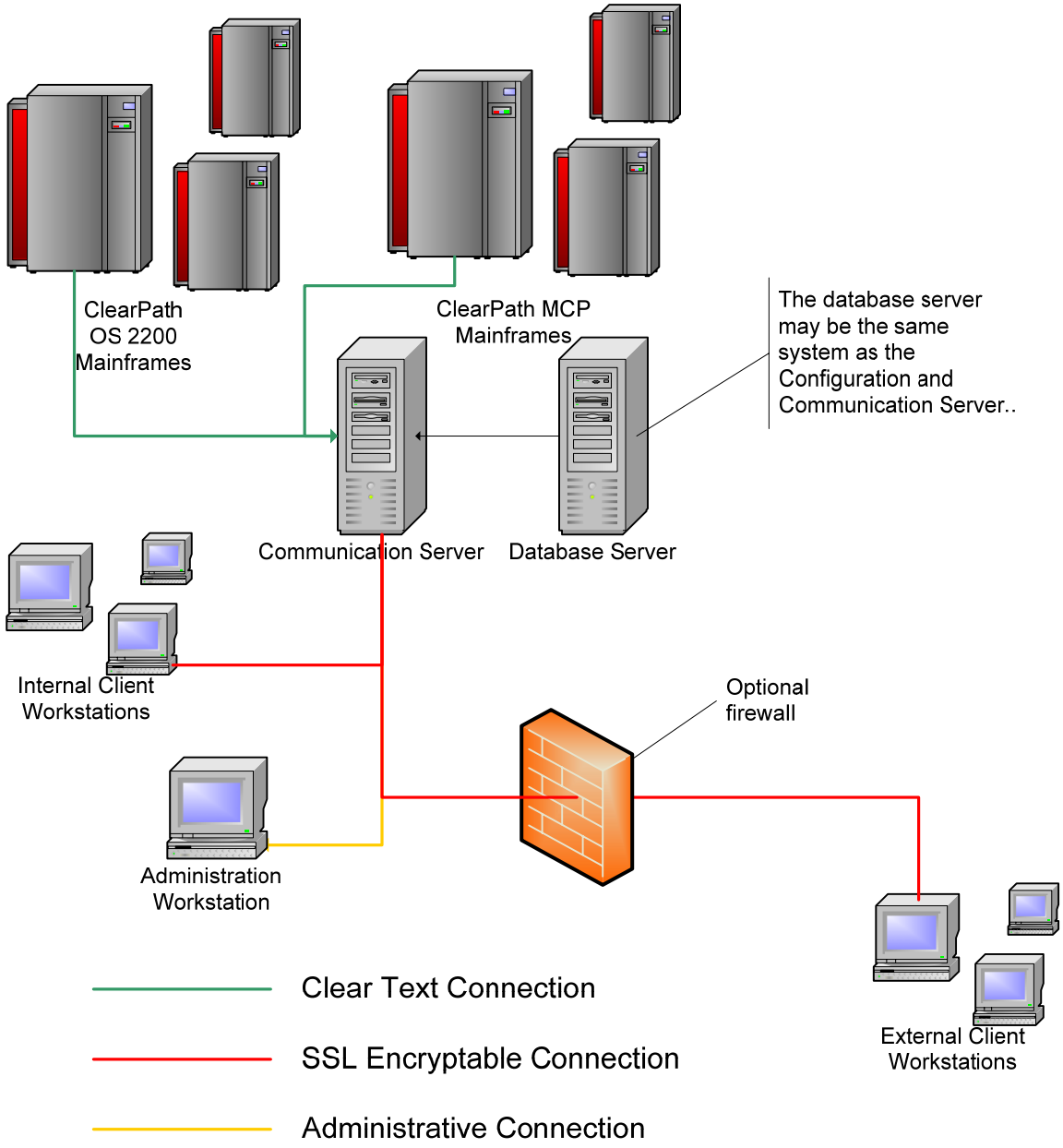

Figure 1 - How Host Gateway Server Fits in the Network

System Overview

The Host Gateway Server system consists of roles with each role consisting of one or more components.

Role	*Components*	*Installation Instances*	*Installed On*
Communications Server	Host Gateway Server Service	1 and only 1	Supported Servers – *see page 12* – Supported Server Systems
Database Server	Microsoft SQL Server	1 and only 1	Supported Servers – *see page 12* – Supported Server Systems
Configuration Management	Host Gateway Server Configuration Manager	1 or more	Supported Servers – *see page 12* – Supported Server Systems
			Supported Workstations - *see page 12* – Supported Workstation Systems
Monitoring	Host Gateway Server Session and Performance Monitor	0 or more	Supported Servers – *see page 12* – Supported Server Systems
			Supported Workstations - *see page 12* – Supported Workstation Systems
Utility Deployment Site	Host Gateway Server Session and Performance Monitor Deployment Site	0 or more	Any web server

Table 1 - Roles and Components

*Components	Purpose	Supplied By
*Host Gateway Server Service	Handle communication between client systems and the Unisys host system	KMSYS Worldwide, Inc.
*Microsoft SQL Server 2008 RTM or higher	Hold configuration and session state information for the communications server	Microsoft
*Host Gateway Server Configuration Manager	Manage communication and service configurations, licenses and service state	KMSYS Worldwide, Inc.
*Host Gateway Server Session and Performance Monitor	Monitor general performance and sessions	KMSYS Worldwide, Inc.
Host Gateway Server Session and Performance Monitoring Deployment Site	Optionally host a ClickOnce deployment for the Host Gateway Server Session and Performance Monitor	Web server vendor

Table 2 - Components

* - All components marked with an asterisk must be installed on members of the same Active Directory Domain, unless they are installed on the same system, in which case, domain membership is optional.

Account/Group	Purpose	Requirements
Host Gateway Server Administration Group	Only members of this group are allowed to administer all aspects of the HGS system.	Must be a Global Security Group in the Active Directory domain
Host Gateway Server Service Account	The account that the Host Gateway Server Communications Service runs under	Must be a member of the Host Gateway Server Administration Group

Table 3 – Special Accounts and Groups

Note: If the HGS System is being installed on a server that is not a member of an Active Directory domain (IE - a standalone server), the HGS Administration Group should be a local group and the HGS Service Account should be a member of that group and the local machine Administrator's group. Other local machine accounts may be added to the HGS Administration Group.

Pre-Installation Environment Check

General Windows Environment

The systems should be fully patched and hardened according to Microsoft's best practices and your organization's guidelines. If a system is to be a member of a domain, it should be joined to the domain. The following is a minimum configuration for all roles with the exception of the Host Gateway Server Utility Deployment Site role, which does not require a Windows-based host.

- Fully patched and supported operating system *see page 12* – Supported Server Systems and – Supported Workstation Systems
- A network connection
- .NET Framework 3.5 SP1
- 2 GB of free disk space above what is required to run the rest of the system

Database Server Environment

Host Gateway Server requires the use of a database, which can be any version of Microsoft SQL 2008 RTM or higher. The Express Edition may be downloaded from Microsoft, installed and used for no cost. If installing the Express Edition, please install the associated management tools. Because the low use of the database, Host Gateway Server may share an instance of SQL with other applications. The database server may or may not be resident on the same system as the Communications Server role.

	SQL Server Type and Location			
	Local SQL 2008 Express RTM or higher	Remote SQL 2008 Express RTM or higher	Local SQL 2008 RTM or higher	Remote SQL 2008 RTM or higher
Domain Membership Required	No	Yes	No	Yes

Table 4 – SQL Server vs. Domain Membership Requirements

Account and Account Groups

The appropriate accounts and groups, either domain or local, should be setup prior to starting the installation of Host Gateway Server. Please see Table 3 on page 3 for account and account group and requirements.

Installation Steps

Overview

Host Gateway Server installation consists of four separate features:

- Communications Server
- Configuration Manager
- Session and Performance Monitor
- ClickOnce Deployment site for Session and Performance Monitor

These features may be installed in any combination.

Install Role-Based Prerequisites

Communications Server Role Prerequisites

This role has no prerequisites beyond those for the General Windows Environment.

Database Server Role Prerequisites

This role has no prerequisites beyond those for the General Windows Environment.

Configuration Management Role Prerequisites

This role has no prerequisites beyond those for the General Windows Environment when it is installed on the same server as the Database Server Role.

When this role is installed on a system without the Database Server Role, follow the procedure below.

Install Microsoft Core XML Services 6.0 Service Pack 1 available from http://www.microsoft.com/downloads/details.aspx?FamilyID=d21c292c-368b-4ce1-9dab-3e9827b70604&displaylang=en#filelist.

Install the following components in the order listed from http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=b33d2c78-1059-4ce2-b80d-2343c099bcb4.

- Microsoft SQL Server 2008 Native Client
- Microsoft SQL Server System CLR Types
- Microsoft SQL Server 2008 Management Objects

After installation run Windows Update to apply patches.

Session and Performance Monitoring Role Prerequisites

This role has no prerequisites beyond those for the General Windows Environment.

Install the Host Gateway Server Features

Run HGSSetup.msi from the supplied media. You will be required to accept the license agreement. All files setup during the installation phase will be installed in a single directory tree that defaults to %Program Files%\KMSYS Worldwide\Host Gateway Server\3.0 or on 64-bit systems %Program Files(X86)%\KMSYS Worldwide\Host Gateway Server\3.0

Post Install Setup

The steps for the post install setup are unique for each role.

Note: The Communications Server Role Post Install **must** be completed prior to any other step being attempted.

Communications Server Role Post Install

Run the Post Install Setup Utility from Programs | KMSYS Worldwide | Host Gateway Server 3.0 | Post Install Setup Utility. If a User Account Control prompt appears, please click *Allow*.

1. Select database server:
    a. Either browse and select from the dropdown or type the name into the *Entered Instance* text box,
    b. If this is the first Host Gateway Server installation for this database server, continue, otherwise skip to step 4.
2. If this is the first installation of Host Gateway Server, a dialog will appear indicating that the databases were not found and should be created. Click *Create* to create the databases.
3. Once the message "HGS databases created and initialized" appears in the status bar, click *Close.*
4. Select the *owner group* discussed in the System Overview section, starting on page 2. Clicking *Select Owner* will configure the Host Gateway Server databases to allow full access under the selected account or group. *Note:* If the selection is already associated with the DBOWNER role in the SQL server, an error message will appear and it can be ignored.
5. Define the Host Gateway Server Communications Server:
    a. Enter the logical name and description for the server,
    b. Click *Initialize Server.*
6. Exit the Host Gateway Server Post Install Setup program.

Database Server Role Post Install

Ensure that shared memory, TCP/IP and Named Pipes client protocols are enabled. If more than one remote accessible SQL server resides on the system, the TCP/IP port may need to be adjusted from the default.

Configuration Management Role Post Install

If the Communications Server role is installed and setup on the system, there is no post install setup for the Configuration Management Role. If the Communications Server role is not installed, Run the Post Install Setup Utility from Programs | KMSYS Worldwide | Host Gateway Server 3.0 | Configuration Manager and follow these steps.

1. Click *Initialize*,
2. Allow elevation,

3. Either browse and select from the dropdown or type the name into the *Entered Instance* text box.

Monitoring Role Post Install

If the Communications Server role is installed and setup on the system, there is no post install setup for the Configuration Management Role. If the Communications Server role is not installed, Run the Post Install Setup Utility from Programs | KMSYS Worldwide | Host Gateway Server 3.0 | Performance Monitor and follow these steps.

4. Click *Initialize*,
5. Allow elevation,
6. Either browse and select from the dropdown or type the name into the *Entered Instance* text box.

Host Gateway Server Utility Deployment Site Role Post Install

The ClickOnce web site is installed into the HGSWebDeployment sub-directory of the Host Gateway Server installation path. Create a virtual directory in IIS with a name of your choosing and a physical path pointing to the HGSWebDeployment directory.

Configuration

Overview

All configuration actions are performed through the HGS Administration and Configuration Utility (Start | Programs | KMSYS Worldwide | Host Gateway Server 3.0 | Configuration Management). A single instance of the utility can configure and control one or more instances of the Host Gateway Communication Server.

General Usage Guidelines

Configuration sets and their constituent parts may be created from scratch (New), edited (Edit) or created from an existing item (Duplicate). Each action results in the same item configuration dialog being displayed with or without existing information.

OK buttons will remain grayed out until all required fields are present or, in the case of an edit or duplication operation, at least one field is changed. Changes applied to items within a configuration set are not saved until the *OK* button on the HGS Configuration Set dialog is clicked.

Help buttons are used to present general information about the current dialog. Please use the help buttons to become familiar with the purpose of the item being edited and for general information. Tooltips are used to present small amounts of information about a field or button. Field specific extended help is available in many locations by selecting the field or button and pressing F1. If available, the extended help for the selected item will display adjacent to it.

Informational messages are displayed in the status bar (bottom) of the current dialog. A prefix of "*Show Error Details*" may be clicked for more information and the copy button in the resulting dialog will copy the entire contents to the clipboard for pasting into an email for support. The use of the copy button is much preferable to a screen capture of the dialog.

Two distinct aspects of the configuration are maintained through the HGS Administration and Configuration Utility. The first aspect is information that is unique to an installation of the Communications Server role. The second aspect is the communications configuration sets that may be shared among installations of the Communications Server role.

Server Unique Configuration

Server unique information consists of three parts: server identification; diagnostic and logging settings; and service credentials.

Server identification includes a logical server name, a description of the server and the machine on which the server is installed. This information is generated when the Post Install Setup Utility is run after the installation of a Communications Server role.

Diagnostic and logging settings define the location and size of the diagnostic trace file and the audit log file. In addition, a SMTP server may be configured for notification of critical events in the Host Gateway Server Communications Server service.

When installed, the service is configured for manual start. Clicking "*Set Credentials*" will set the current credentials into the service controller and set configure the service for auto start. It will not start until the "*Start Service*" button is clicked. The password for the service credentials is not stored in the configuration database.

Communications Configuration Sets

The data communications configuration is maintained as one or more configuration sets. Each set is a self-contained entity in that any element of a set is available only to that set. A single configuration set may be deployed to more than one Host Gateway Communication Server.

The constituent parts of a configuration set are:

- Listeners – Defines the ports and protocols on which to listen
- T27 Paths – Defines connection paths from T27 devices to ClearPath MCP systems
- UTS Paths – Defines connection paths from UTS devices to ClearPath OS 2200 systems
- Virtual Destinations – Defines the address and port for connecting to a host (MCP or OS 2200) system and its associated Station Name Generation Templates.
- Station Name Generation Templates – Defines how Host Gateway Server generated station names will be generated.

All configuration set names must be unique and all items within a configuration set must have names unique within the set. Even though all items within a configuration set are optional, it must, as a minimum, contain a Listener and a Path (T27 or UTS) and its associated Virtual Destination in order to be deployable and usable.

Server Management

Service Management

Starting and Stopping the Service

Once initially configured, the service may be stopped and started via HGS Administration and Configuration Utility or through standard Windows methods such as the Windows Service management console or the *net start/stop* commands in an elevated command prompt.

Changing Diagnostic Collection Parameters

Select the service from the Server List in the HGS Administration and Configuration Utility. Click *Edit Server*. Change the desired parameters. Click *Save*. If the service is running, click *Apply* to make an immediate change. If the service is not running or *Apply* is not clicked, the service will apply the new configuration on next start.

License Management

Licenses are installed and removed through the HGS Administration and Configuration Utility. Once the service is running, select it from the Servers list and click *Manage Licenses*. NOTE: Licenses can only be installed to a running server.

Click the *Import License* button. Select the server license and click *OK*. Repeat for all client licenses.

Communications Configuration Management

Once a communications configuration set is complete, it may be attached to a server instance. Select the server instance in the Servers list and click *Attach Config*. Select the desired configuration set from the drop-down list. The *Attach & Close* button will only become active if a new set name is chosen. This button configures the service to use the new configuration the **next time the service is started**. The *Apply* button is always active, but it will only succeed if the service is running. Use it to do an immediate configuration update on a running server. NOTE: The *Apply* button installs the content of the selected configuration set to the running instance. It does **not** update the associated configuration set.

Monitoring

Session and Performance Monitoring

Session and performance monitoring can be done through the Performance Monitor program or the Configuration Management program. The operations are identical.

The *Monitor Control* tab controls the collection controls the frequency of the performance statistics refresh and the servers that will be includes in the performance charts. The session monitoring is also enabled on the *Monitor Control* tab.

Performance monitoring refers to general statistics such as session counts and throughput. The information is display in four charts on the *Performance* tab. Any series on a chart may be disabled or enabled by clicking its legend entry. Disabled series are indicated by a grayed out legend.

Session monitoring is enabled by clicking the *View Sessions* button on the *Monitor Control* tab. Once session monitoring is enabled, a new tab will appear with the name of the server selected. Multiple servers may be monitored simultaneously. The new tab displays the license usage information and all active sessions on the selected server. The session list will fully populate within the time specified in the *Refresh Rate* on the server tab. Sessions may be grouped by using the radio buttons in the *Group By* box. In addition, they may be sorted on any column. Session monitoring for a server is terminated by clicking the *X* on the server tab.

Windows Resource Monitor

Host Gateway Server Service provides instrumentation to the Windows Resource Monitor previously known as Windows Performance Monitor. It provides two categories of counters: HGS Global Counts and HGS Session Counts.

The HGS Global Counts category includes current and total session counts, and total message and current message per second counts. The HGS Session Counts category includes counts at an individual session level.

Appendix I – Supported Systems

Operating System Level	*Supported Editions*
Windows Server 2008 – 32-bit editions or 64-bit editions – RTM or higher	Standard
	Enterprise
	Data Center
	Essential Business Server
	Small Business Server Standard or Premium
Windows Server 2008 R2 –RTM or higher	Standard
	Enterprise
	Data Center
	Essential Business Server
	Small Business Server Standard or Premium

Table 5 – Supported Server Systems

Operating System Level	*Supported Editions*
Windows XP	32-Bit - Service Pack 3
Windows Vista	32-Bit/64-Bit – RTM or higher
Windows 7	32-Bit/64-Bit – RTM or higher

Table 6 – Supported Workstation Systems

Appendix II – Host Gateway Server, SSL and Certificates

Overview of Certificate Requirements

Like all SSL protocol servers, Host Gateway Server requires a SSL certificate to be installed on the same system. The rules for this certificate are identical to the rules for a certificate for a web server. The *common name* in the certificate must **exactly** match the machine name that the client systems will be using to access the server. If the client systems will use a fully qualified domain name (FQDN), to access the Host Gateway Server, the *common name* must be the FQDN of the server. If the client systems are going to use a short name such as HGSSERVER, then that is what must be in the *common name*. (It should be immediately obvious that one server cannot have client systems accessing it via both its short and fully qualified name.) The second consideration for the SSL certificate is whether to procure a commercial certificate from a company such as VeriSign or Thawte (for two examples) or to use a privately issued certificate from your organization's own certificate server. A privately issued certificate is free but it has drawbacks depending on your environment. If you do not have a convenient method to distribute the private certificate so that it will be trusted by the client systems, it may well be worth the price of a commercially supplied certificate. If you are running a Microsoft Certificate Server in Integrated mode **and** all of your clients are members of the same domain as your certificate server, the privately issued certificate will work seamlessly.

While the administration and maintenance of "Self-Signed Certificates" may prove to be difficult, they can be useful in a limited test deployment. "Self-Signed Certificates" may be acquired from utilities in the OpenSSL SDK, the Microsoft Windows SDK or SAIL. Any "Self-Signed Certificate" must be imported into the Trusted Root Certification Authorities on the client system before the client will trust it. Any .pem file that contains a "Self-Signed Certificate" may be renamed as a .cer file for import on a Windows client system. If a certificate with its associated private key is required for importing into a Windows Server, the certificate and private key .pem files may be converted to a single .pfx file by using the "OpenSSL pkcs12 –export …" utility from the OpenSSL SDK..

Note: Each configured Listener is associated with a certificate. Multiple Listeners allow for, but do not require, multiple certificates.

Certificate Installation

Follow the Microsoft supplied instructions for installing your SSL certificate on the server hosting the Communications Server role. The certificate must be installed into the *machine certificate store*. After installation, the Certificate Manager Console Plug-in must be used to set the security on the certificate so that the Host Gateway Server Service can access it.

Enabling Host Gateway Server to Access the Certificate

Follow the steps below to set the certificate security.

Start | *Run*

Type MMC

Click *OK*

Allow elevation if requested

File | *Add/Remove Snap-in…*

Click *Certificates*

Click *Add*

Choose Computer account

Click *Next* then *Finish*

Click *OK*

Expand *Certificates (Local Computer)*| *Personal* | *Certificates*

Select the certificate in the center pane.

In the right hand pane, click *More Actions* under the certificate (not under Certificates)

Click *All Tasks* | *Manage Private Keys…*

As a minimum, allow Read for the Host Gateway Server Service Account.

Appendix III – Trouble Shooting Client Connections

Client Message	*Cause*	*Resolution*
Could not establish a connection to any suitable address	No response was received from any IP address associated with the machine in the client Virtual Destination.	Verify correct system name is in the client's Virtual Destination Verify the server hosting Host Gateway Server is running.
No connection could be made because the target machine actively refused it	The system referenced by the HGS server name in the client configuration would not accept a connection.	Verify correct system name is in the client's Virtual Destination. Verify correct port number is in the client's Virtual Destination. Verify that the HGS Service is running on the HGS server system
No such host is known	The HGS server name in the client configuration cannot be resolved by DNS	Verify correct system name is in the client's Virtual Destination
No active license for Host Gateway Server - Please contact your system administrator	The HGS server license has not been installed into the HGS server.	Install the Host Gateway Server license and associated client licenses
SecureEngine set state to ISecureEngineState.ISESAborted	This message indicates that there is a problem with SSL connection from the client to the HGS server. See the text after (*Specific status follows*) for more specification information	

Client Message	*Cause*	*Resolution*
	The target principal name is incorrect	This means that the name in the SSL certificate on the HGS server does not **exactly** match the server name configured in the client connection. This problem often arises because the client may have a short DNS name and the certificate has a fully qualified DNS name or visa versa.

Table 7 – Client Messages with Session Path Closed

Testing Client Connectivity

OS 2200 Client Connectivity Testing

Client connectivity is best tested with DEMAND because DEMAND is easier to setup than TIP. DEMAND does not require a specific terminal id/station name or information about the application group. Once DEMAND is working, you can then test TIP. If you do not wish to run DEMAND in the production environment, then remove it after initial testing, but **KMSYS Worldwide highly recommends that you attempt DEMAND first**.

Configure a client with an installed Client Access License (CAL) for testing. The full featured UTS eXpress Enterprise is the easiest client with which to test. Even if you will not be using this client in the production environment, you should use it to confirm the configuration for both DEMAND and TIP.

MCP Client Connectivity Testing

Configure a client with an installed Client Access License (CAL) for testing. The full featured T27 eXpress Enterprise is the easiest client with which to test.

Appendix IV – Pre-Installation Information Checklist

Fully qualified DNS name of HGS server: _____

Local administrator userid/password of HGS server:

_____

Port for client to HGS Server connections: _____

SSL Certificate

System name for certificate (usually the fully qualified DNS name of server):

_____

Are you using a commercial certificate service?

Yes: Certificate acquired ☐

No: Name of local certificate server:

_____

Is server is member of a Windows domain?

Yes: Domain Name: _____

HGS Administration Group: _____

HGS Service Account: _____

No: HGS Administration Group: _____

HGS Service Account: _____

SQL

Using an existing SQL server?

Yes: Machine\Instance name: _____

Can HGS Service Account access the database server? ☐

No: (install Express Edition during setup)

Fully qualified DNS name or IP address of 2200:

_____

Demand Configuration

CSU name configured in CMS/Silas: _____

Tip Application Group 1 Configuration

CSU name configured in CMS/Silas: _____

Application name configured in CMS/Silas: _____

Tip Application Group 2 Configuration

CSU name configured in CMS/Silas: _____

Application name configured in CMS/Silas: _____

Tip Application Group 3 Configuration

CSU name configured in CMS/Silas: _____

Application name configured in CMS/Silas: _____

Tip Application Group 4 Configuration

CSU name configured in CMS/Silas: _____

Application name configured in CMS/Silas: _____

Tip Application Group 5 Configuration

CSU name configured in CMS/Silas: _____

Application name configured in CMS/Silas: _____

Tip Application Group 6 Configuration

CSU name configured in CMS/Silas: _____

Application name configured in CMS/Silas: _____

Tip Application Group 7 Configuration

CSU name configured in CMS/Silas: _____

Application name configured in CMS/Silas: _____

Firewall(s)

Allow port 102 connections from HGS Server to 2200 ☐

Allow connections from HGS clients to HGS Server ☐

Index