BusinessLink Software Support

Strategi
Distributed HSM Guide

Version v1r7

This manual applies to Strategi version V1R7.

ADVANCED BusinessLink Corp. may have patents and/or patent pending applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents.

Every effort has been made to ensure the accuracy of this manual. However, ADVANCED BusinessLink Corp. and Advanced BusinessLink (Australia) Pty. Ltd make no warranties with respect to this documentation, and shall not be liable for any errors, or for incidental or consequential damages in connection with the performance or use of this manual, or the examples pertaining to products and procedures as described herein. The information in this manual is subject to change without notice.

Other trademarks, trade names and brand and product names used in this manual are trademarks or registered trademarks of their respective holders.

Printed in the United States of America.

Note to Readers

Built on the premise that technological solutions are useless unless they provide real-world business benefits, Strategi has been architected to provide your organization a foundation to enable creative breakthrough e-business solutions. This manual has been designed to enhance your usability experience with Strategi as well.

The latest versions of this document and other Technical Support Bulletins can be downloaded from ADVANCED BusinessLink Corp.'s Support Website, http://support.businesslink.com.

You may print this in duplex format using Adobe's Acrobat Reader, which is available for download from http://www.adobe.com/products/acrobat/readstep.html.

With some installs of Adobe Acrobat, your printer may not resolve the characters correctly, and once printed, all characters will appear as a rectangles or as symbols. If this happens select "Print as image" from the Acrobat print dialogue and the print should occur correctly.

If you have any questions, comments or suggestions, please feel free to contact us via e-mail at 'support@businesslink.com'.

Sincerely,

BusinessLink Software Support

Table of Contents

Overview

Distributed HSM by ADVANCED BusinessLink allows iSeries 400 sites the ability to link iSeries 400 hosts together in a manner conducive to Internet deployment.

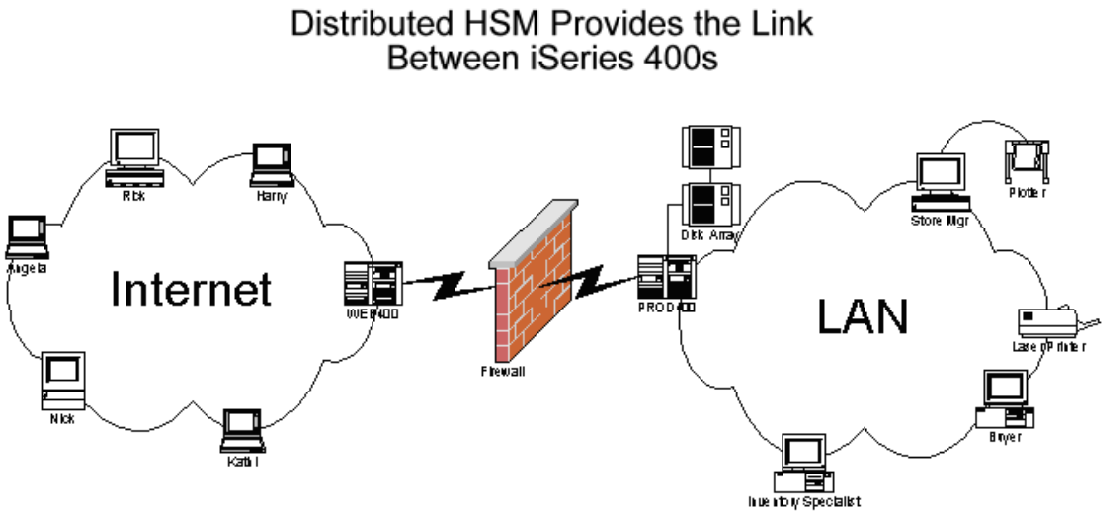

Figure 1 - Distributed HSM example configuration

In order for Distributed HSM to operate, Strategi must be installed on all iSeries 400 systems where Distributed HSM will be used. Specific Strategi size requirements will vary depending upon business needs. Contact your local ADVANCED BusinessLink sales representative for further details.

The setup and documentation information will refer to the iSeries 400 behind the firewall as PROD400, and the iSeries 400 outside the firewall connected to the Internet as WEB400. Typically PROD400 will contain the actual live database files, programs, data areas, etc., while WEB400 will not contain live data, but simply serve as an interface point to Internet users. The iSeries 400s connected are not required to exist on different sides of a firewall, but will be described in this manner for sake of consistency and ease of understanding.

Getting Started

The setup for Distributed HSM involves four main procedures: define peer systems, create peer relay servers, enable peer services, and modify server authorities (optional).

Step 1 – Define Peers Systems

What is a "peer"? A peer is defined as, "One who has equal standing with another." The iSeries 400 systems involved are considered peer systems because the relationship between systems is equal, that is, there is not any implied hierarchy.

The **xxxSGIPEER** commands are used to define a peer system. This definition is used to specify details of the peer system for making a connection (e.g. DNS), the requirements of the connection (e.g. SSL) and the status and identity of the system.

Peer Systems must be defined on both the originating and target systems. Figures 2 through 5 show example parameter values used to generate peer system definitions on one iSeries 400.

When using the xxxSGIPEER commands, review the on-line command help text associated with it for detailed assistance.

Creating Peer System definitions take place when adding new Distributed HSM-able systems to your Distributed HSM environment.

After defining the peer systems on affected iSeries 400s, the next step is to define the peer relay HSM server(s).

Figure 6 is an example of the “Work with Peer System Definitions” screen after defining two peer systems.

```
                    Add Peer System Definition (ADDSGIPEER)

Type choices, press Enter.

System Code  . . . . . .   WEB400
System Serial Number . . .   1044YYY       Character value
DNS Name . . . . . . . . .   some.valid.dns.name.com

Accept Incoming Connections  . .   *YES          *YES, *NO
Text Description . . . . . . . .   'Web System - Loopback Testing'

Status . . . . . . . . . . . . .   *ENABLED      *ENABLED, *DISABLED

                           Additional Parameters

Connect/Authenticate Timeout . .   60            Number
Require SSL  . . . . . . . . . .   *NO           *YES, *NO
Require SSL Certificate  . . . .   *NO           *YES, *NO
Authenticate IP Addresses  . . .   *YES          *YES, *NO

                                                                    More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 2 - Peer System definition creation for originating system loop-back testing (first screen).

```
                    Add Peer System Definition (ADDSGIPEER)

Type choices, press Enter.

TCP/IP Filter:
  Peer Must Match Address  . . .   111.111.111.0
    With Network Mask  . . . . .   255.255.255.0
TCP/IP Ports:
  Standard . . . . . . . . . . .   '0xAB30'      nnnnn, 0xNNNN
  SSL  . . . . . . . . . . . . .   '0xAB31'      nnnnn, 0xNNNN
  SSL with Certificate . . . . .   '0xAB32'      nnnnn, 0xNNNN









                                                                    Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 3 - Peer System definition creation for originating system loop-back testing (second screen).

```
                    Add Peer System Definition (ADDSGIPEER)

Type choices, press Enter.

System Code  . . . . . .   PROD400
System Serial Number . . . . . .   1033ZZZ       Character value
DNS Name . . . . . . . . . . . .   some.valid.dns.name.com

Accept Incoming Connections  . .   *YES          *YES, *NO
Text Description . . . . . . . .   'Production System'

Status . . . . . . . . . . . . .   *ENABLED      *ENABLED, *DISABLED

                           Additional Parameters

Connect/Authenticate Timeout . .   60            Number
Require SSL  . . . . . . . . . .   *YES          *YES, *NO
Require SSL Certificate  . . . .   *NO           *YES, *NO
Authenticate IP Addresses  . . .   *YES          *YES, *NO

                                                                    More...
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 4 - Peer System definition creation on originating system for target system (first screen).

```
                    Add Peer System Definition (ADDSGIPEER)

Type choices, press Enter.

TCP/IP Filter:
  Peer Must Match Address  . . .   111.111.111.0
    With Network Mask  . . . . .   255.255.255.0
TCP/IP Ports:
  Standard . . . . . . . . . . .   '0xAB30'      nnnnn, 0xNNNN
  SSL  . . . . . . . . . . . . .   '0xAB31'      nnnnn, 0xNNNN
  SSL with Certificate . . . . .   '0xAB32'      nnnnn, 0xNNNN









                                                                    Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 5 - Peer System definition creation on originating system for target system (second screen).

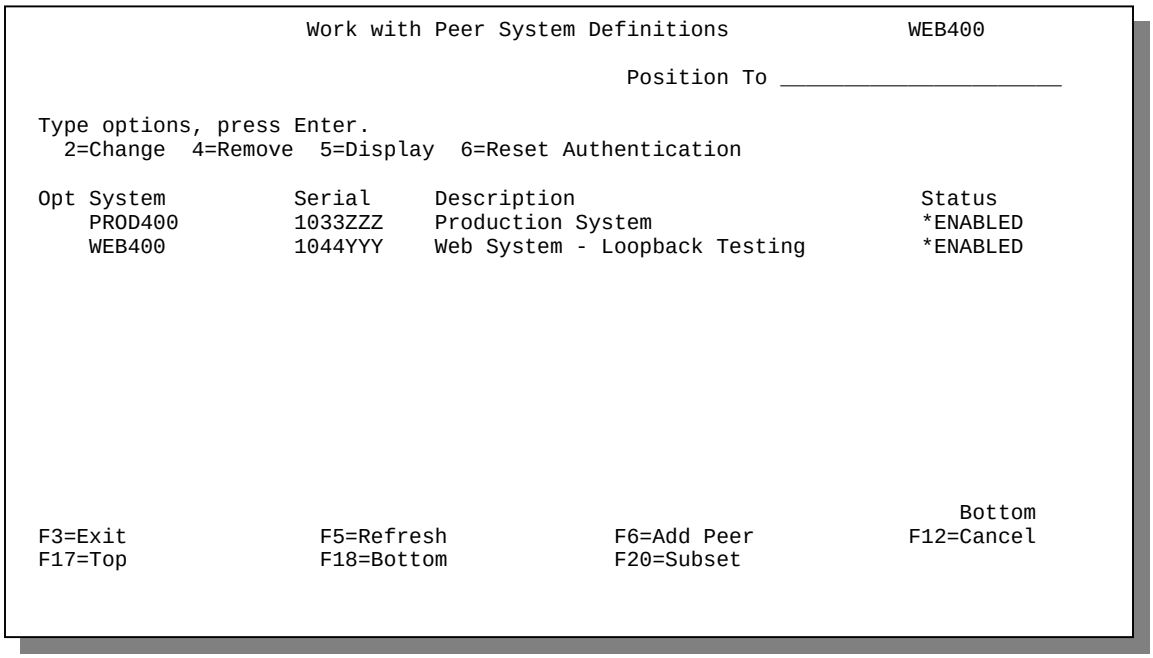

Figure 6 - Work with Peer System Definitions.

Step 2 – Create Peer Relay Servers

Creating a peer relay server is similar to creating a non-peer HSM server, except a few of the parameters to the command **CRTHSMSVR** are different—specific to a peer relay server.

Peer relay servers are used to relay HSM requests from the originating iSeries 400. All [SERVER REQUEST] hsm requests originating from an hsm file must have an HSM server defined on the same system the hsm file resides on.

Creating a peer rely server uses the same command interface as a non-peer HSM server, namely, CRTHSMSVR.

Figure 7 shows the details for creating a peer rely server and Figure 8 shows a completed example of how to create a non-peer HSM server.

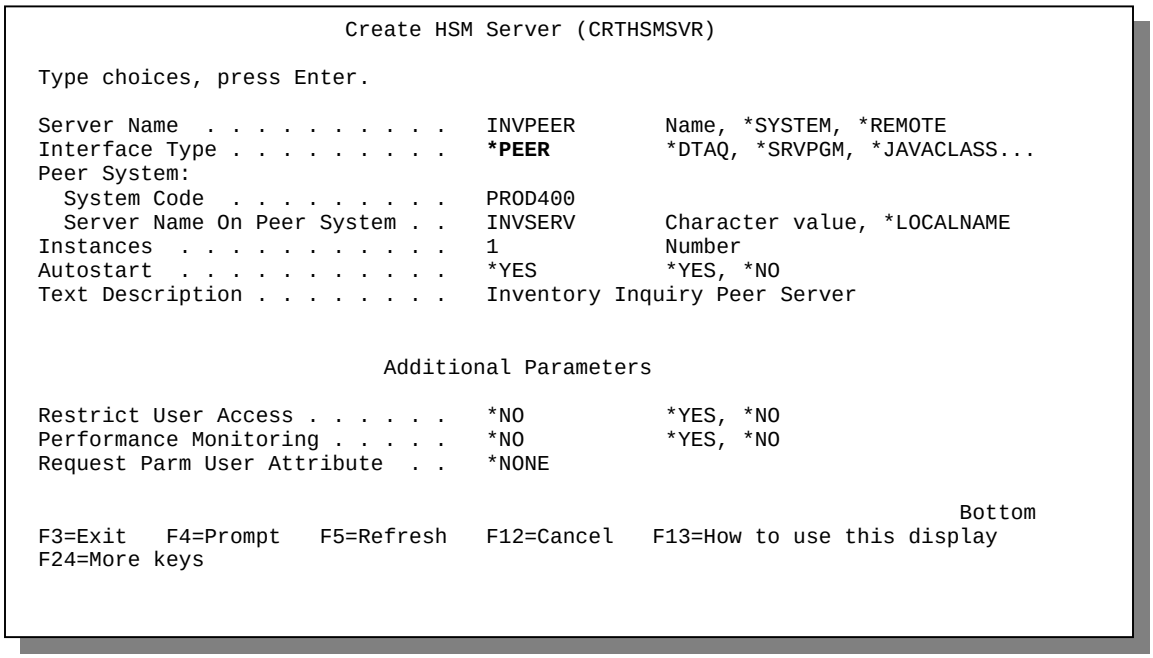

Figure 7 - Example of defining a peer relay HSM server.

Server Name is the name of the server that clients refer to when making requests. It is also used for the job name that runs and to name the communications objects that the server uses. This must be unique.

Interface Type specifies which interface the server uses. *PEER indicates the server is a relay server used to relay requests to a Strategi Peer System.

Peer System specifies the Strategi Peer System the HSM server is running from, if it is running on a Strategi Peer System. It specifies the target Peer System, not the system currently being used to execute the **CRTHSMSVR** command.

> **System Code** specifies the Strategi Peer System Code, or name, for the target system. This system code must have already been defined using the **ADDSGIPEER** command. For this example, PROD400 is the System Code.
>
> **Server Name On Peer System** specifies the name of the HSM server on the Peer System. This makes it possible for the server name on this system and that on the target system to be different (as in this example), relieving any requirement to manage server names with respect to other networked Strategi Systems.

Instances specifies the number of copies of the server to start in parallel.

Autostart specifies whether the server will be automatically started whenever the Strategi subsystem is started.

Text Description specifies the description of the HSM server.

Restrict User Access specifies whether Strategi should check for HSM authority restrictions when processing opcodes for this server.

Performance Monitoring specifies whether performance monitoring will run for this server.

Request Parm User Attribute specifies a Strategi user attribute name. Useful if you need the value of one specific Strategi User Attribute passed on each request made. The server program must make one Strategi API call to

"activate" the option and add an additional parameter on the **HSMRCVRQS** API (see the *Strategi HSM Programmer's Guide* for additional information).

```
                        Create HSM Server (CRTHSMSVR)

Type choices, press Enter.

Server Name  . . . . . .  .   INVSERV       Name, *SYSTEM, *REMOTE
Interface Type . . . . . .   *SRVPGM       *DTAQ, *SRVPGM, *JAVACLASS...
Server Program . . . . . .   INV001R       Name
  Library  . . . . . .  .      INVPRD      Name, *LIBL
Instances  . . . . . .  .    1             Number
Autostart  . . . . . .  .    *YES          *YES, *NO
Text Description . . . . .   Inventory Inquiry Server

Job Description  . . . . .   PRDJOBD       Name, *STRATEGI
  Library  . . . . . .  .      INVPRD      Name, *LIBL

                           Additional Parameters

Restrict User Access . . . . .   *NO          *YES, *NO
Performance Monitoring . . . .   *NO          *YES, *NO
Request Parm User Attribute  . .   *NONE
                                                                  Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Figure 8 - Example of defining a non-peer relay HSM server.

Server Name is the name of the server that clients refer to when making requests. It is also used for the job name that runs and to name the communications objects that the server uses. This must be unique.

Interface Type specifies which interface the server uses. *SRVPGM indicates the server uses the ILE service program interface and is a non-peer server.

Server Program is the qualified name of the program that runs when this server is started.

Instances specifies the number of copies of the server to start in parallel.

Autostart specifies whether the server will be automatically started whenever the Strategi subsystem is started.

Text Description specifies the description of the HSM server.

Job Description specifies the qualified job description name that is used when submitting the server program.

Restrict User Access specifies whether Strategi should check for HSM authority restrictions when processing opcodes for this server.

Performance Monitoring specifies whether performance monitoring will run for this server.

Request Parm User Attribute specifies a Strategi user attribute name. Useful if you need the value of one specific Strategi User Attribute passed on each request made. The server program must make one Strategi API call to "activate" the option and add an additional parameter on the **HSMRCVRQS** API (see the *Strategi HSM Programmer's Guide* for additional information).

Step 3 – Enable Peer Services

There are three Strategi Special Values that control Distributed HSM agent services: DHSMADDRESS, DHSMCERTIFICATE and DHSMTHREADS.

DHSMADDRESS

DHSMADDRESS specifies what TCP/IP address and port to listen on and whether or not to allow incoming SSL connections.

TCP/IP Address has the following valid values:

- *NONE – No Distributed HSM incoming
- *WEBSITES – Uses the addresses listed for websites (but will include a different port)
- specific IP address (e.g., 206.19.198.2)

TCP/IP Base Port is shipped with the default value of '0xAB30'. The value entered must be in hexadecimal and must not conflict with another port number used by the TCP/IP address. The value in hexadecimal translates to port 43824. The Base Port is the non-SSL port to listen on. SSL is assumed to be the Base Port value plus 1. SSL and Certificate is assumed to be the Base Port value plus 2.

Allow Incoming SSL is a 1-byte flag used to enable SSL listening and has the following valid values:

- 0 – Disable SSL listening
- 1 – Enable SSL listening

DHSMCERTIFICATE

DHSMCERTIFICATE supplies the certificate for both client and server SSL connections. It may be *NONE or a website name. This is typically the principle website for the iSeries 400.

DHSMTHREADS

DHSMTHREADS controls the initial, increment and maximum threads Distributed HSM can run. These are licensed and controlled just like HTTP Threads.

Perform any necessary changes to these three Strategi Special Values as applicable to your specific setup.

Step 4 – Modification of Server Authorities

A peer relay server making a request of a non-peer server has its Interface Type (*PEER) and System Code validated on the target system (PROD400) as defined on the target system.

Any servers that are desired to be protected from access by a peer system should be changed to be restricted, and a *PEER *ALL *NO authority added.

User Checking

Specific checking of individual users can only be done on the originating system. The user details are not relevant or applicable on the target system for the purpose of checking server authority.

For example, if the originating system defined Strategi User 231, there is no guarantee Strategi User 231 on the target system is the same user or even exists. This allows you to validate and authenticate a user on the originating machine before allowing access to your live data via Distributed HSM.

Step 5 – Restart Strategi

Restart Strategi for the affected systems when you are ready to activate Distributed HSM. Make sure your firewall has the appropriate port open for Distributed HSM communication.

Security Overview

One of the critical fields in this process is the serial number of the peer system. This must match **RTVSYSVAL SYSVAL(QSRLNBR)** and the Strategi software will retrieve the system serial number and pass it to the other end to identify itself. The serial number is analogous to a User's access name. Once the serial number is matched against the peer file, the defined system code is used in all other operations with reference to this system.

The two programs that connect for Distributed HSM perform bi-lateral authentication with each other. Authentication requirements must be fulfilled at both ends before the connection can proceed with HSM transactions.

The fundamental basis for this is a dynamic exchange key. This key is analogous to a user's passphrase and is generated every time the record is "Reset" via an option in the **WRKSGIPEER** menu. The key is hashed with several other specific pieces of information and the hash is sent for validation - this is a form of digest authentication. Thus, after the key is initially exchanged on the first connection with the peer, it is never resent.

Whenever a mismatch occurs with the exchange key, the record is immediately locked and a reset is required. Whenever the record is reset, all connections are always accepted until the new challenge key is confirmed as stored at the other end (in practical term this is measurable in milliseconds from the time of TCP connection).

The peer definition can specify an IP filter from which connections will be accepted - this filter is checked by the both sides of the connection.

The peer definition can specify that SSL, and optionally, a client certificate (SSL always uses a server certificate) is required. The originating side (the one making the TCP/IP connection) will validate its recorded DNS name against the certificate common name, provided the DNS name is not an IP address. If a client certificate is used then the host side validates the certificate received from the client matches the DNS name of the peer record (use of a client certificate excludes configuring a simple IP address for the DNS name).

Frequently Asked Questions

Q: Now that I have defined the Peer Systems on the two iSeries 400 systems, where do I put the html and hsm files?
A: The html, hsm, jpg, etc., files (web pages) necessary to support your application are placed on the iSeries 400 users will first access (or authenticate if the zone requires authentication) your web pages. For example, if using Distributed HSM and your iSeries 400 outside the firewall is named WEB400, and the iSeries 400 containing your Java, RPG, CL, etc., programs reside on the iSeries 400 named PROD400, you will place all web page information onto WEB400. PROD400 will contain the required iSeries 400 *PGM objects necessary for database access. This prevents users outside the firewall from directly accessing any resource on your production iSeries 400.

Q: Which server name do I use when performing a [SERVER REQUEST] to invoke HSM processing? The name associated with the HSM server on the originating system or the target system?
A: This is applicable to Distributed HSM systems as well as traditional Strategi HSM processing systems. The HSM server name to use is always the name specified on the SVRNAM parameter of the **xxxHSMSVR** commands for the iSeries 400 the html and hsm files reside on. Another way to determine this is perform the **WRKHSMSVR** command and notice the HSM server names. The names listed on the screen under the column heading "Server" are the server names you would code into the hsm files. When a web page is requested that has a corresponding hsm file, Strategi running on that iSeries 400 reads the hsm file and performs the requested action, regardless of the Interface Type of the HSM server.

Q: Which iSeries 400 do I create Strategi users on? WEB400 or PROD400?
A: Since users in a Distributed HSM environment do not authenticate against the target system (PROD400 for our previous examples), they must be created on the WEB400 server. Strategi will pass onto the target system the Strategi User Id if a user authenticated at the originating iSeries 400 (WEB400). This is extremely useful if your application requires user specific information, such as item pricing or minimum purchase quantity restrictions. You do not have to duplicate your database information onto the originating iSeries 400. Strategi will take care of passing that information along in the server request.

Q: Do I have to have the same licensing requirements on the target iSeries 400 that I do on the originating system?
A: Distributed HSM by ADVANCED BusinessLink is a licensed product of Strategi. In order to run Distributed HSM, Distributed HSM must be installed on both systems wanting to communicate in this manner. The number of Distributed HSM threads is determined by the maximum number of HTTP threads allowed by Strategi licensing.

List of Figures

Index