Verastream Host Integrator Administrative Console

Administrative Console Guide

None

Table of contents

1. The Administrative Console

The Verastream Administrative Console is an Eclipse-based management hub that puts monitoring and management tasks at your fingertips. The Administrative Console uses perspectives, views, and overviews to provide a configurable and totally customizable user experience.

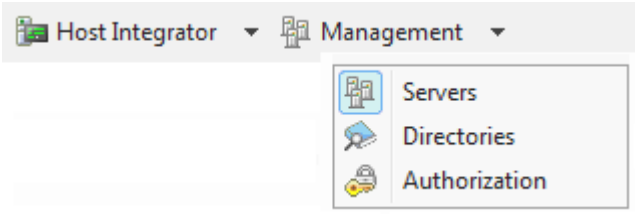
1.1 Using Perspectives

The Administrative Console hosts different perspectives, each one containing different views and editors. This lets you switch from one application to another and to adapt your workspace to your own administrative needs.

You can save perspectives, modify a perspective and then revert to the last one saved, or create a custom perspective. Each perspective group remembers the last perspective and you can switch quickly from one perspective to another.

1.2 Custom Perspectives

To tailor the console to your own workflow and needs, you can combine views and editors from different perspectives and create a custom perspective. These custom perspectives are easy to create; after you've modified the console layout, just open the Perspective menu, and select **Add Custom Perspective**.



1.3 Using the Management Perspectives

Using the Management perspectives, you can configure and monitor your management servers, handle authorization and authentication, and administer directory services. These perspectives are: - **Servers**: Load distribution domains and data replication with management server peers in a cluster. - **Directories** The Administrative Console uses LDAP as a directory service provider. When you configure an LDAP provider in the console, user and group directory services for management server clients are authenticated by an LDAP service provider. - **Authorization** Access control and authentication. The type of access allowed on the server is determined by the security profile that is assigned to the user ID.

1.4 Using Views

Views provide information about components you are working with in the console. Each perspective has views associated with it, by default. You can open or close views using the View menu or add views from other perspectives by selecting **Other views** from the View menu.

You can resize, minimize, maximize, restore, and detach views. Some views have their own toolbars which provide additional functionality. Some toolbar options are dependent on particular items within the view being selected.

Selecting an object in one view can affect what is displayed in other views. Often there is a description of what is displayed in the view.

More information

- What is a Directory?
- Using Authorization and Authentication

2. Host Integrator Management

2.1 Managing Host Integrator

The Verastream Host Integrator management server and Administrative Console provides directory services, authorization, and server management and monitoring for Host Integrator deployments. The Administrative Console tracks servers and domains in your installation and the management server provides authorization, authentication, and directory services.

By installing more than one management server you can establish replication and failover support.

How do things fit together?

When a session server starts, it registers with the management server.

When a connector connects to the session server with security enabled, the session server authenticates with the management server on behalf of the client.

When a non-connector connection is made to the session server with security enabled (such as a connection from the Administrative Console, or activatemodel command), it authenticates directly with the management server.

If a connector performs a connection via domain, the connector uses the management server for directory services. The management server provides the connector with the address of the session server that is functioning as the domain server.

2.1.1 Host Integrator components

This component	Does this...
Session server	Use the VHI session server to access data on a variety of host systems, including IBM mainframes and AS/400s, VAX/Open VMS and other ASCII hosts using the VT-420 terminal protocol (including VT-52 and VT-100), and HP 3000 hosts.
Web server	The Web server runs Java or HTML5 Web application projects deployed from within Web Builder, as well as the Zero-footprint terminal session Web applications.
Administrative Console	Use to remotely view and configure server information. The console contains both the Host Emulator and logging functions.
Management server	Use to provide security and directory services, and track servers and domains for Host Integrator installations.

This component	Does this...
Host Emulator	Use to test an application without a host connection. This tool is accessed through the Administrative Console.

This component	Does this...
Logging	Use to perform detailed queries against the Host Integrator. Logging is accessed through the Admininstrative Console.

More information

How to Use Host Integrator

Deploying a Model

Working Securely

2.1.2 Introduction to the Host Integrator Administrative Console

The Host Integrator Administrative Console is an Eclipse-based management hub that puts monitoring and management tasks at your fingertips. The Administrative Console uses perspectives, views, and overviews to provide a configurable and totally customizable user experience.

2.1.3 Using Host Integrator Perspectives

Using Host Integrator perspectives, you can configure and monitor your session servers, handle logging, and configure the Host Emulator. These perspectives include:

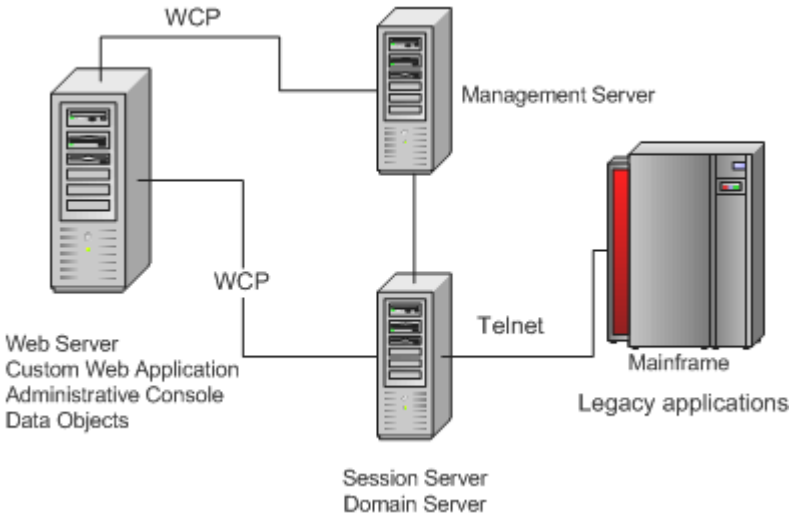
- **Session Servers** The Administrative Console provides a central hub where you can manage and monitor your session servers. You can add, remove, and configure directories, load distribution domains, security, and logging for session servers.
- **Logging** Host Integrator can log server errors and can issue warnings and informational messages as it runs.
- **Host Emulator** The Host Emulator runs 3270 and 5250 models without having a live connection to a mainframe.

More information

How to Use Host Integrator

2.2 How to Use Host Integrator

The diagram below shows a Host Integrator installation in which users can access legacy application data using a Web browser. Although each component is represented as running on separate machines, more than one component can run on the same machine. It is important to note, however, that although it is possible to run all Host Integrator components on the same machine, this is usually only done for development and testing.



2.2.1 Accessing Legacy Host Data from a Web Application

Although Web applications are the most common way to access Host Integrator server, you can also create client/server applications. You can have an installation in which users access host data by running client applications that communicate directly with Host Integrator Server over WCP.

In this type of deployment, the client application on the computer must contain all the logic for accessing the host data, which includes connecting to the Host Integrator Server, requesting the model, providing the user interface between the model and the client, managing the session, and trapping and resolving errors.

2.2.2 Sessions

In this documentation, the term "session" is a general term that describes a single session between a client or Web application and the host. The term "host session" refers to the connection between a Host Integrator Server and the host; host sessions run over Telnet.

More information

Managing Host Integrator

Deploying a Model

Working Securely

2.2.3 Working Securely

By default, Host Integrator access control is disabled. When access control is enabled for a session server, an administrative login, while always required for the Administrative Console, will also be required for deploying models, generating Web applications, and executing connectors. Encryption is always enabled.

Host Integrator access control includes authentication and authorization.

> **Note**
>
> You can also use SSL to ensure security between the Host Integrator server and an IBM 3270 or AS/400 host. To use SSL, configure your model to use Telnet SSL or Extended Telnet SSL as a transport when you set your connection properties. If you are connecting to a VT host, you can use SSH to ensure a secure connection. To use SSH, configure your model to use SSH when you set your connection properties.

Authentication and Authorization

The management server provides authorization and authentication for both the Administrative Console and Host Integrator. When you first install Host Integrator, you provide a password for the "admin" user. The "admin" user is a built-in user that has access to all the features of the Administrative Console, including Host Integrator configurations. You use the "admin" credentials to log onto the Administrative Console and then assign additional users and groups from configured external LDAP capable directories to authorization profiles. If a management server needs to be manually reset, then the default password of '=secretpassword ' is restored.

How do I configure Access Control?

Using the Administrative Console:

1. Add sources for security users and groups by either configuring directories or by enabling OS Groups in the Directory perspective.
2. Assign users and groups to the authorization profiles, Administrator, Developer, and User, available in the Authorization perspective.
3. Check the security option for each selected session server on the server property page. Since the Administrative Console is the only way to configure Host Integrator servers, enabling security controls access to servers for configuration purposes and establishes access control for data objects and client programs.
4. The management server always is running in secure mode (requires a username/password to connect) and is independent of session server security.

The built-in "admin" user is automatically part of all authorization profiles and has access to all areas of the system. To enable security follow the steps above to provide system access to additional users.

Security Profiles

The Host Integrator provides three different security profiles; user, developer, and administrator. The type of access allowed on the server is determined by the security profile the user ID belongs to. This access control is separate from and in addition to the access control provided by the host. There are scenarios in which host user ID's and passwords are sufficient for controlling access; in these cases you may decide not to enable authentication on your servers.

Configuring Server Authentication

Although the management server always runs in secure mode and a user name and password is required to access the Administrative Console and configure session server properties, this security does not control access to servers by data objects and client programs. You can establish this access control by enabling security on individual servers.

Encryption

The channel between the server and the clients that connect to it is always encrypted. A server forces encryption over SSL with every client that connects to it.

In previous versions, the RequireSecureConnection API in the connectors would be used to enable encryption between the client and the Session Server without also enabling authentication and authorization. In the current version, encryption is always enforced by the Session Server, and the value of the RequireSecureConnection flag in the connectors no longer has any effect.

Federal Information Processing Standards (FIPS) are guidelines established by the United States government to standardize computer systems. To use FIPS 140-2 validated TLS version 1 encryption for SSL support, in a Windows environment, you must first define an environment variable, VHI_FIPS = 1. After this variable is set all SSL support will use the FIPS 140-2 Crypto Libraries.

2.2.4 Using Profiles

The Host Integrator provides three different security profiles.

This security profile	Can do this....
User	Users can load Host Integrator models, create and attach to sessions, and interact with the host system. Client application user IDs are typically assigned this profile. Members of the User profile cannot log on to the Administrative Console to view or configure Host Integrator servers and cannot deploy models.
Developer	Developers can do everything users can do, as well as log on to the Administrative Console. Developers can see server configurations and status information, but cannot make configuration changes. Developers of client applications are typically assigned to this profile.

This security profile	Can do this....
Administrator	Administrators (those logging on with an Administrator profile) can create and attach to sessions, interact with the host system, and access the console. An administrator can view and configure servers, domains, and security.

In the Administrative Console, open the Management prospective, and then the Authorization Explorer to add members to the security profiles.

More information

Working Securely

2.2.5 Deploying a Model

Deployment is the process of transferring a model and its associated files and settings to the production server or servers where it's going to run. You deploy a model from the Design Tool or you can use command-driven deployment.

After a models is deployed, it is visible in the Models view of the Administrative Console. To open the Models view, from the View menu, select Models.

You can use the Design Tool to deploy a model with one configuration to one server, in this case a development server, running on the same computer as the Design Tool,for test purposes. In a command-driven deployment, you use Verastream Host Integrator's deployment commands from a command line or in a batch or shell file to deploy a model with one or more configurations to one or more production servers.

> **Note**
>
> If your integration solution includes a Web application created with Verastream's Web Builder, you must also separately deploy the Web application files. See Deploy Web Applications in the Web Builder help for information.

Using the Design Tool to deploy

If you are deploying a model with one configuration to the development server for test purposes, it's easiest to use the Design Tool.

With this approach, you use the Design Tool's Deployment Options command on the File menu to designate any session pool and model variable list settings. Next, you use the File menu's Deploy to Local Server or Deploy to Remote Server command to deploy the model. If Verastream security is enabled on the server, you are prompted for credentials. Unlike the command-driven method described below, you can only deploy the model to one server, using one model configuration. See Using the Design Tool to Deploy a Model in the Design Tool help for more information.

Using commands to deploy

If you are deploying a model with one or more configurations to one or more production servers, you should use Verastream Host Integrator's deployment commands from a command line or in a shell or batch or shell file.

With this approach, you create a model package and then use commands or a batch or shell file to deploy that model package. Your batch file can automate the deployment to multiple Host Integrator Servers. In the model package, the model file can be combined with event handler .JAR files and descriptors that tell the servers how to provide access to the model -- such as via a session pool of a certain size, or by using specific requests for a new session. See About Model Packages and Using Commands to Deploy a Model Package for more information about this deployment method.

More information

There are topics on deploying model packages and working with descriptor files and commands in the Design Tool help. See Deploying Model Packages.

Updating models deployed with earlier versions of Host Integrator

If you're upgrading from an earlier version of Host Integrator, you may have a lot of model or session pool configuration information in the Administrative Console. If you want to update a model without affecting existing configuration information, do not include descriptor files in your model package.

Once you deactivate a model that has configuration information in the console, that configuration information is lost. So if you're creating new models, you should put such information in a configuration descriptor file and then build it into your model package.

More information

How to Use Host Integrator

2.2.6 Working with Load Distribution Domains

Host Integrator load distribution domains provide load balancing and failover support for installations that contain multiple Host Integrator session servers.

The Domain Session Server view displays session servers that are associated with a load distribution domain, called domain session servers, as opposed to the Session Server view which displays all session servers in an installation, regardless if they are associated with a domain. A session server can be associated with multiple load distribution domains, or none at all. In the Domain Session Server view you can monitor all of your domain session servers, their properties, and the number of sessions that are currently active.

To open the view, on the Host Integrator perspective, from the View menu, choose Domain Session Servers.

How does it work?

When you configure a load distribution domain client, applications can connect to a domain instead of connecting to individual session servers. The management server will apply logic based on the domain configuration to distribute load among the session servers in the domain, and if a session server in a domain becames inactive for whatever reason, client applications will still be able to connect to their active session servers in the domain.

To achieve session server load distribution and failover at runtime, your client should connect "via domain":

If you write your own client application code, use the `ConnectToModelViaDomain()` or `ConnectToSessionViaDomain()` connector API method calls.

If you generate a client in Web Builder, select **Connect to model via domain** or **Connect to session pool via domain** as the connect method in your project properties.

If you use the embedded Web service, configure the domainName property.

Management Server Domain Handling Logic or What Happens at Runtime

The basic process that occurs at runtime to achieve session server load distribution and failover is:

- The management server runs a domain server for each configured domain. The management server also monitors the online status of session servers by receiving status updates and proactively checking at regular intervals.
- The client application calls the connector with `ConnectToModelViaDomain()` or `ConnectToSessionViaDomain()` API method. The arguments specify the management server address, domain name, and model or pool name. If security is enabled in the session server, then the Host Integrator user ID and password credentials are also specified.
- The connector (data object) sends a request to the management server for a session from the specified domain.
- The management server first determines which servers in the domain contain the specified model or pool and thus are eligible to fulfill the request.
- The management server then takes all eligible servers with the lowest priority value and adds up their weight values. A random number is generated between 1 and the weight total. This number is used to determine which server will be asked to fulfill the request. For example, if there is Server A with a weight of 80, and Server B with a weight of 20, then a random number is generated between 1 and 100. If the number is between 1 and 80, then Server A is asked, and if the number is between 81 and 100, then Server B is asked.
- If the server is unable to fulfill the request because it has reached the server session limit or, in the case of session pools, it has reached the pool limit, then the server is considered not eligible to fulfill the request and the process repeats with the remaining servers in the priority group. If the server is unable to fulfill the request because it is offline, then it will not be considered eligible for future requests until it becomes online again. Online status is automatically monitored by the management server.
- If all servers in the priority group are unable to fulfill the request then the whole process is repeated for server in the next higher priority group.
- When a server is able to fulfill the request, it allocates a session for the client to connect to, and responds to the management server with its address and session ID.
- The management server returns the connection information to the connector client, which connects to the session server that has the allocated session. If security is enabled for the session server, the channel is encrypted and credentials are provided to the session server. The session server also contacts the management server for authentication and authorization.
- The session server replies to the connector with the status of the initialization.

More information

Adding, Removing, and Configuring Load Distribution Domains

2.2.7 Adding, Removing and Configuring Load Distribution Domains

You add load distribution domains and session servers to a domain in the Session Server Explorer of the Administrative Console.

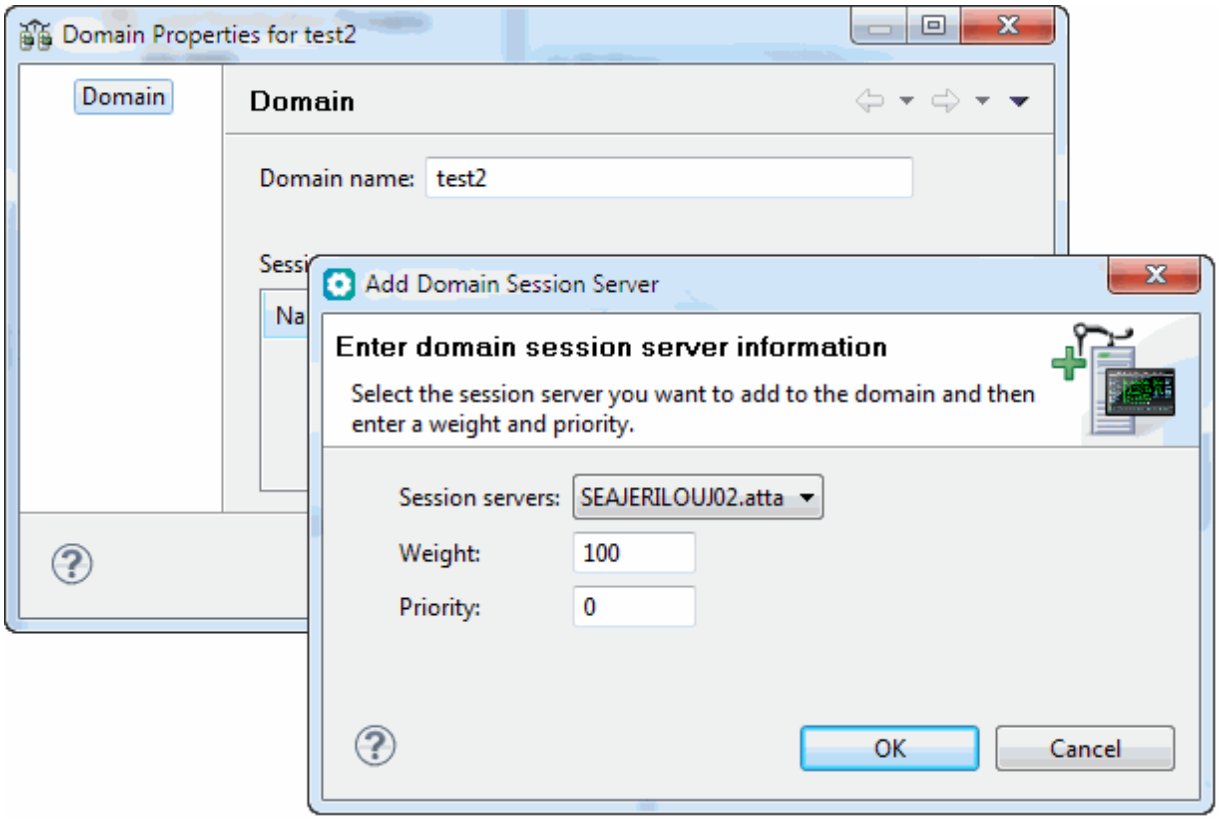
Session servers and management servers have different failover mechanisms.

> **Note**
>
> After installing Host Integrator on the first system, install subsequent servers using the Join an existing installation option. Use the management server name and password set in the first installation.

To add and edit a domain

In the Administrative Console, connect to the management server cluster with the user name admin and the password set during installation or other administrative credentials set in the Administrative Console. From the Host Integrator perspective, choose Session Servers.

2. In the Session Server Explorer tree, right-click **Load Distribution Domains**, and choose **Add domain**. The **Add Domain** dialog box displays.
3. Type a name for the new session server load distribution domain, and click OK. The new domain is listed under Load Distribution Domains in the Session Server Explorer.
4. In the Session Server Explorer, select the new domain, right-click and choose **Properties**. The properties page for this domain displays.
5. Click Add to identify the session servers that will be used by this domain. In the **Add Domain Session Server** dialog box, select the session server you want to add to the domain and then enter a weight and priority.



1. The session server has two properties associated with it; weight and priority.
2. **Weight**— This property controls the amount of load that the session server will handle within a given domain and a given priority. The value is relative to the weight values for other servers in the same domain with the same priority. Weight values are used for load distribution.
3. **Priority**— This property controls when a session server is considered eligible to handle a request for a session. A session server with a higher priority value will only be asked to fulfill a session request if ALL the servers with a lower priority value are unable to handle the request. The value '0' is the highest priority for this property. The higher the number, the lower the priority. Priority values are used for failover.

For each set of servers with the same priority, make their weight vlaues total to 100. This makes it easier to identify each server's load as a percent of the total.

For example:

With this domain setup Server A handles approximately 80% of the session requests and Server B handles approximately 20%. If Server A is unavailable, then Server B will handle 100% of the session requests. Server C will only be asked to handle a session request if both Server A and Server B are unavailable. As soon as Server A or Server B becomes available then Server C will no longer be asked to handle a session request.

Server	Weight	Priority
Server A	80	0
Server B	20	0
Server C	100	1

Editing and Removing Session Servers and Domains

To....	In the Session Server Explorer, do this....
Edit domain session server properties	Select the domain whose server properties you want to edit, right-click and choose Properties. On the Properties page, select the session server, and then click Edit.
Remove a domain	Select the domain you want to remove, right-click, and choose Remove.

To....	In the Session Server Explorer, do this....
Remove session servers from a domain	Select the domain whose server properties you want to remove, right-click and choose Properties. On the Properties page, select the session server, and then click Remove.

More information

Working with Load Distribution Domains

2.3 Working with Host Integrator Session Servers

The Host Integrator Session Server provides seamless integration of host application data and business logic into client/server and Web applications. The session server supports multi-tier client/server and Web application architecture and is designed to provide concurrent access by thousands of Web application users to host information systems and applications. Using the Host Integrator Session Server, a single Web or client/server application can concurrently access data on a variety of host systems, such as:

- IBM mainframes and compatibles, using the Telnet and TN3270E (Telnet Extended) protocols.
- IBM AS/400 systems, using the 5250 terminal protocol via Telnet.
- VAX/OpenVMS and other ASCII hosts using the VT-420 terminal protocol, which includes VT-52 and VT-100 via Telnet.
- HP 3000 hosts, using the 700/92 terminal protocol via Telnet or NS/VT.

The Host Integrator Session Server works in conjunction with the Host Integrator Design Tool and the Host Integrator Software Connectors to integrate host application data and business logic into client/server and Web applications.

Using the Design Tool, a developer builds a model of a host application, accessing fields that contain information needed by the client application. The model is then loaded into Host Integrator Session Server. The model contains all the information about the host application, including its traversal logic, application screen signatures, and data attributes, and can be accessed from a variety of software development environments using an Application Programming Interface (API) included in the Host Integrator Development Kit. When the Host Integrator Session Server receives a request from a client application, it instantiates a host session using the logic stored in the model specified in the request. Host Integrator Session Server navigates through the host application, fetches the requested data, and returns it to the client application.

For more information about creating and working with models and working with Host Integrator connectors, see the Design Tool online help, which is included in the Host Integrator Development Kit.

2.3.1 Managing the Session Server

The Administrative Console provides a central hub where you can manage and monitor your session servers. You can add, remove, and configure directories, load distribution domains, security, and logging for session servers.

To have complete administrative control over the session server you must be logged in with an administrator profile.

To start managing your session servers, from the Host Integrator perspective, choose Session Servers, and open the Session Server Explorer. From here you can view and configure logging, notification, and various session server properties. Additionally, you can view and configure models that are deployed to the session server, model variable lists associated with the session server, and session pools.

More information

Viewing Server Properties

Adding a Session Server

Working with Session Pools

2.3.2 Adding a Session Server

In the Administrative Console you add session servers that you want to manage. When you install the session server it is either registered with an existing management server or with the management server that is also being installed. You can only register a session server with one management cluster at a time.

To add a session server

1. From the Session Server Explorer Servers node, click to add a session server. The Add Session Server dialog box displays.
2. Type the name of the session server you want to manage, and then click OK. The server displays in the Session Server Explorer tree. You can now configure the properties associated with the server.

Adding additional session servers

To add a session server post-install you must supply the address of the session server, either the machine name or IP address. A session server that can be contacted and is not already a part of another management cluster is added and the name will default to the address you supplied.

If the session server can be contacted, but is already part of a management cluster, an error message displays since a session server can only be a part of one management cluster.

If the session server cannot be contacted you can add it anyway. If you do so, it will not be added to a cluster until the server is online. When the server comes online and is part of another management cluster, error messages will display in the log, and the server will be offline to the second management server.

Load balancing and failover

In order to configure session servers in a Host Integrator load distribution domain:

- All session servers in a load distribution domain must share the same management server cluster.
- Each session server can be registered with only one management server cluster.
- Session servers can be members of multiple load distribution domains.

See Adding,Removing and Configuring Load Distribution Domains for instructions on setting up load distribution.

More information

- Working with Host Integator Session Servers
- Adding, Removing and Configuring Load Distribution Domains
- Working with Session Pools

2.3.3 Removing a Session Server from a Cluster

A session server can only be registered with one management server cluster. If you want to register a session server with a different management server cluster, you must first remove it from the existing cluster.

If you uninstall a session server while it is registered with a management cluster that is not uninstalled, you must remove the session server from the management server cluster before reinstalling the session server on the same machine. If this is not done, the management cluster thinks the session server is registered, but may not be able to communicate with it. If this occurs just remove the session server and re-add it.

Removing a session server from a management cluster does not affect its configuration.

To remove a session server from a management server cluster

If the session server is...	Then this...
Online	Select the session server you want to remove, right-click and choose Remove.
Offline	Depending on your operating system, run either the `HostIntegrator/bin/resetsessionserver.bat` or `resetsessionserver.sh` script before you add the session server to a different management cluster.
	- You can run the script while the session server is online, but the session server must be restarted for the script actions to take effect.
	- If you run the resetsessionserver.bat script on a system with UAC enabled, then you must run the script with administrator privileges.

More information

Adding a Session Server

Removing a Management Server From a Cluster

2.3.4 Configuring the Session Server to Run as a System Daemon

To have installed services start automatically when your system boots up

Command line options	Description
atstart -d	-d before other options logs debugging info
atstart -install `<component>`	install component as a daemon process
atstart -uninstall `<component>`	uninstall the daemon process
atstart -start `<component>`	start the daemon process
atstart -stop `<component>`	stop the daemon process

Command line options	Description
atstart -status `<component>`	display current status of component

Start and stop "all" starts or stops all five services and -status displays the status of all five components. For example:

```
alpjanw03:/opt/microfocus/verastream/hostintegrator/bin # ./atstart -status
LogMgr      Started
Server      Started
HostEmul    Started
MgmtServer  Started
WebServer   Started
```

1. Create a file called `vhi` containing the following and entering your installation directory: These instructions will start all services, including the management server if it is installed. To start a particular service, replace the parameters (`<component>`) with one of the following:
2. `server` —VHI session server

`mgmtserver` —VHI management server

`logmgmr` —VHI log manager

`hostemul` —VHI host emulator

`webserver` —VHI web server

`all` —all installed services (start and stop only)

```
### BEGIN INIT INFO
# Provides: VHI
# Required-Start: $network
# Should-Start: $network
# Required-Stop: $network
# Should-Stop: $network
# Default-Start: 3 5
# Default-Stop: 0 1 2 4 6
# Description: Micro Focus Verastream Host Integrator Services
### END INIT INFO
```

```
INSTALL_DIR=<enter installation directory>
BIN_DIR=$INSTALL_DIR/hostintegrator/bin
case "$1" in
start)
echo "Starting Verastream"
$BIN_DIR/atstart -start all
```

```
RETVAL=0
;;
stop)
echo "Stopping Verastream"
$BIN_DIR/atstart -stop all
```

```
RETVAL=0
;;
status) echo "Current Verastream status"
$BIN_DIR/atstart -status
```

```
RETVAL=0
;;
restart) echo "Restart Verastream"
echo "-- stopping all components --"
$BIN_DIR/atstart -stop all
echo "-- starting all components --"
$BIN_DIR/atstart -start all
```

```
RETVAL=0
;;
*)
echo "Usage: $0 {start|stop|status|restart}"
RETVAL=1
;;
esac

exit $RETVAL
```

1. On Linux platforms, follow these steps:
2. Copy the file to the `/etc/init.d` directory`
3. Set the file permission. Run `chmod` using the value 755. For example, `chmod 755 vhi`

Run `chkconfig` to add the initialization script. For example, `chkconfig --add vhi`

> **Note**
>
> Status information and error messages are written in the system log, which you can find in the MicroFocus\Verastream\ManagementServer\logs directory.
>
> Optional debug information is written in the vhi/etc directory
>
> For all command line options a return code of 0 indicates success and a non-zero return means that the command was unsuccessful.

More information

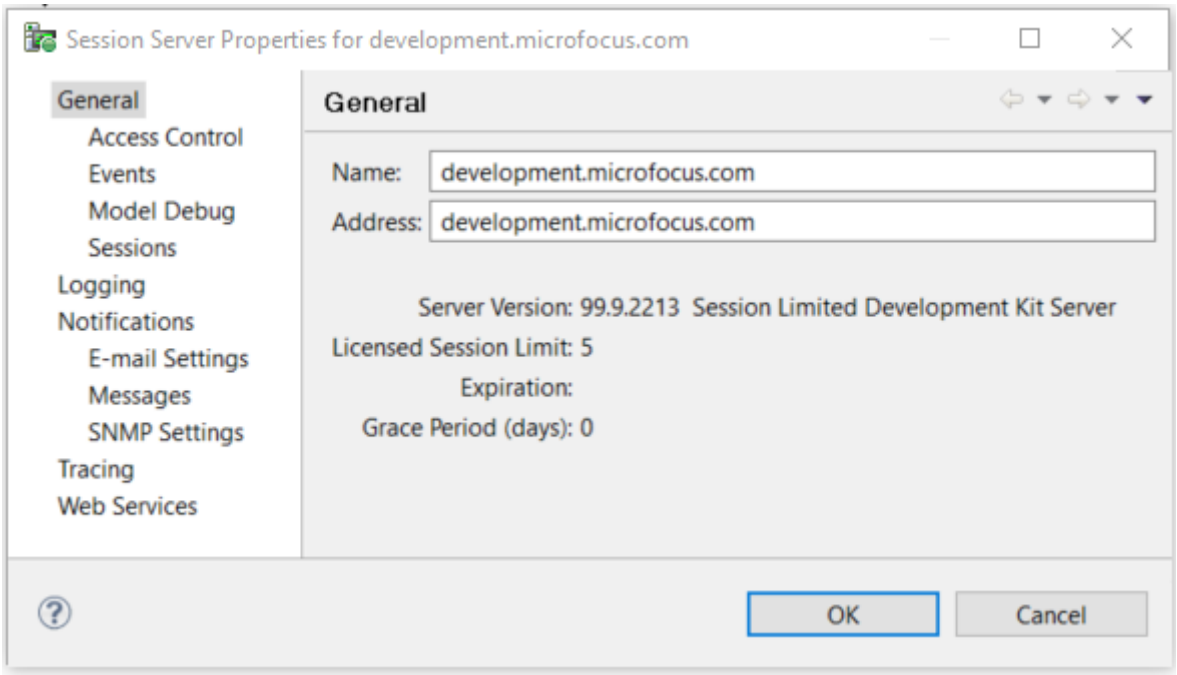
Removing a Session Server from a Cluster

Adding a Session Server

Working with Host Integrator Session Servers

2.3.5 Using Session Server Properties

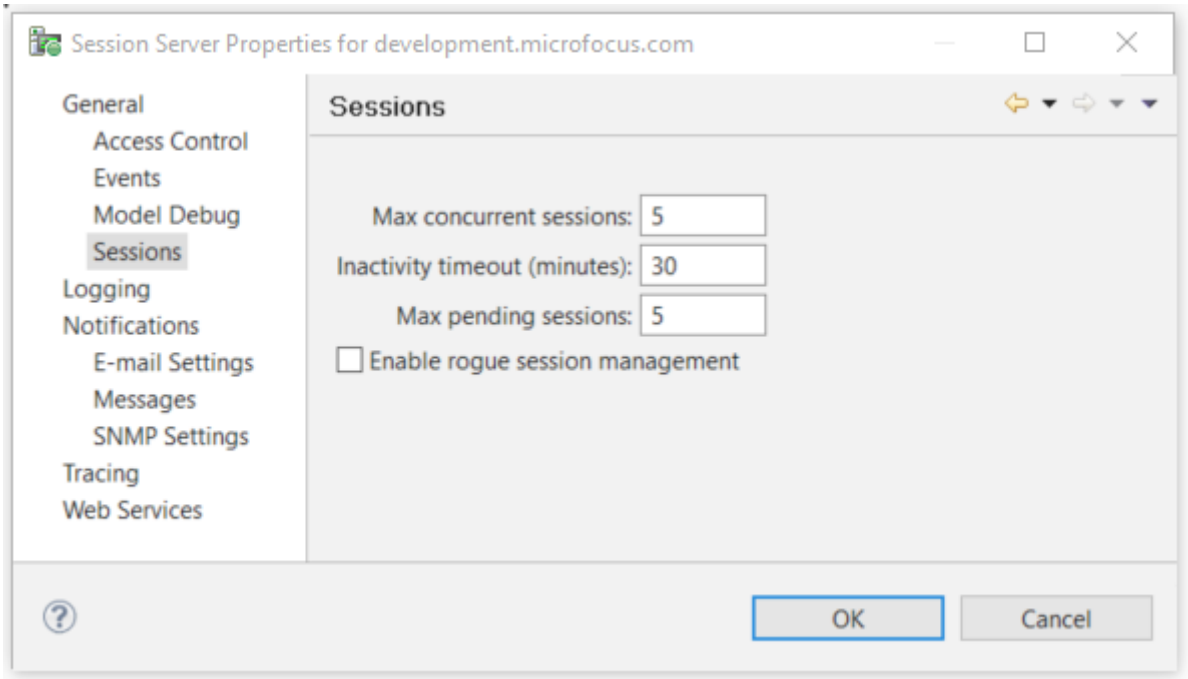
Each session server that you have added to the Session Server Explorer has a set of properties associated with it.



To view session server properties

In the Session Server Explorer tree, choose the server whose properties you want to view, right-click and choose Properties. Alternatively, you can click the Properties icon on the toolbar.

On the Properties dialog box, from the left pane, select the type of properties you want to view. Properties are separated into four categories; General, Logging, Notifications, Tracing, and Web Services.



Property categories	Available properties
General	The server name is case-sensitive. Be aware of this when using this information elsewhere in Host Integrator.
	- Events
	- Model Debug
	- Access Control
	- Sessions
Logging	Set system logging options, including deletion, storage location, and logging levels.
Notifications	-E-mail Settings
	- Messages
	- SNMP Settings
Tracing	Set tracing options, including the trace engine settings, maximum trace file size, and available trace nodes.

Property categories	Available properties
Web Services	Set options for the Web service configurations, including enabling HTTP or HTTPS connections and other WSDL elements. You can also decide whether to make Web services available for models and pools and link to the list of all available Web services.

More information

General Server Properties

Logging Server Properties

Notifications Server Properties

Tracing Server Properties

Web Services Server Properties

2.3.6 General Server Properties

These properties are specific to the selected session server.

Events

Set event handler options:

- **Disable event handler timeouts** controls the use of event handler timeouts on the server. If event timeout is enabled, the event timeout specified in the model is used. If event timeout is disabled, no timeouts are enforced when an event handler is processing an event.
- **Enable script manager debug port** allows you to enable or disable the debug port on the server. This port is used by the script manager for communicating with a Java debugger. You must restart the session server for this option to take effect.
- **Requested event handler debug port** is the port number from which the Host Integrator Session Server will start searching for an available remote debugging port. The session server looks first at port 5005.
- **Assigned event handler debug port** is the JVM remote debug port that is currently in use. If the requested debug port is unavailable, then a higher number will be requested until an available port is found.

2.3.7 Model Debug

When developing models in the Design Tool, model debug message recording is always on. When deploying models to the server, you can specify the model debug messages recording level as a deployment descriptor, or you can change Model Debug Message Recording in the Administrative Console's properties page. By default, the model debug messages recording level for a deployed model is to record nothing. When debugging, the recommended setting is to record errors only.

The settings below handle the size and location of the runtime model debug message recording files.

- Model Debug Messages Directory By default, this is in the \etc\reports directory for the Host Integrator installation. You can change the directory location on the local machine.

  Model debug message files (with a .vmr extension) are saved in a structure based on the time a server started. The time-stamped directory contains model debug message files named by model name and session ID, for example, CICSAccts.8.vmr. Since older .vmr files are automatically removed from the server (by default, after 7 days), you should copy the files (or increase or disable the cleanup thresholds) if ongoing analysis is necessary.

> **Note**
>
> Changing the setting for the directory will not take effect until the server is restarted.

- **Model Debug Messages Cache Size** The size of the in-memory buffer for model debug messages. The cache size is the amount of memory per session on the server. (For example, 500 concurrent sessions x 2 MB cache size = 1000 MB of system memory required.) When this limit is reached, the model debug message contents are written to the model debug messages file. The model debug message recording process continues, and additional messages are added to the file when appropriate.

  If you find that model debug message recording is slowing down the server, you may want to increase this value.

- **Model Debug Message Time Threshold** The amount of time that a model debug message file remains on the server. If Model Debug Message Space Threshold is set to 0, then daily maintenance is performed and any model debug message files older than the setting specified will be removed. The default is 7 days.

  If Model Debug Message Space Threshold is set to a number greater than 0, then hourly maintenance of model debug messages is performed and any model debug message older than the setting specified will be removed, regardless of disk space availability.

- **Model Debug Message Space Threshold** The amount of disk space, in MB, that is maintained for the most recent model debug message files. The model debug message directory is reduced to this size on an hourly basis, keeping the newest files that fit within this threshold. The reduction process removes oldest files when necessary. A good value for this setting is half of the maximum space for model that you want to allocate for model debug message files.

  If you want to enforce a maximum for model debug message space, it is recommended that you specify a dedicated virtual drive on the local machine.

Access Control

Enable access control Select this option to have all communication between the session server and the management server handled by means of SSL. When access control is enabled for a session server, an administrative login, while always required for the Administrative Console, will also be required for deploying models, generating Web applications, and executing connectors. See Working Securely for information on access control options.

FIPS Status Federal Information Processing Standards (FIPS) are guidelines established by the United States government to standardize computer systems. To use FIPS 140-2 validated encryption, in a Windows environment, you must define an environment variable, VHI_FIPS = 1.

Sessions

Set session options.

- Max Concurrent Sessions Max Concurrent Sessions is the maximum number of concurrent sessions that can run on this server. The range of values is 1 - 5000, and the default is 10.

  Max Concurrent Sessions must match the number of licenses purchased by your organization. If you are running multiple servers, the combined total of Max Concurrent Sessions on all servers must match the number of licenses purchased. For example, if you have three servers and you purchased 75 licenses, you can set Max Concurrent Sessions on your servers to 20, 25, and 30 respectively. You can divide the numbers any way you want, as long as the total on all servers does not exceed your number of licenses.

> **Note**
>
> On the server included with the Development Kit , the range of values is 1 - 5, and the default is 5.

Inactivity Timeout (minutes) The Inactivity Timeout is the number of minutes a data object-to-host session connection can be idle before the host session disconnects from the data object and either terminates or returns to its session pool. The range of values is 0 - 2147483647 and the default value is 30 minutes. Setting the Inactivity Timeout to 0 means the session will never time out.

> **Note**
>
> The inactivity timeout used for a session is the timeout that is in effect when the session connects. If you change the timeout, the new value will be used for sessions that connect after the change is saved to the server; it will not affect sessions that were connected when the change was made

- Max Pending Sessions The maximum number of sessions trying to connect to the host simultaneously. The actual number may be much less if the sessions start and login rapidly. The pools might not be able to keep up. This setting is intended to protect the host from a denial of service attack, not to guarantee performance.

  Set this option to at least 1 to ensure that pools are created concurrently. Higher values are recommended for optimal performance.

- Enable Rogue Session Management Rogue sessions within a session pool exhibit a circular behavior when attempting to log in and reconnect under conditions such as the following:

  There is an expired password within the model variable list

  A session fails to reach the defined starting point of a pooled session

  After logging in, a session fails to reach the home entity

You can configure the server to handle these rogue sessions so that they are "quarantined" until you have addressed the underlying problem. Select this option to enable rogue session management. When enabled, any session that has been suspended for any of the conditions described above is marked in the Sessions view list. This may helpful during development. However, during production this option should only be used to help diagnose problems.

Click on the Sessions view toolbar to only show rogue sessions.

More information

- Using Session Server Properties
- Logging Server Properties
- Notifications Server Properties
- Tracing Server Properties

2.3.8 Setting Log Properties

These properties are specific to the selected session server.

Logging

Host Integrator can log server errors and can issue warnings and informational messages as it runs.

Set logging options:

- **Default logging level** Specifies which events are inserted into the log files by default. These messages are also sent to the operating system log if system logging is enabled (see below). This is a server wide setting. Client applications also have the ability to increase the logging level for their own private sessions. To record all server activity, select Log All Messages. This will include in the log all informational messages, warnings, and errors. Because this setting requires the server to track all activity, expect additional resource consumption on the server.

  You may optionally select a reduced logging level for improved performance on heavily loaded servers.

- **Log storage directory** Specifies the directory in which log messages stored, which by default is `<installation directory>\VHI\etc\logs\server (Windows)` or `<installation directory>/vhi/etc/logs/server (Linux)`. An administrator can specify a different local directory where new messages are stored. The directory you specify must already exist. Any existing messages are transferred to the newly specified location.

- **System logging** With this option enabled Host Integrator sends logging messages to both the Host Integrator log files and the operating system log, which is the Event Log on Windows systems and the syslog daemon on Linux systems. Host Integrator also sends a message to the System Log when it detects a logging system failure, regardless of this setting.

> **Note**
>
> Host Integrator does not manage the size of the operating system log. When System Logging is enabled, you must take steps to limit the size of your system log.

- **Failed request information logging** This option helps you troubleshoot client application problems. When Failed Request Information Logging is enabled and the server encounters an error, the server writes all activity for the failed request to the log file. This information appears immediately before the error message in the log file. Because Failed Request Information Logging requires the server to track additional activity, enabling it consumes additional resources on the server.

  Failed Request Information Logging does not have to be enabled for request failures to be recorded; enabling this setting simply appends all activity associated with the failure in addition to the failure itself. When Failed Request Information Logging is disabled, the error itself is still logged.

> **Note**
>
> If Logging Level is set to Log All Messages, all activity is written to the log file even when no errors are encountered and regardless of the Failed Request Information Logging setting.

- **Delete logs when disk space exceeds threshold** When the Delete logs when disk space exceeds threshold check box is selected, the oldest log entries are deleted when the amount of disk space used by the log records exceeds the threshold. The oldest messages are deleted until space utilization is decreased to 80% of the configured maximum limit.
- **Log space threshold (in MB)** The total amount of disk space in MB that can be used to store log records. The default is 100 MB and the range of values is 1 - 100000 MB.

  In addition to the space required to store messages, the logging system requires administrative storage space. For proper function of the logging system, ensure that the actual free disk space in the configured logging directory is at least twice the value of the Log Space Threshold setting.

> **Note**
>
> The space and time thresholds can be enabled at the same time. In this case, the most restrictive setting is used.

- **Delete logs older than threshold** When selected, messages older than the specified threshold are purged.
- **Log time threshold (in days)** The expiration date for all log records. The default is 30 days, and the range of values is 1 - 100000 days.

> **Note**
>
> The space and time thresholds can be enabled at the same time. In this case, the most restrictive setting is used.

More information

Using Session Server Properties

General Server Properties

Notifications Server Properties

Tracing Server Properties

2.4 Notifications Server Properties

These properties are specific to the selected session server.

You can configure session servers to send e-mail notifications of server events to designated recipients.

There are three different property pages:

- **E-mail** This is where you setup and configure notifications and generate a test message.
- **SNMP** Configure the session server to use Simple Network Management Protocol (SNMP) to distribute status information.
- **Messages** Specify which messages will generate e-mail notifications and which will interact with the SNMP subsystem.

To enable Notifications

Select this option on the E-mail Settings property page.

More information

Configuring Messages

Configuring E-mail

Configuring SNMP

Using Session Server Properties

2.4.1 Configuring SNMP

You can use these options to configure the Host Integrator's SNMP system to suit the requirements of an individual organization.

- **Enable SNMP** Check this box to have the Host Integrator Server maintain use statistics and generate SNMP traps for selected events. If you want to deactivate SNMP, while maintaining other aspects of its configuration, clear this item.
- **SNMP Port** Enter the UDP port number you wish the Host Integrator SNMP agent to use to service SNMP GETs for statistical data. The default port number is 161.
- **SNMP Trap Destinations** If you plan to use SNMP traps, enter their destinations in this box. Enter one fully-qualified domain name or IP address per line for each Network Management Station (NMS) that you wish to receive traps. Traps are sent to UDP port 162 of each address listed in this item.
- **Seconds between duplicate** traps When identical, duplicate, trap-generating events occur rapidly within the Host Integrator Server, a buffering mechanism is used to prevent network saturation. The first occurrence of an event is reported immediately, while future occurrences, as well as the occurrence count, are not reported until the configured time has elapsed. Enter a duration of time, in seconds, that the Host Integrator Server should wait before sending duplicate event traps to configured trap recipients. By default, this option is set to 5 seconds. Enter an amount between 0 and 65535 seconds.

Specifying the Events that Generate SNMP Traps

To specify the Host Integrator events that generate SNMP traps, click Messages under Notifications in the Session Server Property page.

More information

Working with SNMP

Configuring Messages

Configuring E-mail

2.4.2 Configuring E-mail Options

You can configure Host Integrator servers to send e-mail notification of server events to a list of recipients. Use E-mail Settings to enable and configure e-mail notification and generate a test message.

To enable and configure e-mail notification:

Some fields are optional, while others are required. Required fields are denoted by an asterisk on the dialog box.

In the Session Server Explorer, choose the server you want to configure, and open the Properties page. Under Notifications, choose **E-mail Settings**.

Specify the E-mail settings you want to use.

Click Apply, and then click **Test Message** to verify that your configuration is correct. The Administrative Console does not report whether the test message was successful; the receipt of the message is your indication that the settings you entered are correct.

Click **Messages** in the left pane of the Properties page to specify which events you want to generate e-mail notifications for.

2.4.3 Settings

- **Enable E-mail notification**

  This configures the currently selected server to generate e-mail messages whenever an event specified in the E-mail Messages panel occurs.

- **E-mail address from which messages are sent**

  In this field, enter a single, valid e-mail address. This option specifies the e-mail address from which event notification messages are sent.

- **E-mail address to which messages are sent**

  In this field, enter a valid e-mail address, and then click Add after each address you enter. This puts each address on its own line. This is a required field.

- **E-mail server name or IP address**

  Specify the name or IP address of the mail server to which event notification messages should be sent. Enter a valid IP address or a valid network name. This is a required field. If

you have enabled SMTP authentication, the server name and address must be set to that of the SMTP server.

- **E-mail server port**

  Specify the port used by the mail server you specified. Most mail servers use port 25. This is a required field. If you have enabled SMTP authentication, the port must be set to that used by the SMTP server.

- **Subject field of the notification message**

  Specify the subject line for event notification messages. By default, this option is set to Host Integrator Notification. This is a required field.

- **Text added to the error text in the body of the notification message**

  Specify a message to be sent along with event notification messages. This option is not required, and is blank by default. It can contain up to 255 characters, and will be the first line of all messages that are sent.

- **Enable SMTP authentication**

  Select this option to turn on Simple Mail Transfer Protocol (SMTP) authentication. SMTP is an Internet standard for transmitting e-mail. This option is not enabled by default. SMTP authentication requires that you supply username and password values for the SMTP server.

Advanced SMTP settings

There are three advanced settings for SMTP. These settings are used to add customized functionality at the socket level. For more information on sockets, see the Java tutorial, All About Sockets.

These settings are configured in the logmgr.conf file, located in the HostIntegrator/etc/ directory of your installation. If you make any changes to this file, you must restart the server before the changes take effect.

- **mail.smtp.socketFactory.port**

  Specifies the port to connect to when using the specified socket factory. If not set, the default port is used.

- **mail.smtp.socketFactory.class**

  If set, specifies the name of a class that implements the javax.net.SocketFactory interface. This class will be used to create SMTP sockets.

- **mail.smtp.socketFactory.fallback**

  If set to true, failure to create a socket using the specified socket factory class will cause the socket to be created using the java.net.Socket class. Defaults to true.

```
For example:
        java.additional.4=Dmail.smtp.socketFactory.port=465
        java.additional.5=Dmail.smtp.socketFactory.class=javax.net.ssl.SSLSocketFactory
        java.additional.6=Dmail.smtp.socketFactory.fallback=true
```

Your values may be different. For more information on these settings, see JavaMail API.

More information

Configure Messages

Configure SNMP

2.4.4 Configuring Messages

These properties are specific to the selected session server. To enable and configure message options, click Messages in the left pane of the Properties page for the selected server.

Messages

In the Messages property page you can specify the messages that will generate e-mail notifications.

Find message You can search for a specific message. Enter either the number of the message or a text string. As you enter the number of the message or a text string, the matching messages display in the All Messages tree.

Click  to erase any text in the Find text field.

- **Message filters** You can filter the messages based on these options.

  Email enabled

  Monitor in SNMP MIB enabled

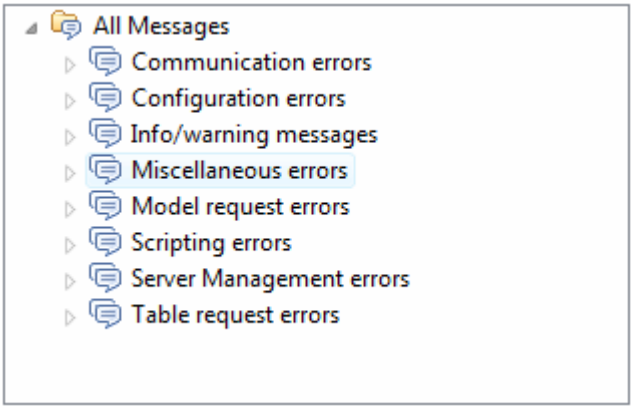
  SMNP Trap/Monitor in SNMP MIB enabled

  Show modified configuration— This option finds messages that no longer have a default configuration.

List of messages

You can select the error and information messages, or groups of messages, that will generate e-mail notification messages. To do this, select the message or message group you want in the All Messages tree. For example, if you select **Communication errors**, all the errors in that group will generate a message. You can, however, select just one message by expanding the Communication errors node and selecting the specific message.

After you've selected the error messages you want to use, click Apply.



Right information pane

- **Group** The node under which the message selected is located.
- **Description** The description of the selected message.
- **ID** The ID number of the selected message.
- **Type** The type of message; error, info or warnings.
- **Notification settings** Select Send e-mail notification to send an e-mail notification to the list of recipients designated on the E-mail Settings page.
- **SNMP property** You can choose which SNMP property you want to use.

  Don't monitor with SNMP— select this option if you do not want the SNMP subsystem to track occurrences of this message.

  Monitor in SNMP MIB— select this option if you want the SNMP subsystem to track occurrences of this message. When a Network Management Station performs an SNMP GET for monitored events, the Host Integrator Server will include occurrences of this message in the response.

  Send SNMP trap and monitor in SNMP MIB— When this message occurs, send an SNMP trap to all configured Network Management Stations in addition to tracking occurrences in the MIB.

See Configuring SNMP for more information on these properties.

More information

Using Session Server Properties

Configuring SNMP

Configuring E-mail Options

2.4.5 Setting Tracing Properties

These properties are specific to the selected session server.

Host Integrator session server tracing is a diagnostic tool which is available for you to use in conjunction with technical support to troubleshoot various session server problems such as transport difficulties or session problems. Since only development staff and technical support can read traces generated by Host Integrator, the only reason to configure these properties is if you have been instructed to do so by technical support.

Tracing

To start the trace engine you must first provide a trace file name. Once you've finished configuring the tracing properties, to start the trace, right-click on the session server in the Session Server Explorer, and choose **Start Trace**.

To stop the trace engine, right-click on a session server and select **Stop Tracing**.

Set trace engine options:

- **Trace file name** Type the name of the trace file. For example, a path name such as `C:\Program Files\VHI\Trace.trc (Windows)` or `/usr/local/vhi/trace.trc` (Linux) means that the trace file is on the same machine as the Host Integrator server. If you want the trace to be generated on a machine other than the machine running the server, you must enter the fully qualified network path name. The directory location you specify for the trace file must exist and the file name must be valid for the trace engine to start.
- **Max trace file size** Enter the maximum amount of disk space that the server can use to create trace files. Enter a value between 0 and 1024 MB.

> **Note**
>
> Setting the maximum trace size to 0 means that the trace size is unlimited and the server will continue to send data to the trace file until the problem occurs or there is no more available disk space. When tracing is active, the server writes trace data to the trace file until the file is half the maximum trace file size. The server then creates a second file, appending a 2 to the trace file name, and sends trace data to the second file until it is the same size as the first. It then starts overwriting the data in the first trace file.

- **Trace new sessions** Select this option if you want new sessions to have tracing activated when they are allocated. In some cases, selecting this option may slow server activity to the point where the problem is masked.
- **Trace server startup** Select this option to have Tracing start as soon as the server is started.

Enable trace nodes Select the events that you want collected in the trace. To do this, select the appropriate categories in the navigation tree. Technical support will tell you which nodes to select.

Trace configuration files

In some cases technical support may provide a trace configuration file that you will load instead of enabling tracing nodes.

To load a trace configuration file:

Right-click anywhere on the Trace Nodes tree and select Load Trace Configuration File.

From the dialog box, select the file you want to load.

After the file is loaded, the trace node tree indicates what trace nodes were enabled in the file.

More information

Using Session Server Properties

Logging Server Properties

General Server Properties

2.4.6 Setting Web Services Session Server Properties

The session server Web services property page displays information and options for the Web service associated with the selected session server. Click OK for the changes you make to take effect; it is not necessary to restart the session server.

After you make changes to Web service configurations, you may have to reconfigure your clients (by importing the new WSDL) to continue using them.

- **Enable HTTP Web services** — Select this option to provide an HTTP connection to the Web service. Click the link to open your default browser to the list of available Web services. If the link is not visible, you may have a port conflict. The default port is 9680.

  From the right-click context menu, click **Copy URL** to copy the Web services URL address to the clipboard.

- **Enable HTTPS Web services** — Select this option to provide an HTTPS secure connection to the Web service. Click the link to open your default browser to the list of available Web services. If the link is not visible, you may have a port conflict. The default port is 9681.

  From the right-click context menu, click **Copy URL** to copy the Web services URL address to the clipboard.

- **Publish Web services for models (non-pooled sessions)** — Select this option to make Web services available for all non-pooled sessions.
- **Publish Web services for pooled sessions** — Select this option to make Web services available for all pooled sessions.
- **Enable WS-Addressing and WS-Resource** — This setting is specific to SOAP Web services and does not affect REST services. If you are using SOAP services, select this option to have WS-Addressing and WS-Resource elements listed in the WSDL file. If you disable this option, the Web service still executes requests using these elements, but the WSDL will not contain these elements. This can make the WSDL easier for some clients to consume. Stateful Web services are still available with inbound support.
- **Enable executeSQLStatement Web method** — Select this option to use the executeSQLStatement method. If you disable this option, the WSDL element and schema datatypes are removed from the WSDL and a client will not be able to execute this Web method.
- **Enable processString Web method** — Select this option to use the processString event handler method. If you disable this option, the WSDL element and schema datatypes are removed from the WSDL and a client will not be able to execute this Web method.
- **Method timeout** — The number of milliseconds to wait for a procedure to complete. If the timeout expires clients will receive a SOAP fault indicating the timeout condition.
- **Suspend timeout** — The time, in minutes, that a session remains suspended. This timeout takes effect when you are using stateful Web services. If the timeout period is exceeded, the session is reclaimed, and clients will receive a SOAP fault stating that the session is no longer available when a stateful Web service attempts to execute against the session.
- **Specify a custom namespace for the pool** — Specify a custom namespace for the session server to use during deployment.
- **Restore Defaults** — Click Restore Defaults to restore the default settings for this property page.

More information

Changing Host Integrator Port TCP Numbers

Deploying a Model

Setting Model Level Web Service Properties

Using Session Pool Properties

Using Session Server Properties

2.4.7 Using Model Properties

The Models property page displays information and options for a selected model that is deployed to the session server.

- **Host name** — The host the model connects to from this server. The name specified here overrides the name stored in the model.
- **Host port** — The port ID for the host connection. The port ID specified here overrides the port ID stored in the model.
- **Model debug messages recording** — The model debug message reporting level for the model. Options include Disabled, Record Errors, Record Error Sessions, and Record Everything. Use the Design Tool Model Debug Messages tool to troubleshootand debug your model.
- **Version** — The timestamp of the last time the model was saved.
- **Startup entity** — The name of the entity that host session connections made with this model will navigate to after the connection is made.
- **Variables** — A list of all the variable names defined for this model.

More information

Deploying a Model

Setting Model Level Web Service Properties

Working with Session Pools

2.4.8 Setting Model Level Web Services Properties

The model level Web services property page displays information and options for the Web service associated with the selected model that is deployed to the session server. If you choose to override the session server values for a particular model, those settings are displayed in boldface. To see the configured session server Web service properties, click Open **Session Server Properties**.

- **Override session server settings** — Select this option to customize the session server properties on a model-level basis. When you select this option you can set the following options for the selected model.
- **Publish Web services for this model (non-pooled sessions)** — Select this option to make the Web service available for non-pooled sessions associated with a particular model.
- **Enable WS-Addressing and WS-Resource** — This setting is specific to SOAP Web services and does not affect REST services. If you are using SOAP services, select this option to have WS-Addressing and WS-Resource elements listed in the WSDL file for this selected model. If you disable this option, the Web service will still execute requests using these elements, but the WSDL will not contain these elements. This can make the WSDL easier for some clients to consume.
- **Enable executeSQLStatement Web method** — Select this option to use the executeSQLStatement method on the selected model. If you disable this option, the WSDL element and schema datatypes are removed from the WSDL and a client will not be able to execute this Web method.
- **Enable processString Web method** — Select this option to use the processString event handler method with the selected model. If you disable this option, the WSDL element and schema datatypes are removed from the WSDL and a client will not be able to execute this Web method.
- **Method timeout** — The number of milliseconds to wait for a procedure to complete. If the timeout expires, clients will receive a SOAP fault indicating the timeout condition.
- **Suspend timeout** — The time, in minutes, that a session remains suspended. This timeout takes effect when you are using stateful Web services. If the timeout period is exceeded, the session is reclaimed, and clients will receive a SOAP fault stating that the session is no longer available when a stateful Web service attempts to execute against the session.
- **Specify a custom namespace for the model** — Choose a custom namespace for the model to use during deployment.
- **Show WSDL** — Click either HTTP or HTTPS (secure connection) to open the WSDL in the default browser. From the right-click menu, select **Copy URL** to copy the URL to the WSDL to the clipboard.

  The links will be disabled if you have not enabled the HTTP or HTTPS Web services options in the session server Web services property page or have not published the Web services.

More information

Deploying a Model

Web Services Server Properties

Working with Session Pools

2.4.9 Working with SNMP

Host Integrator Servers can be configured to use Simple Network Management Protocol (SNMP) to distribute status information. The SNMP system uses a Network Management Station (NMS) of your choice to gather information about agents on your network. Host Integrator acts as an SNMP agent.

SNMP uses two communication methods:

SNMP GET, which services Network Management Station requests to UDP port 161, by default.

> **Note**
>
> Some Linux systems use port 161 as the default for SNMP. If the Verastream configuration uses the same port, no data will be returned. You may not notice the port conflict until you request statistics. Change the Host Integrator SNMP port number to something other than 161 to address the problem.

SNMP TRAP, which asynchronously sends an event to configured Network Management Stations listening on UDP port 162.

Host Integrator supports both of these methods.

Using SNMP GETs

A GET is initiated when the NMS asks a Host Integrator Server (the agent), for information about its status. The NMS gathers information from agents using a Management Information Base (MIB), which specifies the structure and format of the information that is passed between the NMS and an agent. The NMS can use this information to track the general health of a Host Integrator Server and chart performance trends over time.

Using SNMP TRAPs

When the Host Integrator Server is configured to use traps, it sends a message (trap) to all configured management stations whenever certain events or error conditions occur. The trap contains little information (the event ID). Its purpose is to trigger the NMS so that it can perform an SNMP GET for more information, if desired, from the originating server.

Working with the Host Integrator MIB

The host integrator MIB file, vhi.mib, describes the types of information the Host Integrator makes available via SNMP to a Network Management Station. It is installed by default to the `HostIntegrator\lib\java\` folder when you install the server. In most cases, you should copy the MIB on to an NMS workstation and load it into your NMS application of choice. The format of vhi.mib follows a standard defined by the IETF RFC 1155, which can be viewed on the IETF Web site.

The information provided in the Host Integrator MIB can be divided into three broad categories:

Statistics on the usage of configured models and the performance of their respective host application.

Statistics on the usage and load of configured session pools.

Statistics on the occurrences of errors and other events within the Host Integrator Server.

For a list of specific data items provided within the above categories that are available via SNMP, see the contents of the vhi.mib file installed with the product.

Configuring Host Integrator SNMP Features

To configure SNMP, click SNMP Settings in the left pane of the Session Server Properties page.

To select the messages that are monitored by SNMP, click Messages in the left pane of the Session Server Properties page, and then click a category of messages. By default, all messages at error severity generate traps and are monitored in the SNMP MIB.

More information

Configuring Messages

Configuring E-mail

2.4.10 Using the Session Monitor

You can use the session monitor within the Administrative Console to view and navigate between real-time screens of host session that are running on a given session server.

Viewing Sessions

After you connect to a session server, you can view active sessions on that server.

To view a session or session pool

Connect to the session server that contains the session you want to view.

In the Sessions view, select the session associated with the pool on the session server, right-click and choose View.

A session view window opens, displaying the session you selected. The current state of the session is represented, including the cursor position. The session window displays a real time view of the state of the session. All entity navigations and attribute updates are visible.

Session states visible in session monitor

There are 5 session states that are represented within the session monitor. They are:

Idle - released from client, reset and ready to use. When idle sessions are created, they may briefly display Not Connected before connecting to the host.

Active - in use by a client, or being told to disconnect from the host.

Rogue - released from client, not reset, and not ready to use.

Suspended - a persistent session waiting for a reconnect to occur.

Terminated - normally a transient state signalling the end of the session.

Troubleshooting using the session monitor

You can use the session monitor view to collect the session's screens. This makes finding errors easier, especially for sessions in which the host interaction is rapid. Any change to the host screen causes the Session Monitor to record the current screen as a record.

More information

Working with Session Pools

Working with Host Integrator Session Servers

2.5 Working with Session Pools

2.5.1 Session Pools

Session pools are a set of host sessions that you preconfigure for access by data objects. You can configure these host sessions with model variables and a starting entity, which provides faster host session allocaton and access to the host system because the host session can be logged on and waiting at the host application's main entry screen (entity) when a data object is ready to use it. This ability significantly enhances the Host Integrator's performance.

The Pools View

The Administrative Console provides a Pools view that contains the data you need to monitor your session pools.

To open the Pools view

- From the Host Integrator perspective, open the **View** menu, and select **Pools**.

  This view shows pools that are associated with the objects you select in the Session Server Explorer or other views in the Administrative Console.

Creating Session Pools

To create a pool you must have at least one model deployed to the session server. You can deploy models using the Design Tool or on the command line. See the Design Tool help for instructions.

To create a session pool

1. From the Session Server Explorer tree, select **Pools** under the appropriate session server, and then right-click and choose **Add Pool**.

1. The Add Session Pool dialog box is displayed.
2. Specify the name of the pool.

2. When you create a new session pool, it is assigned, by default, the name `Pool-1` (or whatever number is appropriate). You can specify any name you want.
3. From the **Models to use** drop down list, select the model you want to associate with the new pool.

3. The Start pool option is enabled by default. This option starts the pool as soon as it is created.
4. Clear the **Start pool** checkbox to delay starting the pool and then click **Next**.

4. The Session Pool Details panel displays.
5. Determine the details for the new session pool.

5. Session pool options include session management and host information. For complete descriptions of these settings, see Session Pool Details.
6. Click **Next** to configure more advanced options or click **Finish** to complete creating the session pool.
7. If needed, complete the **Advanced Session Pool Details** panel.(For descriptions of these settings, see Advanced Session Pool Details.
8. Click **Finish**. The pool is added to the Pools view and it's associated session information is added to the Sessions view. You can open both of these views using the View menu.

You can add model variables to the session pool and set pool scheduling options using the Pool Properties page.

To open the property page

Click on the toolbar or right-click the pool name in the Session Server Explorer and choose **Properties**.

Viewing Session Pool Options

The following options are displayed in the Add Session Pool panels for each individual session pool:

SESSION POOL DETAILS

Max concurrent sessions Specifies the maximum number of concurrent sessions that can be active in this pool. This is the "high water mark" for the number of sessions that can be created. The value you specify for this option cannot exceed the server's global setting Maximum concurrent sessions, or your licensed session limit. If the session pool has the maximum number of clients connected, any additional runtime client connection request will result in an exception. You can configure the server to automatically notify an administrator when this situation arises by using email configuration or SNMP configuration.

Initial idle sessions Specifies the number of sessions that are preloaded by the server. This is the number of sessions that a server should preconnect. The idle session count cannot exceed the server's global setting Maximum concurrent sessions or your licensed session limit, which is displayed as the maximum value for this option. If the session pool uses a model variable list, plan for enough model variable list entries for the expected (or maximum) number of concurrent sessions. Otherwise, when all entries are used, any attempt by an additional client to connect to the session pool will result in an exception.

Use **Max pending sessions** to control how quickly the sessions are preloaded.

Setting **Initial idle sessions** to a number equal to the expected number of concurrent sessions may provide better server performance.

Min idle sessions Minimum number of idle sessions to maintain.

Max idle sessions Maximum idle sessions cannot exceed the Maximum concurrent sessions defined for the pool, or your licensed session limit, which is displayed as the maximum value for this option.

Startup entity Specifies the entity the host session will be initialized to when a data object attaches to the host session. If the host session is returned to the pool when the data object releases it, it will automatically return to this entity for the next data object.

Host name Specifies the host the sessions in the pool connect to. The name specified here overrides the name stored in the model.

Host port Specifies the host port ID that the sessions in the pool connect to. The port ID specified here overrides the port ID stored in the model.

ADVANCED SESSION POOL DETAILS

Connection throttle delay (seconds) The amount of time to wait since the last host connection before attempting another. This option is often set to zero; it is usually preferable to use Max Pending Sessions.

Max retry backoff (minutes) Each time there is an error starting host sessions in a pool, the pool waits for an increasing amount time before trying again (it backs off). This option limits the retry backoff so the delay doesn't become too long.

Max pending sessions The maximum number of sessions trying to connect to the host simultaneously. The actual number may be much less if the sessions start and login rapidly. The pools might not be able to keep up. This setting is intended to protect the host from a denial of service attack, not to guarantee performance.

Model Debug Messages Recording Specifies the model debug reporting status for the model. Options include Disabled, Record Errors, Record Error Sessions, and Record Everything. Use the Design Tool Model Debug Messages feature to troubleshoot and debug your model. Configure recording options on the Server Properties page of the Administrative Console.

More information

- Using Session Server Properties
- Scheduling Session Pools
- Working with Model Variable Lists
- Deploying a Model
- Scheduling Session Pools

Using Session Pool Properties

2.5.2 Using Session Pool Properties

To view and modify session pool properties, select the pool you want to work with, and click toolbar icon on the Session Server Explorer toolbar.

There are five groups of session server properties:

General

Model

Model Variable Lists

Model Variables

Schedule

Web Services

General

You can modify the options set when you created the session pool.

- **Max concurrent sessions** Specifies the maximum number of concurrent sessions that can be active in this pool. This is the "high water mark" for the number of sessions that can be created. The value you specify for this option cannot exceed the server's global setting Maximum concurrent sessions, or your licensed session limit. If the session pool has the maximum number of clients connected, any additional runtime client connection request will result in an exception. You can configure the server to automatically notify an administrator when this situation arises by using email configuration or SNMP configuration.
- **Initial idle sessions** Specifies the number of sessions that are preloaded by the server. This is the number of sessions that a server should preconnect. The idle session count cannot exceed the server's global setting Maximum Concurrent Sessions or your licensed session limit, which is displayed as the maximum value for this option. If the session pool uses a model variable list, plan for enough model variable list entries for the maximum number of concurrent sessions. Otherwise, when all entries are used, any attempt by an additional client to connect to the session pool will result in an exception.

Use Max Pending Sessions to control how quickly the sessions are preloaded.

Setting Initial idle sessions to a number equal to the expected number of concurrent sessions may provide better server performance.

- **Min idle sessions** Minimum number of sessions to maintain.
- **Max idle sessions** Maximum idle sessions cannot exceed the Maximum concurrent sessions defined for the pool, or your licensed session limit, which is displayed as the maximum value for this option.
- **Connection throttle delay (seconds)** The amount of time to wait since the last host connection before attempting another. This option is often set to zero; it is usually preferable to use Max Pending Sessions.
- **Max retry backoff (minutes)** Each time there is an error starting host sessions in a pool, the pool waits for an increasing amount time before trying again (it backs off). This option limits the retry backoff so the delay doesn't become too long.
- **Max pending sessions** The maximum number of sessions trying to connect to the host simultaneously. The actual number may be much less if the sessions start and login rapidly. The pools might not be able to keep up. This setting is intended to protect the host from a denial of service attack, not to guarantee performance.
- **Model Debug Messages Recording** Specifies the model debug reporting status for the model. Options include Disabled, Record Errors, Record Error Sessions, and Record Everything. Use the Design Tool Model Debug Messages feature to troubleshoot and debug your model. Configure recording options on the Server Properties page of the Administrative Console.

Model

You can modify the model and host information for a session pool.

- **Model to use** From the drop down list, select the model associated with the session pool.
- **Startup entity** Specifies the entity the host session will be initialized to when a data object attaches to the host session. If the host session is returned to the pool when the data object releases it, it will automatically return to this entity for the next data object.
- **Host name** Specifies the host the sessions in the pool connect to. The name specified here overrides the name stored in the model.
- **Host port** Specifies the host port ID that the sessions in the pool connect to. The port ID specified here overrides the port ID stored in the model.

Model Variable Lists

Model variable list property page contains a table of all lists available to the pool and a table containing those lists that cannot be used by the pool for stated reasons. To add a model variable list, in the Session Server Explorer, right-click on Model Variable Lists, and select Add Model Variable List.

Model Variables

The Model variables property page contains a list of the variables defined in the model associated with the session pool. From this page, you can also add, edit, or remove fixed value model variables for the pool. See Working with Model Variables for more information about these options.

Schedule

The pool schedule table contains the information supplied when scheduling pool start and stop activities.

To set up a schedule for the pool, click Add. The Add Schedule dialog box displays. See Scheduling Session Pools for information on how to create a pool schedule.

Web Services

The Web services property page contains settings to configure the Web service for the associated session pool. This is where you can override the session server properties set for the Web service and view the WSDL file. If you choose to override the session server values for a particular session pool, those settings are displayed in boldface. To see the configured session server Web service properties, click Open Session Server Properties.

Override session server settings Select this option to customize the session server properties on a pool-level basis. When you select this option you can set the following options for the selected pool.

Publish Web services for pooled sessions Select this option to make the Web service available for sessions associated with a particular pool.

Enable WS-Addressing and WS-Resource This setting is specific to SOAP Web services and does not affect REST services. If you are using SOAP services, select this option to have WS-Addressing and WS-Resource elements listed in the WSDL file for this selected pool. If you disable this option, the Web service will still execute requests using these elements, but the WSDL will not contain these elements. This can make the WSDL easier for some clients to consume.

Enable executeSQLStatement Web method Select this option to use the executeSQLStatement method for the selected pool. If you disable this option, the WSDL element and schema datatypes are removed from the WSDL and a client will not be able to execute this Web method.

Enable processString Web method Select this option to use the processString event handler method with the selected pool. If you disable this option, the WSDL element and schema datatypes are removed from the WSDL and a client will not be able to execute this Web method.

Method timeout The number of milliseconds to wait for a procedure to complete. If the timeout expires, clients will receive a SOAP fault indicating the timeout condition.

Suspend timeout The time, in minutes, that a session remains suspended. This timeout takes effect when you are using stateful Web services. If the timeout period is exceeded, the session is reclaimed, and clients will receive a SOAP fault stating that the session is no longer available when a stateful Web service attempts to execute against the session.

Specify a custom namespace for the pool Specify a custom namespace for the pool to use during deployment.

Show WSDL Click either HTTP or HTTPS (secure connection) to open the WSDL in the default browser. From the right-click menu, select Copy URL to copy the URL to the WSDL to the clipboard. The links will be disabled if you have not enabled the HTTP or HTTPS Web services options in the session server Web services property page or not published the Web services.

More information

- Using Session Server Properties
- Scheduling Session Pools
- Working with Model Variable Lists
- Deploying a Model

2.5.3 Scheduling Session Pools

You can set up a schedule that automatically starts, stops, or restarts the session pool. To create a schedule, from the Session Server Explorer, select the pool you want to schedule, right-click Properties, and choose Schedule.

A pool can support multiple schedules.

Creating a Schedule

1. In the right pane of the Schedule property page, click **Add**. The Add Schedule dialog box displays.
2. Provide a meaningful name and description for the schedule.
3. Select which command you want the schedule to execute; Start, Stop, or Restart.
4. Select **Force stop/restart** to ignore the status of the pool when stopping or restarting. By default, if a pool contains a number of sessions (one of which is in use and running, while the others are idle) and a stop event is scheduled, the idle sessions will be stopped. However, the

session in use will be allowed to finish it's task before being stopped. If you check Force stop/ restart the session is stopped regardless of its status.

5. Set the date and time for the scheduled event. You can either choose to select the exact day of the month for the event, or set up an ongoing event, such as the second Tuesday of the month. As you choose the date and time a Cron expression is built in the Cron expression field.
6. Select **Enable** and click **OK** to activate the schedule.

After scheduling a task, the schedule, including its values, displays in the Schedule table. You can enable and disable the scheduled task from this table using the Enabled column check box.

Creating your own Cron expression

Cron expressions are strings that you can use to create and trigger schedules to execute a routine, such as: "At 10:00 am every Tuesday". Cron is a Linux tool that has well-tested scheduling capabilities.

You can use the Add Schedule dialog box to build your Cron expression, or you can manually write your own expression in the Cron expression field.

Cron expression details are available on the Internet. Here are a few basic examples and formatting information.

FORMAT

Cron expressions are strings that consist of 6 or 7 fields separated by white space. There are allowed values for each field and special characters that you can also use.

Field name	UIs the field mandatory?	Supported values	Supported special characters
Seconds	Yes	0-59	, - * /
Minutes	Yes	0-59	, - * /
Hours	Yes	0-23	, - * /
Day of the month	Yes	1-31	, - * ? / L W C
Month	Yes	1-12 or JAN-DEC	, - * /
Day of the week	Yes	1-7 or SUN-SAT	, - * ? / L C #

Field name	UIs the field mandatory?	Supported values	Supported special characters
Year	No	empty, 1970-2099	, - * /

Note

In a Cron expression forward slashes denote increments of time. For example, 1 / 2 in the Months field indicates January and every 2 months thereafter. You cannot use the text equivalent of the month (JAN) to express the same message. While the dialog box will accept JAN / 2, it does not actually schedule the event.

SPECIAL CHARACTERS

- Use # ** ("all values") to select all values within a field. For example, "" in the minute field means "every minute". The names of the months and days are not case sensitive.
- If you are setting firing times between midnight and 1:00 am, be aware that daylight savings can cause problems when the time moves forward or back.
- The C character is not fully implemented in Cron, but specifies that the values are to be calculated against an associated calendar, if there is one. "1C" in the day-of-week field means "the first day included by the calendar on or after Sunday".
- You can enter unsupported characters in the Cron field, however the scheduler will ignore any portion of the expression that follows the unsupported character. For example, x x x @ x x, where x is a supported character and @ is not, the scheduler will read x x x.

See examples for a more detailed explanation.

Special character	Description
*	An asterisk indicates that the cron expression matches for all values of the field. For example, using an asterisk in the 4th field (month) indicates every month.
Minutes	?* No specific value.
Hours	-* Specifies ranges. "9-11" in the hour field means 'the hours 9,10, and 11'.
Day of the month	,* Specifies additional values. "MON,WED,FRI" in the day-of-week field means "the days Monday, Wednesday, and Friday".
Month	/* Specifies increments. "0/15" in the seconds field means "the seconds 0, 15, 30, and 45".

Special character	Description
Day of the week	L* ("last") Specifies different things depending on the field in which it is used. "L" in the day-of-month field means "the last day of the month" (day 31 for January, day 28 for February on non-leap years).Used alone in the day-of-week field, it means "7" or "SAT". However if you use it in the day-of-week field after another value, it means "the last xxx day of the month" - for example "6L" means "the last Friday of the month". When you use the 'L' option do not specify lists or ranges of values to avoid confusing results.
Year	#* Specifies 'the nth' XXX day of the month. '6#3' in the day-of-the-week field means the third Friday of the month (day 6 = Friday, #3 = the third one in the month). '4#5' means the fifth Wednesday of the month.

Special character	Description
W (weekday)	Specifies the weekday (Monday-Friday) nearest the given day. '15W' in the day-of-the-month field means the nearest weekday to the 15th of the month. If the 15th is a Saturday, the trigger will fire on Friday the 14th.

L and W characters can be combined in the day-of-the-month field ('LW') which means the last weekday of the month.

The question mark (?) is a non-standard character. It is used instead of '*' for leaving either day-of-month or day-of-week blank.

Examples:

```
Expression Schedule Trigger Description
0 0/5 14,18 * * ?  Every 5 minutes starting at 2 pm and ending at 2:55 pm, AND every 5 minutes starting at 6 pm and ending at 6:55 pm, every day
0 15 10 ? * MON-FRI 10:15 am every Monday, Tuesday, Wednesday, Thursday and Friday
0 15 10 * * ?  10:15 am every day
0 15 10 15 * ?  10:15 am on the 15th day of every month
0 10 10 10 10 ?  Every October 10th at 10:10 am
```

More information

- Using Session Server Properties
- Working with Model Variable Lists
- Deploying a Model
- Viewing Session Pool Options
- Using Session Pool Properties
- Creating Session Pools

2.6 Working with Model Variable Lists

When you build a model in the Host Integrator Design Tool, you can create model variables, which are placeholders for data. Situations where model variables are useful include:

- The same fixed model variable value needs to be used for all sessions in a session pool.
- Host user IDs and passwords must be provided for all sessions in a session pool, rather than being provided by the user.

You can accomplish these same tasks by configuring your session pools to provide values for the model variables in the models in your session pools. To use the value for all sessions in a pool, configure an individual model variable. If you need to provide a unique model variable value for each session in the pool, create a model variable list that contains a set of values for the model variables in the model on which your session pool is based.

> **Note**
>
> When the data object provides a value for a model variable, it overrides any model variable values that have been assigned in the Administrative Console.

For more information about creating model variables in the Design Tool, search for "Model variable" in the Design Tool Reference.

2.6.1 Using Model Variable Lists

A typical use of a model variable list is to store host user IDs and passwords for the session server to use when logging into the host. This simplifies the login process. It is often necessary to create a pool of host user IDs and passwords for your client applications to use. In this case, you would create a model variable list that would assign a host user ID and password for each client session.

Keep the following restrictions in mind as you create and configure model variable lists:

- A session pool can use more than one model variable list, but a variable cannot appear in more than one list being used by the same session pool.
- The model on which the session pool is based must contain all the variables specified in the variable list.
- A session pool's total session count cannot exceed the number of entries in the model variable lists it uses.

2.6.2 Creating and Configuring Model Variable Lists

You can use the Administrative Console to create and configure a model variable list, or define it during deployment with deployment descriptors. It is recommended that you choose one of these options and continue to use the same option for other updates; changes performed in the Administrative Console are overwritten when you use a deployment descriptor file.

1. Open the Administrative Console and log onto the management server using an Administrator profile. Open the Host Integrator perspective.
2. In the Session Server Explorer tree, click Servers, and then select the session server for which you want to create the model variable list.
3. Right-click Model Variable Lists and select Add Model Variable List. The Add Model Variable List dialog box displays.
4. Type a name for the new model variable list in the List name field, and then click OK. The model variable list displays in the Session Server Explorer tree and in the Model Variable List view. To open the view, click Open Model Variable Lists view in the Overview panel or right-click Model Variable Lists in the Session Server Explorer tree and select Open Associated Views.

2.6.3 Creating entries in your list

At this point, you have a model variable list. This list can be used by all session pools on the server. To complete the process, follow the steps below to create list entries in your model variable list:

1. In the Session Server Explorer tree, click the model variable list you just created, and then click Properties.
2. In the Model Variable List panel, click Add to add variables and variable values. In the Variable Name box, enter the name of the variable, for example, userID. The variable name you enter here must be a variable configured in the model on which the session pool that will use this model variable list is based.
3. To continue adding variables, click Create on the Add Variables dialog box. As you add variables they are entered in the Variables list on the Properties page. When you add a variable, you can specify if the value of the variable is unique or will contain hidden values. At least one variable in the list should contain unique values.
4. To hide the value for a variable, select Hide Values. These variables are encrypted. This corresponds to Encrypt value in the Design Tool. Once you've hidden and submitted a value, they remain hidden.
5. In the Entries section, click Add to enter a value for each variable, for example User1. Click Create to add multiple entries. Click Close.

2.6.4 Configuring session pools to use the list

Now that you've created a model variable list, configure one or more session pools to use it.

1. In the navigation tree, click Pools, and then click the session pool that you want to configure.
2. Right-click Properties, and then select Model Variable lists. A list of available model variable lists is displayed in the top panel.
3. Select one or more lists, and then click OK.

You can review the information regarding available session pools and model variable lists in the corresponding Pool or Model Variable Lists views.

2.6.5 Determining Variable Names in a Model Variable List

Session pools are based on models. When you create a model variable list, variable names must be valid for the model on which the session pool is based.

1. In the Session Server Explorer tree, select the session pool, right-click, and select Properties.
2. In the left pane of the Properties pane, open Model Variable Lists. You can see the model variable lists available for use with the session pool and those that are not.

The page contains a list of variables defined in the model that is associated with the selected pool, as well as the model variable lists that cannot be used by the model, including the reason why.

2.6.6 Securing Host Passwords

If you use session pools (especially with 3270 or 5250 hosts), a model variable list defines the unique host user names and passwords for the session server to use. The variable values are specified in the model deployment package and stored on the server.

Whether you create a model variable list in the Design Tool deployment options (mvl_desc.xml) or in the Administrative Console, it is the best practice to use the Hidden option for host passwords. This option provides the following benefits:

When creating your model package file, the variable values can be encrypted. In the packagemodel command, if you add the -e "passphrase" option, your phrase will generate a 3DES (Triple DES) encryption key to encrypt the hidden variable values. It is best to use a phrase of at least eight random characters or at least five space-delimited words. The same passphrase will be required to decrypt values when deploying with the activatemodel command.

On the session server, the variable values are automatically encrypted in the sesssrvr.config file using 3DES (Triple DES).

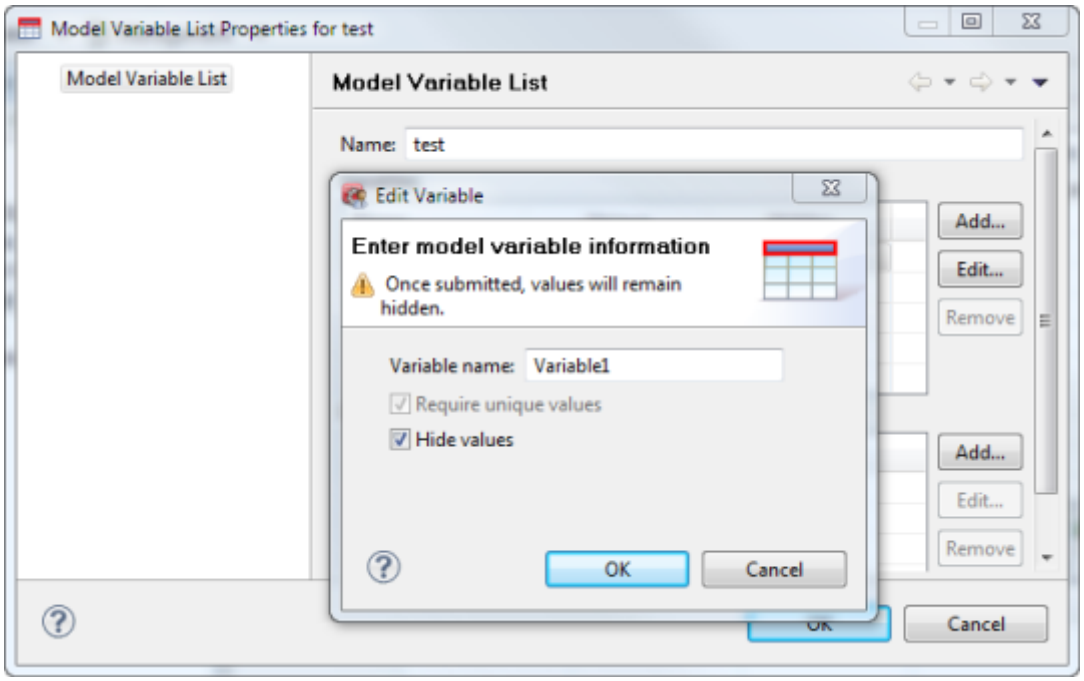
In the Administrative Console, the encrypted variable values are not visible in View or Config Mode. Requiring administrator authentication to use the model variable management API is also a very good practice. See Working Securely for information on authentication and authorization.

TO USE THE HIDE OPTION IN THE ADMINISTRATIVE CONSOLE

In the Session Server Explorer, select the server associated with the model variable list.

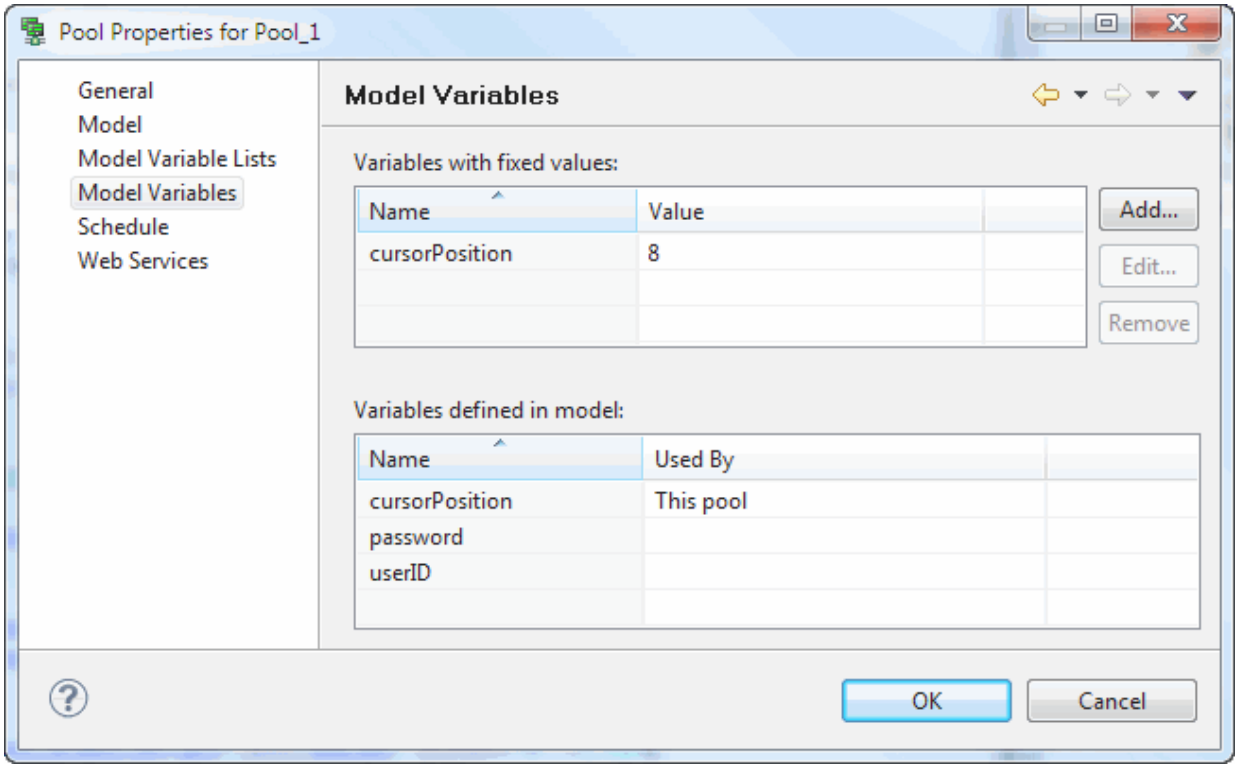
Expand the Model Variable List node and select the model variable list you are securing. From the right-click menu, choose Properties. This opens the property dialog for the model variable list.

3. For each variable you are adding, choose Hide values to encrypt the variable.

3. 

2.6.7 Using Fixed Value Model Variables

Values for fixed value model variables are associated with all sessions in the associated pool. To configure a model variable:



1. In the Session Server Explorer, if necessary, create a session pool.
2. Open the properties page for the pool. To open the properties page, right-click on the pool and choose Properties, or click on the toolbar.
3. In the left pane of the Properties page, select Model Variables.
4. Click Add to enter the name of the pool model variable you wish to create and the fixed value. The Variables Defined in Model table shows where the variables are used. You cannot interact with this table. By default, all models have the variables userID, cursorPosition, and password. The model you're working with may have additional variables; these were designated when the model was created in the Design Tool.

> **Note**
>
> The model variable value you provide here will be used for all sessions in the session pool. If you want to provide a unique value for each session, create a model variable list.

More information

Working with Session Pools

Creating Session Pools

2.7 Working with Session Server Logging

The Host Integrator logging component coordinates all logging activity for the Host Integrator session server.

Host Integrator can log server errors and can issue warnings and informational messages as it runs. Using the Administrative Console, in the Logging perspective, Log view, you can build queries to provide valuable logging data.

Logging properties, such as storage location and disk utilization, are set on the Properties page. In the Session Server Explorer, Logging perspective, click  to open the Properties page.

Log messages are shown in reverse order, that is from most recent at the top of the log to the oldest messages at the bottom.

Clearing the Log

To clear the log, click the Clear button. All the log messages currently in the log will be deleted. Note: The Clear button is not visible if security is enabled and the current user is not in the Administrator profile.

More information

- Building Queries
- Understanding SQL Dialect for the Logging System
- Setting Logging Properties

2.7.1 Setting Logging Properties

Host Integrator can log server errors and can issue warnings and informational messages as it runs. In the Logging perspective, Log view, you can build queries to provide valuable logging data.

To set logging properties

The options in this panel specify the type of logging that is performed, the location of log files, and time and space limits for log files.

Default Logging Level

The Default Logging Level item specifies which events are inserted into the log files by default. These messages are also sent to the operating system log if system logging is enabled (see below). This is a server wide setting. Client applications also have the ability to increase the logging level for their own private sessions. To record all server activity, select Log All Messages. This will include in the log all informational messages, warnings, and errors. Because this setting requires the server to track all activity, expect additional resource consumption on the server

Select a reduced logging level for improved performance on heavily loaded servers.

- **Log Storage Directory**

  This option specifies the directory in which log messages stored, which by default is `<installation directory>\VHI\etc\logs\server (Windows)` or `<installation directory>/vhi/etc/logs/server (Linux)`. Using this setting an administrator can specify a different local directory where new messages will be stored. The directory you specify must already exist. Any existing messages are transferred to the newly specified location.

- **System Logging**

  When System Logging is enabled, Host Integrator sends logging messages to both the Host Integrator log files and the operating system log, which is the Event Log on Windows systems and the syslog daemon on Linux systems. Host Integrator will also send a message to the System Log when it detects a logging system failure, regardless of this setting.

> **Note**
>
> Host Integrator does not manage the size of the operating system log. When System Logging is enabled, you must take steps to limit the size of your system log.

- **Failed Request Information Logging**

  The Failed Request Information Logging option helps you troubleshoot client application problems.

  When Failed Request Information Logging is enabled and the server encounters an error, the server will write all activity for the failed request to the log file. This information will appear immediately before the error message in the log file. Because Failed Request Information Logging requires the server to track additional activity, enabling it will consume additional resources on the server.

  Failed Request Information Logging does not have to be enabled for request failures to be recorded; enabling this setting simply appends all activity associated with the failure in addition to the failure itself. When Failed Request Information Logging is disabled, the error itself is still logged.

  If Logging Level is set to Log All Messages, all activity is written to the log file even when no errors are encountered and regardless of the Failed Request Information Logging setting.

- **Log Space Threshold Settings**

  The Log Space Threshold is the total amount of disk space in MB that can be used to store log records. The default is 100 MB and the range of values is 1 - 100000 MB. When the Delete logs when disk space exceeds threshold check box is selected, the oldest log entries will be deleted when the amount of disk space used by the log records exceeds the threshold. The oldest messages are deleted until space utilization is decreased to 80% of the configured maximum limit.

  In addition to the space required to store messages, the logging system requires administrative storage space. For proper function of the logging system, ensure that the actual free disk space in the configured logging directory is at least twice the value of the Log Space Threshold setting.

  The space and time thresholds can be enabled at the same time. In this case, the most restrictive setting is used.

- **Delete logs older than threshold**

  Enable this option to delete logs older than the threshold set in the Log Space Threshold.

- **Log Time Threshold (in days)**

  The Log Time Threshold is the expiration date for all log records. The default is 30 days, and the range of values is 1 - 100000 days. When the Delete logs older than threshold check box is selected, messages older than the specified threshold will be purged.

  The space and time thresholds can be enabled at the same time. In this case, the most restrictive setting is used.

More information

Exporting Log Files

Understanding the SQL Dialect of the Logging System

Building Queries

You can securely perform detailed queries against session servers using the Host Integrator logging component.

You can run these queries against any installed session server.

Queries are specified through a flexible SQL SELECT expression.

The messages returned from a query are displayed in the Logs view where you can rearrange and sort columns.

The Log view toolbar

This button	Does this...
	Runs the query
	Cancels a running query. If you want to interrupt a query while it is running, click this toolbar button.
	Brings up the Build Query dialog box where you can create a query.

This button	Does this...
	Clears the messages from the viewer and from the server.

To create a query

1. From the Host Integrator drop down list, open the Logging perspective.
2. From the list of session servers, select the ones you want to run the query against. You can run a query against multiple session servers.
3. The drop down list displays the default query string and the most recently used queries. You can run a query using this filter or build your own query. The default query, select * from messages, displays all messages.
3. You can type a query directly into the text box, however, you must be careful to use the correct syntax.
4. If you decide to build your own query, click Build Query on the toolbar.
4. The Build Query dialog box displays.
5. Set the parameters for your query.
5. As you build the query it displays in the Query box.
6. Check Execute Query to activate the query automatically when you close the dialog box.

To set query parameters

You set query parameters using the Build Query dialog box. To use multiple values for Message ID, Session ID, Request ID, and so forth, separate them using commas.

- **Event types**

  You can filter the log to display any combination of error messages, warnings, and informational messages. Select the check box for each event type you want to be displayed.

- **Specifying View From and View To Options**

  The From (msgtime) options set the starting selection for the records that are displayed. You can decide to view records from the first record, or by selecting a date and time. If you choose First Record, the Start Date and Start Time options are ignored and the displayed list begins with the oldest available record.

  If you select Start Date/Time, then you can set the date and time to see the records that occurred after the date and time specified.

  The To (msgtime) options specify the ending date of the records that are displayed. You can decide to set the ending date when the last record displays, or you can set a specific date and time. When you select the Last Record option, the Stop Date and Stop Time options are ignored and the displayed list ends with the most recent available record.

  When the First Record and Last Record options are selected, all log records are displayed, up to a maximum of the first 1000 records. To view records prior the 1000 records that are displayed, specify a stop date and time that is before the 1000th record.

- **Message ID**

  The Message ID is the value associated with this particular message.

- **Session ID**

  The Session ID is the number assigned at run time to the session. The first byte in the number represents the processor; servers that contain multiple processors may have large values for the Session ID.

- **Request ID**

  The Request ID is assigned at run time for each unique request.

- **Client IP Address**

  The Client IP Address is the IP address of the user who connects to the Host Integrator Server.

- **User Name**

  The User Name is name of the person who connects to the Host Integrator Server.

- **Model or Session Pool Name**

  When connecting to the Host Integrator Server, a session will use either a session pool or a specific model, but not both.

Viewing Query Results

Logging results display in the Log view of the Administrative Console and are selectable using the right-click context menu. You can select multiple rows from the query table and save them to a clipboard in a comma-separated format.

Log messages are shown in reverse order, that is from most recent at the top of the log to the oldest messages at the bottom.

The results of the query are scrollable. The statement describing the query will determine the order and number of columns displayed.

More information

- Setting Log Properties
- Exporting Log Files
- Understanding the SQL Dialect of the Logging System

2.7.2 Exporting Log Files

The logexport command line utility provides you with the ability to securely perform detailed queries against the Host Integrator logging component. It is capable of performing bulks extracts of messages from the logging component suitable for parsing or importing into third-party applications.

- The utility can be run from any host on the network. (Windows or Linux)
- Access control is integrated with the Host Integrator security architecture.
- Queries are specified through a flexible SQL SELECT expression.
- The output format is configurable and parseable by other applications.
- The utility can perform bulk extracts of messages form the Host Integrator logging system.

Operation

The logexport utility can be found in the bin directory of the Host Integrator installation. You can run it from this location, or you can add this directory to your PATH for easy access. The utility has a variety of command line switch options.

Help on available options can be obtained with the use of the command line switch `-help`.

```
logexport -help

LogExport -query sql [ -delim delim_char ] [ -escape esc_char ]
                  OR
          -purge msgserial

          -server servername
          -ds mgmtservername
          -user username
          -password userpass
          -profile ( Administrator | Developer )
          [ -config filename ]
```

```
The utility performs two primary functions:
```

Query a message store for messages. (`-query switch`)

Purge old messages from a message store. (`-purge switch`)>

One of these options must be specified, but they are mutually exclusive. The -server switch is required. This option specifies which log service to contact.

Regardless whether security is enabled on the Host Integrator installation in question, logs are protected from access by unauthorized users. Access to logs always requires a user to authenticate with the management server. The options `-ds` , `-user` , `-password` , and `-profile` are required. Both administrators and developers can perform queries against the logs, but only administrators can execute message purges.

Querying Messages

The `-query` option takes a SQL select statement which specifies which messages you want to see. For example:

```
logexport -server s1 -query "select msgtime, msgtext from messages"
```

This invocation will contact the logging service (Log Manager Service) running on host "s1" and output the message time and message text of all messages currently in the Host Integrator server logs. The results will be directed to standard out. Any errors that occur will be directed to standard error. Columns of output will be separated with the "|" character.

Along with the `-query` option, two optional parameters can be specified, `-delim` and `-escape` . Each of these options takes a single character. Use the -delim switch to specify the character used to separate columns in the output. It is the "|" character by default. Use the `-escape` option to specify the character used to escape occurrences of the column delimiter that occur within any column of message data. It is the "\" character by default.

For details on the SQL supported by the Host Integrator logging system, see Understanding the SQL Dialect of the Host Integrator Logging System.

Within the SELECT statement, specify the columns of the message entry desired in the output, and the order they will appear. To specify all columns in the default order, use "*" as the column identifier.

Each message entry has the following columns available:

Name	Type	Description
msgserial	INTEGER	Message primary key
msgtime	TIMESTAMP	Date/Time message
msgid	INTEGER	Numeric message identifier

Name	Type	Description
sessionid	INTEGER	Session identifier
requestid	INTEGER	User request identifier
cltaddr	VARCHAR	User's network name
user	VARCHAR	User's name
model	VARCHAR	Model or pool name
msgtext	VARCHAR	Text of the message

Name	Type	Description
severity	VARCHAR	Message severity

The SQL SELECT statement optionally can contain a WHERE clause that allows the user to specify complex matching criteria on the message entries they desire to see.

Purging Messages

If this utility is used to perform a bulk extract of messages from the Host Integrator logging system, you will need the ability to purge messages from the system after they have been safely loaded into another database or application. All messages within a message store are tagged with a unique serial number that can be obtained by specifying the msgserial column in a query. This column is the message's primary key. The -purge option takes a message serial number, and deletes all messages in the specified message store, up to and including the serial number specified. For example:

```
logexport -server s1 -purge 1234
```

This example deletes all messages with a msgserial number less than or equal to 1234 on machine "s1".

Advanced Features

Due to the relatively large number of available switches on the logexport utility, you may want to specify run-time arguments from a configuration file. Specify the file containing run-time options on the command line. To employ this feature, create a file containing the desired options, and specify the path to the file as the argument to the -config switch.

```
logexport -config sample.config
```

Any switch that can be specified at the command line, with the exception of the -config switch, can be placed in the config file. The format of the file is shown below:

```
#
# Comments look like this.
#
# Line tags are the same as switch names.  Any number required can
# be specified in the file.
#
# server
# query
# purge
# delim
# escape
# ds
# user
# password
# profile
#
# Here are some real entries.
#
server=s1
query=select msgtext from messages
```

A config file can be specified in combination with other command line switches. If a setting is specified more than once, the value of its final specification is used during run-time. This allows you to create a default configuration file, but override particular values for a given run. For example:

```
logexport -config myconfig -server somepc
```

In the above example, logexport will contact server "somepc" regardless of whether "server" is specified in the file "myconfig".

More information

- Building Queries
- Understanding the SQL Dialect of the Host Integrator Logging System
- Setting Logging Properties

2.7.3 Understanding the SQL Dialect of the Logging System

The use of SQL provides a flexible and expressive way to locate messages of interest within the Host Integrator logging system. This topic defines the dialect of SQL supported by the Host Integrator logging system.

Functional Specification

Host Integrator supports the SQL SELECT statement and its associated WHERE clause. Nested conditional expressions in the WHERE clause are supported, using the following relational and logical operators:

```
AND, OR, NOT, =, <>, >=, <=, LIKE
```

As an example take the following SQL statement:

```
select msgtime, severity, msgtext from messages where sessionid = 45 and msgtime < timestamp '2001-09-10 10:00:00'
```

This statement returns a result set of three columns, the message time, its severity, and the text of the message itself, in that order, for all messages whose session identifier was 45 that occurred prior to 10 am, September 10, 2001. Many more queries are possible.

The logging system contains a single table named “messages”. This table contains the following columns:

Column Name	Type	Description
msgserial	INTEGER	Message primary key
msgtime	TIMESTAMP	Date/Time of message

Column Name	Type	Description
msgid	INTEGER	Numeric message identifier
sessionid	INTEGER	Session identifier
requestid	INTEGER	User request identifier
cltaddr	VARCHAR	User's network name
user	VARCHAR	User's name
model	VARCHAR	Model or pool name
msgtext	VARCHAR	Text of the message
severity	VARCHAR	Message severity

Ordinarily, you will be comparing column names to literal values in our WHERE clauses, so conditional expression phases will look something like the following:

Expression Description

Expression	Description
colname <&234	Compares a column to a numeric literal
colname = 'Some Text'	Compares a column to a character literal
colname > TIMESTAMP '2001-08-12 22:12:45'	Compares a column to a TIMESTAMP literal

It is important to compare similar types to avoid a type mismatch error. Also note that if a character literal contains a single quote, as in 'Let's', it is escaped by a preceding single quote.

The LIKE operator performs simple pattern matching on character columns in accordance with the SQL standard. The pattern is specified as a character literal. The characters *"" and "%" have special meaning. A ""* matches any single character while a "%" matches zero to any number of characters. If you want to match a "_" or a "%" literally, you must specify an escape character using escape and use it in the expression. For example:

Expression	Result
msgtext LIKE 'entity'	Matches "entity" exactly
msgtext LIKE 'entity%'	Matches entries that start with "entity"
msgtext LIKE '%entity%'	Matches entries that contain "entity"

Expression	Result
msgtext LIKE '___ entity%	Matches entries that start with "(any 3 letters) entity"
msgtext LIKE '%entity%error%'	Matches entries that contain "entity" before "error"
msgtext LIKE '%&%%' ESCAPE '&'	Matches entries that contain "%"

Additional Example Statements

Below are several examples of supported statements. For a formal definition of what is supported, see the section: BNF Specification.

Statement	Result
select * from messages where msgtime > timestamp '2001-23-08 10:00:00'	Returns all columns, in the default order, of any messages that occurred after 10:00 am, August 23, 2001.
select msgtime, severity, msgtext from messages where sessionid = 23 and user = 'ralf'	Returns columns msgtime, severity, and msgtext, in that order, of any messages that originated from session 23 under the control of "ralf".
select msgtime, severity, msgtext from messages where sessionid = 12 and msgtext like '%session%'	Returns columns msgtime, severity, and msgtext, in that order, of any messages that originated from session 12 and whose msgtext column contains the string "session" anywhere within it.

Statement	Result
select cltaddr, msgtext from messages where sessionid = 45 and (cltaddr like ‘150.123%’ or cltaddr = ‘grumpy’)	Returns columns cltaddr and msgtext in that order, of any messages that originated from session 45 and whose cltaddr column starts with “150.123” or whose cltaddr is “grumpy”.

BNF Specification

This section provides a detailed description of the supported grammar in BNF. (it all starts with 'select-exp').

```
select-exp
    ::=
   SELECT select-item-commalist FROM table-ref
          [ WHERE cond-exp ]

select-item-commalist
    ::=   select-item [ , select-item-commalist ]

select-item
    ::=   column-ref
        | *

table-ref
    ::=   messages

cond-exp
    ::=   cond-term
        | cond-exp OR cond-term

cond-term
    ::=   cond-factor
        | cond-term AND cond-factor

cond-factor
    ::=  [ NOT ] cond-primary

cond-primary
    ::=   simple-cond
        | ( cond-exp )

simple-cond
    ::=  comparison-cond
        | like-cond

comparison-cond
    ::=   scalar-exp comparison-oper scalar-exp

like-cond
    ::=   char-string-exp LIKE char-string-exp [ ESCAPE char-string-exp ]

scalar-exp
    ::=   numeric-exp
        | char-string-exp
        | datetime-exp

comparison-operator
    ::=   =
        | <
        | >=
        | >
        | <=
        | <>

numeric-exp
    ::=   numeric-primary

numeric-primary
    ::=   column-ref
        | numeric-literal

char-string-exp
    ::=   character-string-primary

character-string-primary
    ::=   column-ref
        | character-literal

datetime-exp
    ::= datetime-primary

datetime-primary
    ::=   column-ref
        | timestamp-literal

timestamp-literal
    ::=  TIMESTAMP character-literal
```

More information

Building Queries

Setting Logging Properties

2.8 Working with Host Emulator

The Host Emulator runs 3270, 5250, and VT recordings without having a live connection to a mainframe. Using Host Emulator is an easy way to test your client or Web application. Host Emulator simulates the host connection you used to create your recording in the Design Tool. Host Emulator does not actually connect to the host.

The recording contains all data communication between the Design Tool and the host, including screens, navigational commands, and errors messages. This allows your application to access the data as if it was coming from the actual host. You can then load this model into the Host Emulator, connect to it using the Design Tool, or another third-party client, and create the actual models you will deploy in your applications. The recordings you create in the Design Tool and play back in the Host Emulator are static; they contain only the screens and data captured by the recording files. Although you can play back a recording in the Host Emulator to test your client application's ability to navigate the host, you cannot test your client application's ability to update data on the host.

When you replay a recording in the Host Emulator, the Host Emulator can only display the entities the model contains. For example, if you have only one AcctProfile entity, you'll only be able to see the one set of data that entity contains. Because a recording contains multiple entities for different sets of data, it allows you to display multiple AcctProfile screens, each with different data.

Host Emulator recordings have these benefits:

- You can test your applications more thoroughly. Including customer specific entities in your recording that allow you to test your application's ability to access specific data.
- After you connect to the host and create the recording, you can develop and test multiple recordings and applications without being connected to the host.
- You can build error messages into your model. By creating entities for specific error messages, you can test the way your client application handles host errors.

After you create your recording in the Design Tool, copy the .trc_GROOMED file (located in `My Documents\Attachmate\Verastream\HostIntegrator\recordings to your Host Emulator configuration (Program Files\MicroFocus\Verastream\HostIntegrator\hostemulator\recordings` so that the Design Tool can connect to it and allow you to create models from it. Recordings can also be copied to a Linux VHI server's microfocus/verastream/hostintegrator/recordings directory and used by the Administrative Console to add the files to the Host Emulator Recordings.

Creating Recordings

Recordings represent the host application and should simulate that application as closely as possible. Follow these guidelines when creating a recording:

- Define each host screen as an entity.
- Use the entire screen as the pattern for each screen. The Host Emulator does not use the pattern information so there's no performance hit, but this does ensure that each host screen is unique.
- Navigate all possible paths between entities.
- To create spaces in a field use the space bar, never use the cursor keys. For example, "Last Name" should be typed with a space between the t and the N, rather than using cursor keys to leave a blank space.
- Do not use login or logout scripts. The first entity defined in the recording should be the first screen displayed when you connect to the host.
- The recording is a text file. It may be occasionally necessary to edit the recording to modify the behavior to act more like the actual host. Contact Technical Support for more information on this process.

More information

Adding Host Emulator Recordings

Using Host Emulator

2.8.1 Using Host Emulator

You can use the Host Emulator to run and test 3270, 5250, and VT recordings, created with the Design Tool without having a live connection to a host. To simulate this live connection, the Host Emulator opens the recording, such as CCSDemo.trc_GROOMED, of the host application model while the corresponding "normal" model, or CCSDemo,is loaded in the Design Tool or Host Integrator Server. Example recordings are installed in the `<install_directory>\MicroFocus\Verastream\HostIntegrator\hostemulator\recordings` folder.

The Host Emulator Server (localhost) is started by default.

> **Note**
>
> Before you can add a recording to Host Emulator, you must copy the recording file (for example, `ccsdemotrace_65342_00001.trc_GROOMED`), created in the Design Tool, to the `<install_directory>\MicroFocus\Verastream\HostIntegrator\hostemulator\recordings` directory. On Linux platforms, copy the file to `/opt/microfocus/Verastream/HostIntegrator/recordings`.

How to Access Recordings

Recordings are created and automatically groomed in the Design Tool, saved, and after you copy them to the Host Emulator server, they are available to you for playback.

From the Administrative Console, open the Host Emulator perspective (Host Integrator drop down list, select Host Emulator). On the Host Emulator Server Explorer you can add a Host Emulator server or use the default (localhost) server. Using the information on the Host Emulator Recordings view, verify that the port number for the recording in the server configuration matches the port number specified for that recording in the Host Emulator, and modify the host profile for the recording to point to the machine where the Host Emulator is running. By default, details about the recordings provided with this installation are listed.

To simulate a live connection to a host, open the recording in the Design Tool and click Connect to localhost via Telnet on the Connection menu.

2.8.2 Adding Host Emulator Recordings

Before you can run a recording on the Host Emulator, you must add it to the Host Emulator's configuration. When you add a recording, you configure the Host Emulator to connect to the recording so you can run it.

Before you add a recording

Your recording is created and saved in the Design Tool.

On the Connection menu, point to Host Emulator Recording, and select Start. You now can record screens and how to navigate between them as you create your model.

Select the name and the location of the recording.

3. Click Stop on the toolbar or select Stop from the Connection menu | Host Emulator Recording.
3. If you attempt to create a new model or open an existing one, after agreeing to continue the action, the recording is also stopped.

After you create your recording in the Design Tool, to enable the Host Emulator to connect to the recording, copy the newly created `.trc_GROOMED file` (default location is `My Documents\Attachmate\Verastream\HostIntegrator\recordings` to your Host Emulator configuration (`Program Files\MicroFocus\Verastream\HostIntegrator\hostemulator\recordings`. On a Linux server, the default location is `/opt/microfocus/verastream/hostintegrator/recordings`. This makes the file visible in the Administrative Console and available to playback.

Adding a recording to the Host Emulator

1. In the Administrative Console, open the Host Emulator Perspective, which is available from the Host Integrator drop down list.
2. On the Host Emulator Servers panel make sure you have an Host Emulator Server listed. By default, there is an Host Emulator server associated with localhost available.
3. With the desired Host Emulator Server selected, on the Host Emulator Recordings panel, click the Add a New Recording icon add recording in the top right corner.

Provide the details needed in the Add New Recording dialog box for the recording you are adding, and then click OK to add the recording to the currently selected Host Emulator Recording list.

More information

Configuring Host Emulator Recording Properties

Using Host Emulator

2.8.3 Using the Host Emulator Recordings List

To open the Host Emulator Recordings list, from the Administrative Console toolbar, open the Host Integrator perspective drop down list and choose Host Emulator. From the View menu, choose Host Emulator Recordings.

From the Host Emulator Recordings list you can playback, stop, edit, and remove Host Emulator recordings.

This column	Describes this...
Name	The name of each recording
Port	The TCP port the recording uses to communicate with client applications and the Host Integrator Server.
Status	A recording can be either in playback mode or stopped. You can only set recording properties when a recording is stopped. In playback mode, the Design Tool or Host Integrator server can connect to the Host Emulator server, assuming that the correct ports have been configured.

This column	Describes this...
Sessions	The number of sessions currently connected to the recording.

More information

Adding Host Emulator Recordings

Configuring Host Emulator Recording Properties

2.8.4 Configuring Host Emulator Recording Properties

You can use the Host Emulator recording properties page to set and view options for your recordings within the Administrative Console.

To open the properties page, select a recording from the Host Emulator Recordings list, right-click, and choose Properties. The settings are specific to the model you selected.

You can only set model properties when the model is stopped. To change the status of a model, right-click and choose either Playback or Stop, or alternatively click the appropriate Host Emulator Recordings list toolbar buttons.

This option	Does this...
Recording name	The name of the selected recording.
Port	The default TCP port. If you plan to have more than one recording running at the same time, they must use different TCP ports.
Terminal type	Choose the terminal type that the recording is using; 3270, 5250, or VT.

This option	Does this...
Open recording when server starts	Select this option to have the recording be available in Playback mode when the server starts.

More information

- Adding an Host Emulator Recording
- Stopping and Playing Back Host Emulator Recordings
- Using the Host Emulator Recordings List

2.8.5 Stopping and Playing Back Host Emulator Recordings

Host Emulator recordings listen on their specified TCP ports for connection requests. You can have recordings playback automatically when the server starts by selecting that option in the Host Emulator Recording properties page. The status of the recording is listed in the Host Emulator Recordings view in the Status column.

You can only set recording properties when the recording is stopped. To change the status of a recording, right-click and choose either Stop or Playback, or alternatively click the appropriate Host Emulator Recording list toolbar buttons. If a client application attempts to connect to a recording while it is not listening for connection requests, it will receive a "Connection refused" error message.

To playback an Host Emulator recording

Select the recording from the Host Emulator Recordings list and click playback on the toolbar. Verify the recording is in Playback mode by checking its status.

To stop an Host Emulator recording

Click  to stop the recording, which causes the recording to stop listening for connection requests. All pending connections should be closed first.

> **Note**
>
> Do not have more than one recording listening on the same TCP port at the same time for connection requests. If you have configured more than one recording to use the same TCP port, make sure only one of them is set to Playback at a time. The best way to ensure this is to not configure these recordings to start automatically.

More information

2.9 Reference

These help topics give you more information about Host Integrator:

Troubleshooting

Changing Host Integrator Port TCP Numbers

Host Integrator Port TCP Numbers

2.9.1 Troubleshooting

This section of the Host Integrator Server Reference provides tips for troubleshooting problems you may encounter.

- Invalid model names

  Model name and folder name must be the same: As of Version 5.5, the `.model` file must be in a folder with the same name. If you try to open a model with a folder name that is different, you'll see this message on a Windows system: `"<model>` is not a valid model name. Please check the name and model path for accuracy."

  Case sensitivity: When you save a model in the Design Tool, it is stored to a folder with the same name and case as the model. After deploying the model on a Linux system, you may see a message that the model name is invalid. Make sure the case of the folder name and the model name match. This is not an issue on Windows systems since the Windows file system is not case-sensitive.

- Allocated session timed out waiting for client connection

  This is caused when the IP address of a Host Integrator Server changes after it has been started. The most likely cause is that the server briefly lost contact with the network, and when the connection was reestablished, the server was assigned a new IP address, different from the one it had upon startup. This can also happen if a server is reassigned a new IP address by DHCP dynamically after starting. To solve the problem, stop and restart the affected servers. Be sure that any machines running Host Integrator Servers retain the same IP address from the time they are started until they are stopped.

2.9.2 Changing Host Integrator Port TCP Numbers

If you need to reassign the port numbers used by Host Integrator components, do the following:

Stop all Host Integrator services.

Create a file called vhibaseport.properties and place it in the `vhi/etc` directory.

Add `vhibaseport=n` to the file, where "n" is a valid TCP port number.

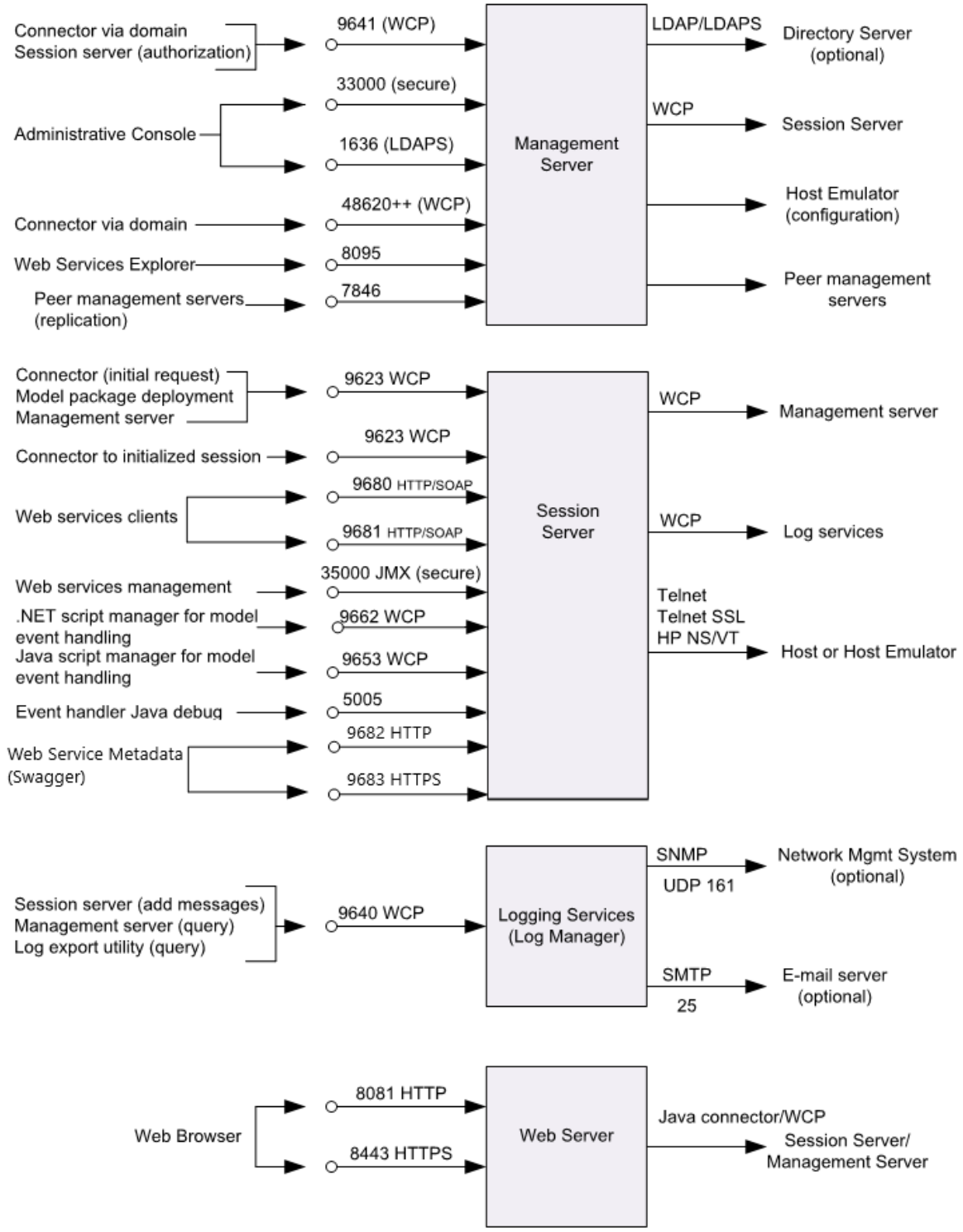
Restart all Host Integrator services.

After you reassign the VHI base port, the Host Integrator components are assigned these TCP ports:

Component	TCP Port Assignment
vhibaseport	n
Session server	n-> n+16
Logging utility	n+17
Management server	n+18

Component	TCP Port Assignment
Script manager	n+30

Existing Host Integrator TCP Port Numbers



See Technical Note 10105 for more detailed information on VHI ports.

Configuring Port Numbers

You can change port numbers if needed.

Changing the Event Handler Java Debug Port

By default, the Design Tool or the Session server starts searching at port 5005 for an available remote debugging port. You can change the starting point for locating an available port. You must restart the server for the change to take effect.

To change the Java debug port for event handling in the Design Tool, use the Event Handler Settings Debugging tab.

To change the Java debug port for event handling for a server, in the Session Server Explorer of the Administrative Console, open the session server properties, and choose Events.

Configuring the Management Server secure RMI port

This port can be configured to enable Administrative Console to connect through a firewall.

Edit the `MicroFocus/Verastream/ManagementServer/conf/container.properties` file.

Set the desired port number in the rmi.export.port.ssl line (0 is the default for a random ephemeral port).

After saving the changed file, restart the management server.

> **Note**
>
> Some components may use additional ephemeral ports. When configuring Windows Firewall exceptions, in addition to specifying port numbers, it is recommended you add program `C:\Program Files\MicroFocus\Verastream\java\jdk1.6.0_16\bin\java.exe`.

Configuring the Management Server non-secure RMI port

This port is disabled by default. To enable non-SSL JMX for third-party JMX tools, follow the steps above, except set rmi.port to a desired port number such as 33001 (default 0 turns it off).

More information

Technical Note 10105: Ports Used by Verastream Host Integrator 7.x

Host Integrator Port TCP Numbers

2.9.3 Host Integrator Port TCP Numbers

Host Integrator components use the following TCP port assignments.

Component	Listens on destination port	From and purpose
Management server	9641 (WCP)	Client connector, connecting via load distribution domain Session server for client authentication and authorization
Management server	33000 (secure JMX)	Administrative Console (JConsole API for configuration and monitoring)
Management server	33001 (JMX)	JConsole API
Management	server	7846
Management server	8095	Web Services Explorer, used for testing Web services deployed from Design Tool
Management server	1636 (LDAPS)	Administrative Console (authorization profile configuration, aggregates user data from all configured directory servers)
Management server	48620 and higher (WCP)	From client connector to domain server (one port used per load distribution domain)
Management server	32000	Wrapper service for JVM
Session server	9623 (WCP)	Client connector (requesting session)Deployment tools (activatemodel,deactivatemodel, Design Tool)Management server (configuration, monitoring, domain server requesting session)
Session server	Ephemeral (WCP)	From client connector, to requested initialized session
Session server	9680 (HTTP/ SOAP)	Web services clients
Session server	9681 (HTTPS/ SOAP)	Web services clients (SSL)
Session server	9682 (HTTP)	Web services metadata
Session server	9683 (HTTPS)	Web services metadata

Component	Listens on destination port	From and purpose
Session server	35000 JMX (secure)	Web services management
Session server	9653 (WCP)	Java script manager for model event handler scripting
Session server	9662 (WCP)	.NET script manager for model event handler scripting Session server
Logging service	9640	Session server (adding messages)Management server (querying messages)Log Export utility (querying messages)
Host Emulator	9670-9671, 1096-1099	Default master models, for demo connections from Session server
Host Emulator	36000 (secure JMX)	Management server (for configuration)
Host Emulator	36001 (JMX)	JConsole API
Design Tool	5006, or next available	Event handler Java debug port
Design Tool	9654 through 9661	Script manager for Java event handlers (one port per Design Tool instance)
Design Tool	9663 through 9669	Script manager for .NET event handlers (one port per Design Tool instance)
VHI Web Server	8081 8443 (SSL)	Java Web application projects generated in Web Builder
Hosts	23 (Telnet, default) or 992 (Telnet SSL, default) or 1570 (HP NS/VT, default)	Session server
Network monitoring system (optional)	161 UDP (SNMP)	Logging, notifications

Component	Listens on destination port	From and purpose
E-mail server (optional)	25 (SMTP, default)	Logging, notifications

Component	Listens on destination port	From and purpose
Directory server (optional)	636 (LDAPS, default), 389 (LDAP, default)	Management server (authentication requests for Administrative Console, deployment tools, and client connector)

More information

Changing Host Integrator Port TCP Numbers

2.9.4 Host Integrator Perspective Symbols and Icons

Both the Management and Host Integrator Perspectives have symbols and icons that are used to provide a visual indicator of what components and properties are available, currently in use, and the state they are in. See the Management Perspective Symbols and Icons topic under General Management Services in the online Help for icons specific to that perspective.

More information

Introduction to the Host Integrator

How to Use Host Integrator

3. General Management Services

3.1 Setting Connection Preferences

To set connection preferences for the Administrative Console, from the Console menu, select Preferences, and then open Connections.

Auto Login: Select Auto Login to have the Administrative Console re-establish on start up the connection to the management server you were previously connected to when the console shut down.

Clear list of management servers: Click Clear Now to erase the list of management servers that had been previously connected to.

Clear list of cached user names and passwords: Click Clear Now to erase the list of cached user names and passwords.

Connection port: This is the default secure port that the management server is running on. If you want to change the port, you must update this setting with the correct port number.

- **Connection heartbeat**: In seconds. The heartbeat verifies that the management server was active, at least 30 seconds ago, and the connection is reliable. You can raise the value to minimize network traffic, or lower the value for a quicker response. This value must be a positive number and cannot be set to 0. When the management server goes offline, a notification is sent informing you that the management server is offline.

  You can use a heartbeat to keep the connection alive. This not only prevents the connection from timing out, but prevents the necessity for a new connection before communication can continue.

3.2 Understanding security

Management servers communicate with each other and with the Administrative Console using Secure Sockets Layer (SSL). SSL is a protocol that provides security for communication over networks. The Administrative Console uses TLS (Transport Layer Security) v1.2, which is the successor of SSL.

There is no configuration necessary to take full advantage of secure communication channels.

More information

Adding a Management Server

Configuring Management Servers

3.3 General Management Perspective Symbols and Icons

Both the Management and Host Integrator Perspectives have symbols and icons that are used to provide a visual indicator of what components and properties are available, currently in use, and the state they are in. See the Host Integrator Perspective Symbols and Icons topic under Host Integrator Management | Reference in the online Help for icons specific to that perspective.

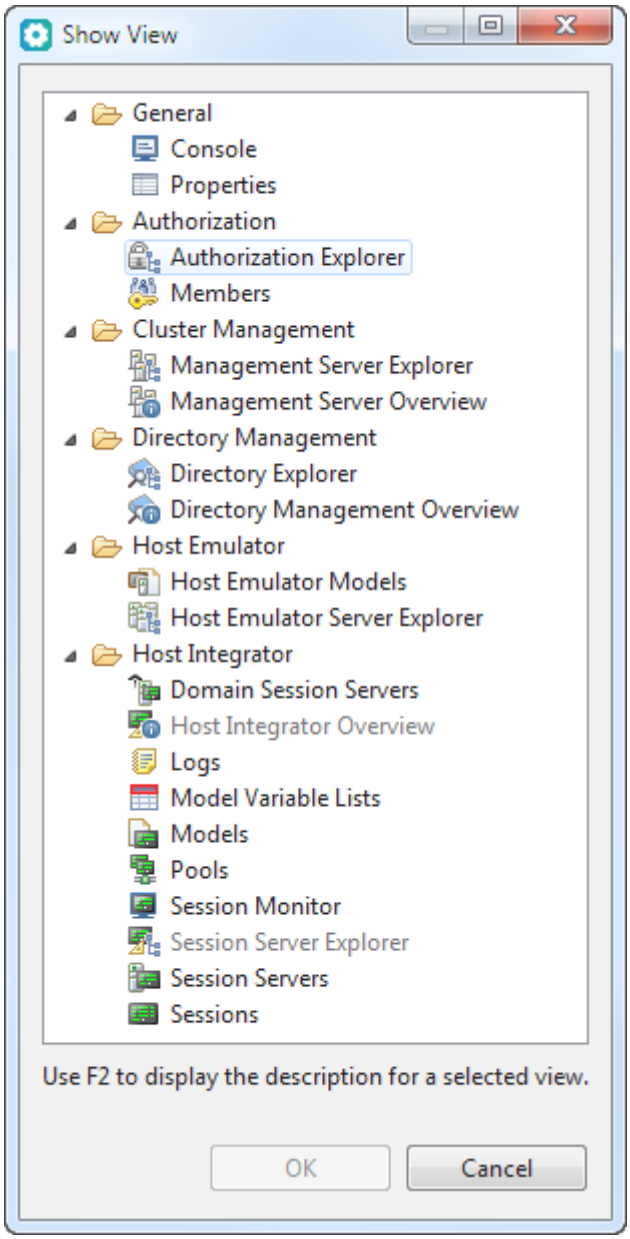
3.3.1 Administrative Console Management Perspective

Icon	Description
	Add a directory, member to authorization group, or management server
	Connect to management server
	Indicates that the management server is offline
	Indicates that the management server is online
	Restart management server
	Stop management server

Icon	Description
	Delete

3.3.2 Other Views

To see a list of views available in the Administrative Console, from the View menu, select Other Views. This dialog box provides a list of all the views that you can interact with, as well as their corresponding icons and a brief description (click F2) of its purpose.



3.4 Understanding Management Servers

3.4.1 About Management Server

The management server provides support for the following features:

- Administrative Console
- Session server load distribution domains
- Authentication and authorization security (including LDAP directory services)
- Web Services Explorer
- Session pool scheduling

You can add more than one management server to your installation, creating a management server cluster, which provides replication and failover support. You can add a management server to an existing cluster during installation or, using the Administrative Console, add it at a later time. Data is automatically replicated between the management server peers in a cluster. Each management server is a member of only one cluster. See Configuring Management Servers for information on configuring failover.

Management servers also:

- external directories that support LDAP as a source for authentication principles (users and groups).
- Provide authorization profiles, which can be used by other Micro Focus products, and to which you can add users and groups from external directories.
- Support secure communication via SSL.

Management Server Explorer

The Management Server Explorer provides a tree view of the management servers that are currently connected. Each management server has an associated overview that contains system information, including a summary, memory information for the process, and operating system and JavaVM data.

When the management server is initially installed it uses a default user name and password. You can change this password in the Management Server Explorer view, right-click on the Management Server, and choose **Change Admin Password**.

Viewing Management Server Logs

Logs are available for your management servers.

TO CONFIGURE AND VIEW MANAGEMENT SERVER LOGS

The management server uses Apache Log4j to provide logging services. Each service has server-specific logs available in their respective META-INF directory. For example, `Micro Focus\Verastream\ManagementServer\services\authorization\META-INF\log4j-authorization.xml`.

For information on configuring Log4j, see Log4j XML Configuration Primer.

Open `Verastream\ManagementServer\conf\log4j.xml`.

To view the management server logs, open `Verastream\ManagementServer\logs`. There are directory, server, and console logs available, depending on your configuration in the log4j.xml file.

USING THE CONSOLE VIEW

You can use the Console view to see a running collection of data associated with the Administrative Console functions. The Console view provides advanced debug and low-level diagnostic information.

The Console view displays a running collection of information regarding interactions with the Administrative Console. To open the Console view, from the **View** menu, choose **Other views**, and then, under **General**, choose **Console**.

3.4.2 Adding a Management Server

A management server is installed when you install the Administrative Console. Before you can add additional management servers, directories, or configure authentication, you must connect to this management server using the password you supplied during installation.

To connect to a management server

On the Administrative Console toolbar, click **Connect Management Server**  to connect to the management server that was installed during setup.

2. Type the user name and password for the management server. The password is the same password you entered during installation and the initial user name for the administrator account is 'admin'. You can change this password in the Management Server Explorer view, right-click on the **Management Server**, and choose **Change Admin Password**.
2. The administrator, after connecting to the management server, using authorization, can provide additional user accounts. After being added to a profile, users will login using their own credentials.

You can add additional management servers to this initial management server cluster.

Determining the status of a management server

In the Management Server Explorer you can observe the online or offline status of a particular management server.

 Denotes online status

 Denotes offline status

More information

Stopping and Starting Management Servers

3.4.3 Stopping and Starting Management Servers

Starting and stopping management servers is uncomplicated and the procedure varies depending on whether you are running on a Windows or Linux system.

For this operating system	Do this...
Windows	Click Administrative Tools > Services > Verastream Management Server in Control Panel. Select an action; Start, Stop, or Restart.

For this operating system	Do this...
Linux	Using a command prompt, go to the `ManagementServer/bin` directory in the location you installed the product. `./server start` — Starts the management server `./server stop` — Stops the management server `./server console` — Starts the management server in console mode `./server status` — Displays if the management server is running or not

To run the management server on a Windows platform, in console mode, stop the installed service and run the `Management Server/bin/server.bat` script.

For instructions on running the management server as a system daemon, see Configuring the Management Server to Run as a System Daemon.

Restarting Management Servers

You can restart and stop management servers using the Administrative Console Management Server Explorer toolbar buttons.

- **Restart**: Click  to restart the management server. Restarting the management server first stops and then restarts the server, rather like rebooting your computer.
- **Shut Down**: Click  to stop the management server. You cannot start a management server once it has been shut down from the Administrative Console, but can use the commands described above.

More information

Configuring the Management Server to Run as a System Daemon

Adding a Management Server

Working with Management Clusters

3.4.4 Configuring the Management Server to Run as a System Daemon

To have the management server start automatically when your system boots up

Create a file called `mgmtserver` containing the following and entering your installation directory:

```
INSTALL_DIR=<enter installation directory>
BIN_DIR=$INSTALL_DIR/managementserver/bin
case "$1" in
start)
echo "Starting Verastream Management Server"
$BIN_DIR/server start

RETVAL=0
;;
stop)
echo "Stopping Verastream Management Server"
$BIN_DIR/server stop

RETVAL=0
;;
status) echo "Current Verastream Management Server status"
$BIN_DIR/server status

RETVAL=0
;;
restart) echo "Restart Verastream Management Server"
echo "-- stopping management server --"
$BIN_DIR/server stop
echo "-- starting management server --"
$BIN_DIR/server start

RETVAL=0
;;
*)
echo "Usage: $0 {start|stop|status|restart}"
RETVAL=1
;;
esac
exit $RETVAL</code>
```

Then, complete the following steps

Copy the file to the `/etc/init.d` directory

Set the file permission. Run `chmod` using the value 755. For example, `chmod 755 mgmtserver`

Run `chkconfig` to add the initialization script. For example, `chkconfig --add mgmtserver`

3.4.5 Setting Management Server Properties

To view the properties of a selected management server, right-click the server on the Management Server Explorer and choose Properties.

There are three properties associated with a management server; Server name, Address, and the Replication port. You can edit the name of the management server. The server address and replication port cannot be changed by means of the property panel. These properties must be modified carefully to avoid complications to your clustered environment.

If this	Then this...
A management server is not part of a clustered environment	The properties can be changed, but you must restart the management server for the new values to take effect.
A management server is part of a clustered environment	The properties can be changed, but you first must remove the management server from the cluster, then modify the properties, and add the server back to the cluster.

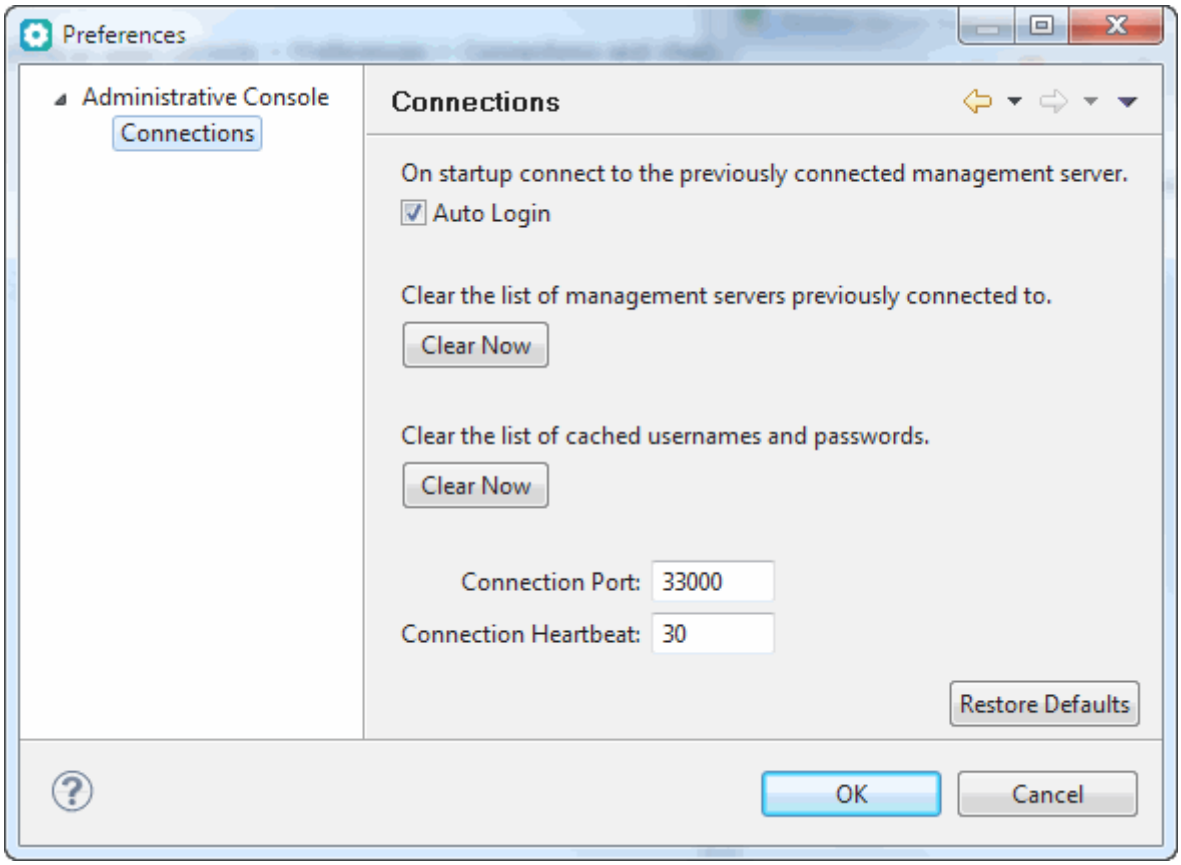
To change the management server address and port

1. Open `ManagementServer/conf/container.properties`. The management server address is located in this file and is specified by the host property.
1. By default, the property is left blank and the address is automatically set to the fully qualified machine name or the actual IP address. If the address is set to 'localhost' or '127.0.0.1' it is also set to the fully qualified machine name or the actual IP address.
2. Specify the address you want to use.

Locate the `rmi.port` (unsecure port) or `rmi.port.ssl` (secure port) properties. The default values are 33000 for the secure port and 33001 for the unsecure port.

Specify the port number you want to use.

Restart the management server.



Note

The server name is case-sensitive and must match the name defined on the General tab of the Session Server Property panel.

Additionally, if a port is not specified when connecting to a management server in the Administrative Console then, by default, it uses port 33000. If the management server port is changed, you will either have to specify the port when connecting or open Console > Preferences > Connections and change the default connection port.

To connect the Administrative Console to the management server through a firewall

You can configure the management server secure RMI port to enable the Administrative Console to connect through a firewall.

Edit the `Micro Focus/Verastream/ManagementServer/conf/container.properties` file.

Set the desired port number in the `rmi.export.port.ssl` line (0 is the default for a random ephemeral port).

After saving the changed file, restart the management server.

More information

Technical Note 10105: Ports Used by Verastream Host Integrator 7.x

Adding a Management Server

Removing a Management Server From a Cluster

Understanding Management Servers

3.4.6 Working with Management Server Clusters

A management server cluster is a grouping of one or more management servers. When a cluster contains more than one management server data is automatically replicated across all servers in the cluster. Clustering management servers can provide failover and load distribution support. Management servers can be easily added and removed from a cluster using the Administrative Console. As you add management servers they display in the Management Server Explorer tree view. You can edit the properties for each server or for the cluster as a whole.

What is replication?

Replication is the process of sharing information between management servers. This ensures that the content is consistent between each server. Multiple management servers, called a cluster, increase the number of computers available to clients and so reduces the load on each one.

> **Note**
>
> All management server data is replicated. This replicated data includes load distribution domains, authentication and authorization security configurations (directory services), and session pool schedules.

Why set up a management server cluster?

A cluster, which is a group of linked computers, improves performance and provides enhanced availability. Clusters are used to provide failover and load balancing functions.

There are a few things to remember when you're setting up a management server cluster:

- It is important that all management servers in a cluster are able to communicate with all other management servers in the cluster using the address specified by the management server.
- Make sure that all management servers in a cluster have their time and dates in synch. Otherwise replication problems may occur.
- When you remove an online management server from a cluster it is returned to its initial state, however the user name and password that was configured for the management server is retained.

More information

- Removing a Management Server From a Cluster
- Adding Management Servers to a Cluster
- Configuring Management Servers for Failover

3.4.7 Adding a Management Server to a Cluster

During the install process you can choose to add a management server to an existing cluster, if you do not do so, a new management server cluster is created consisting of the newly installed single management server. You can add other management servers to this cluster or, post-installation, you can add this management server to an existing cluster.

To add a management server to a cluster

In the Management Server Explorer tree, select the management cluster, and click  to add a management server to the cluster.

Type the name of the management server you want to add to the cluster.

Type the credentials needed to access the management server, and click OK.

You can add multiple management servers to a management server cluster.

More information

Adding a Management Server

Working with Management Server Clusters

Removing a Management Server From a Cluster

3.4.8 Configuring Management Servers for Failover

When you set up a management server failover configuration if one of the management servers fails or is offline, another management server in the cluster can provide services. Failover configuration provides fault tolerance for production environments.

Configuring Failover

You establish failover support by installing multiple management servers, adding them to a single management cluster, and configuring your DNS (Domain Name System) server to associate all management servers in the cluster with one symbolic name.

THINGS TO REMEMBER

Management server and session server components have separate failover mechanisms. Session server failover and load distribution is addressed separately in Technical Note 10108.

In a multi-server failover environment, all servers (running management server or session server components) must be able to communicate with each other, and the clients (running connector API) must be able to communicate with all servers.

Each management server (and each session server) can belong to only one cluster or installation

Management Server failover is based on standard IP name resolution functionality, which allows an alias name to be mapped to multiple IP addresses.

HOW DOES IT WORK?

If you have 3 different management servers installed on 3 different machines called machine1, machine2, and machine3 and have added them to a single cluster, then you can setup a DNS entry with the symbolic name my-management-cluster and in that DNS entry you can add machine1, machine2, and machine3.

When a client wants to connect to the management cluster, instead of providing the address of a management server in the cluster (for example, machine1), the client provides the DNS symbolic name, my-management-cluster. Because the DNS entry contains more than one machine, the DNS service provides the list addresses configured for the entry. If a management server is not running, then the client can connect to another server configured for the DNS entry, and failover support is achieved.

You can also configure the DNS service to achieve load balancing support. Since data replication automatically occurs between all servers in a management cluster the client will have the same experience regardless of the management service to which they are connected.

Setting Up Management Servers for Failover Support

Management server clusters can be set up during installation or anytime using the Administrative Console Management Server Explorer.

During installation, after you install Host Integrator and the management server component on the first server, select **Join an existing installation** and use the host name or IP address of the first server when installing on subsequent servers.

2. Create a single DNS alias (common name) for all the IP addresses of management servers in the installation environment. Each management server IP address must be assigned to the same common name.

   Recommended method: For ease of maintenance, configure you DNS server to setup failover support. The DNS server can return results in round-robin or random order for load distribution, as the default management server configuration (`ManagementServer/conf/container.conf` file) has DNS caching disabled (`-Dsun.net.inetaddr.ttl=0`).

   Alternative method: If you cannot configure your DNS server, you can edit the hosts file on each system with Host Integrator server or client components installed (including connectors used by client applications).

2. Example:

2.

```
# Hosts file on system "workhorse01"
# Verastream Host Integrator production environment in Seattle

# First entry is the unique name for the local system
10.0.0.1 workhorse01

# Common name for the management server cluster
10.0.0.1 vhi-prod-sea
10.0.0.2 vhi-prod-sea
10.0.0.3 vhi-prod-sea
```

If you use this method, update the hosts file on all systems in the environment. All servers (running management server or session server components) must be able to communicate with each other, and the clients (running connector API) must be able to communicate with all servers.

2.

2. The local unique system name is listed separately first to avoid problems with reverse DNS lookups on some platforms. This is followed by lines for the cluster common name (one line for each system running the Management Server service).

2. For systems that have multiple network interfaces, all IP addresses should be listed. On Windows systems, the hosts file is typically located in the `C:\Windows\System32\drivers\etc` folder. On Linux systems, the hosts file is located in the /etc directory.

2. Networking protocols mandate that the hostname contain only ASCII letters a through z (case insensitive), digits 0 through 9, and the hyphen character (-). Comments beginning with the # character (through the end of the line) are ignored.

3. In Administrative Console, it is a good idea to change the name of the management cluster (Perspective > Management > Servers > Management Cluster > Properties). The default

cluster name is the system host name where management server was first installed, but you can change it to the cluster DNS alias for your installation environment. The cluster name displays in the Administrative Console status bar (lower right) when connected.

4. To achieve failover capability, enter the cluster DNS alias name whenever you are required to provide a management server address:

   In your client application, when calling `ConnectToSessionViaDomain` or `ConnectToModelViaDomain` method in the connector API.

   In your Web Builder project properties, when "Connect to model via domain" or "Connect to session pool via domain" is selected for the model connection.

   In the embedded web service functionality, if you are configuring it to use a load distribution domain (see Technical Note 10092).

   In Administrative Console, when prompted to connect.

4. However, when you deploy models (using either the activatemodel and deactivatemodel commands or Design Tool), use the specific individual session server system names (not the cluster common alias name).

What happens at runtime?

When establishing a connection to the management server alias name, IP name resolution returns the list of IP addresses. An attempt is made to contact the first address in the list. If no response is received, the next address is tried, and so forth.

When deploying models, the session server contacts the management server for authentication and authorization. If you see the following errors when deploying a model, you may have an incorrect configuration in step 2 above.

```
[VHI 3852] Deployment of model failed: Cannot establish management session<br>
[VHI 3852] Deployment of model failed: Token binding is invalid
```

More information

Adding a Management Server to a Cluster

About Management Servers

Adding Management Servers

3.4.9 Removing a Management Server From a Cluster

You can see in the Management Server Explorer tree which management servers are online.

 Denotes online status

 Denotes offline status

To remove an	Do this...
Online management server from a cluster	In the Management Server Explorer tree, select the server you want to remove. Click delete to remove the management server from the cluster.

To remove an	Do this...
Offline management server from a cluster	If an offline management server is removed from a cluster, the server must be manually reset back to its initial state before you can return it to the cluster. To reset the management server: Open the `ManagementServer\bin` directory. Depending on your operating system, run either `resetserver.bat` or `resetserver.sh` against the offline management server. This script file resets the server to its initial state. If you run the `resetserver.bat` script on a system with UAC enabled, then you must run the script with administrator privileges. The administrative password for the management server is reset to the default value - 'secretpassword' after you reset the management server configuration.

Note

If a management server is uninstalled before it is removed from a cluster, you will be prompted to reset the server when you attempt to remove it from the cluster. This message can be ignored.

More information

Adding a Management Server to a Cluster

Working with Management Server Clusters

Configuring Management Servers for Failover

3.5 Configuring Directories

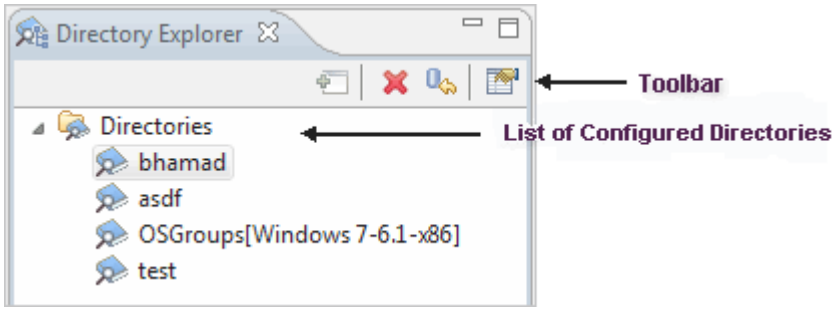
3.5.1 What is a Directory?

A directory is a collection or list of objects arranged in a logical and hierarchical format. Directory services provide the ability to query and edit those objects.

From the Directory perspective in the Administrative Console you configure the connection properties for a directory. You can use any directory type that exposes LDAP, including Active Directory (a Microsoft technology). The Administrative Console provides default values for the schema properties associated with most Active Directory configurations. However, if you want to use a different directory type, you can choose generic LDAP. To work with a generic LDAP directory service, you can modify the schema properties to match your directory configuration. You can work with both types of directories using the same workflow; simply provide the necessary schema properties.

Directory Explorer

In the Directory Explorer you can add directories, delete directories, view and edit directory properties, and verify your directory connection using the toolbar.



The order in which the directories display in the Directory Explorer is the order in which the directories are accessed. You can change the order in the Processing Order property page. Any changes you make are reflected in the Directory Explorer.

More information

Adding or Removing Directories

Using LDAP Directories

3.5.2 Adding and Removing Directories

You can add an Active Directory or one that exposes generic LDAP. The procedure is the same. To work with Directories, from the main toolbar, expand the Management drop down list, and then select Directories to open the Directory Explorer.

Add a directory

The Add Directory wizard, consisting of three pages, walks you the steps necessary to connect successfully to a directory. After you complete the first page, Connection Configuration, you can skip the other pages if you do not need to modify the schema and domain configuration pages.

CONNECTION INFORMATION

In the Directory Explorer perspective toolbar, click  . The Add Directory Wizard Connection Configuration Page displays.

From the Directory Type drop down list, select which directory type you want to connect to.

Provide the necessary information to connect to the directory:

Name: The name of the directory you are connecting to

Address: The directory address (for example, microfocus.com)

Port: The port number to use for LDAP authentication requests. By default, this is set to port 389. If you are connecting using SSL, the default secure port is 636. You must enter the port that your network is using.

Base DN: The distinguished name (DN) of the node in the directory where you want the connection rooted. All children nodes of this node are included when searching for user and groups to add to authorization profiles. A typical base DN might look like: DC=attachmate,DC=com. DC is an abbreviation for domain components.

User name The name of the user to use when making connections to this directory

Password: The password to use for the user named above

4. Select Secure Connection to connect to the directory service using SSL. If you are not using SSL, skip to step 5.

   Click **Add Certificate** to browse for the certificate associated with the directory. Obtain this certificate from the directory administrator.

1. A certificate is an electronic document used to identify an individual, a server, a company, or some other entity and to associate that identity with a public key. Like a driver's license, a passport, or other commonly used personal IDs, a certificate provides generally recognized

proof of a person's identity. Public-key cryptography uses certificates to address the problem of impersonation.

Click **Certificate Info** to see basic certificate information for the certificate that you added for this directory. This option is enabled when a certificate is added.

Click **Test Connection** to verify the connection is successful. If, for some reason, the connection is not successful, it is easier to make the necessary changes before you click OK.

Click Next to enter schema and domain information, or accept the default values on those panels and click Finish.

SCHEMA INFORMATION

You need to supply the schema information that will be used to look up entries on the new directory. If you are using Active Directory, the default values are in place and most likely will not have to be modified. If you are connecting to a generic LDAP directory, you may need to edit the schema values.

User attribute: Specifies the name of the attribute that is used to determine if a directory entry represents a user. See the documentation for your LDAP server if you are unsure what to enter here.

User value: Specifies the value that the user attribute must have in order for a directory entry to be considered a user.

Group attribute: Specifies the name of the attribute that will be used to determine if a directory entry represents a group.

Group value: Specifies the value that the group attribute must have in order for a directory entry to be considered a group.

Member attribute: Specifies the name of the attribute indicating which users are members of a group.

MemberOf attribute: Specifies the name of the attribute indicating what groups a user is a member of.

Entry Name attribute: Specifies the name of the attribute which indicates an entry's name. For example, a user might use the login bobsm, but the entry name will read Bob Smith. The entry name is displayed in the user search dialog box, but the user login is added to authorization profiles.

Login attribute: Specifies the attribute that indicates a user's login.

> **Note**
>
> You can enter a list of values in both the User and Group Value properties fields. You must separate each value by a comma. Additionally, a value can be preceded by the '!' character to indicate that the attribute cannot have this value. For example: if the value is "user,!computer" then the attribute must have the value user and cannot have the value computer.

DOMAIN INFORMATION

You can optimize the directory performance by limiting the range of the search.

- **Remove User Domain**: Ignore whatever domain information is provided by the user.

  For example, if a user supplies `micro focus\bobsm` the domain `micro focus` will be removed and only the string bobsm will be sent to the directory for authentication. This property can be used to allow users to enter what they are used to entering while supplying the directory with what it expects for authentication.

- **Default Authentication Domain**: Add the name of the domain to be used when authenticating users.

  For example, if during authentication a directory is looking for the domain\user_name and the domain is constant, then you can simplify the process for your users by requiring them to enter only their user name. If you set domain1 as the default authentication domain, then domain1 will be added to the user name; domain1\user_name. If you specify a Default Authentication Domain and the Remove User Domain is enabled, then any domain that the user specifies is replaced by the default.

- **Domain Mappings**: If you have multiple directories you can map a domain to a specific directory. This increases directory performance by only trying to authenticate against a directory which matches the domain supplied by a user and not trying all directories in the processing order.

Remove a directory

To remove a directory, select the directory from the Directory Explorer and click  on the Directory Explorer toolbar.

More information

What is a directory?

Using active directory

3.5.3 Using LDAP Directories

Lightweight Directory Access Protocol (LDAP) is a TCP/IP protocol for updating and searching directories.

When you add a directory in the Administrative Console, you can choose to add **Generic LDAP**. When you configure an LDAP provider in the console, user and group directory services are authenticated by an LDAP service provider.

There are performance implications to using LDAP. Because each request for services goes across the network to the LDAP server every time services are requested, your LDAP configuration should be optimally configured to respond quickly to requests from Administrative Console clients.

For complete information on the LDAP parameters required to use LDAP, please refer to your LDAP server documentation.

LDAPS

When possible, you should make secure LDAP connections over SSL or TLS (LDAPS). To enable LDAPS in the Adminstrative Console, add a valid certificate and check the Secure connection box.

The Administrative Console also supports secure connections using Channel binding and Signing without extra configuration on the client. To learn more about Channel binding and Signing, as well as how to enable them on your servers, check out this article from Microsoft.

Using Active directory

Active Directory is a Microsoft technology that provides network directory services. Active Directory uses objects, which are users, systems, and resources, and places them in a hierarchical framework. Since many organizations already have an Active Directory which contains user and group information, the management server can be configured to use the Active Directory as a source for authentication and authorization information.

If you choose Active Directory when you add a directory, then default schema information is provided. You can always edit this information.

More information

Adding or removing directories

3.5.4 Accessing directories

The order in which the directories display in the Directory Explorer is the order in which the directories are accessed. You can change the order in the Processing Order property page. Any changes you make are reflected in the Directory Explorer.

What are OS Groups?

OS (Operating System) groups are local user groups differentiated by their operating system. These groups work like directories, but provide no replication. In additon to using external LDAP capable directories as a source for authentication and authorization, you can use local OS Groups.

To enable OS Groups support select the check box on the Directories properties page. The OSGroup directory displays in the Directory Explorer tree.

Schema and Connection properties are not supported in OS Groups. Only Domain properties are available for the OSGroups directory.

When adding members to authorization profiles, you can use OS Groups as a source in the Add Members dialog box, however, only groups are supported and not users.

To disable OS Groups support clear the check box on the Directories properties page.

> **Note**
>
> If OS Groups are enabled in a clustered environment it is very important to ensure that all machines in the cluster have the same groups (including the same users as members of the groups) defined to avoid inconsistent runtime behavior.

More information

Adding or removing directories

Using LDAP directories

3.6 Using Authorization

3.6.1 Using Authorization and Authentication

When you set up authorization and authentication, you are establishing access control to the system. Access is controlled by assigning users and groups to particular profiles, each of which has different access requirements and restrictions.

When the Administrative Console is installed, the password is set for the "admin" user. The "admin" user is automatically a member of all authorization profiles, but does not display in the list of profile members and cannot be removed.

About Profiles

Each profile provides a different level of access or permission to use parts of the console. To authenticate users and authorize groups you must assign them to one of these profiles:

Profile	Description
Administrator	An administrator can interact, monitor, and configure the different activities available through the Administrative Console.
Developer	Developers can log into the Administrative Console and view all current configurations, but cannot make changes. Developers of client applications are typically assigned to this profile.

Profile	Description
User	Users cannot log into the Administrative Console.

Other Micro Focus products that use the Verastream Management Server can assign additional rights to these authorization profiles. Descriptions of those roles are available in each individual product's online help.

More information

Adding Groups or Users to a Profile

Adding or Removing a Directory

3.6.2 Adding Groups or Users to a Profile

To work with Authorization, from the main toolbar, expand the Management drop down list, and then select Authorization to open the Authorization Explorer.

You can use any number of external LDAP capable directories as a source for authentication and authorization.

To add a group or user

1. Open the Authorization Explorer, select the profile to which you want to add members.
1. The current members of each profile are listed in the right pane.
2. Click  to add a member to the selected profile.

In the **Add Members** dialog box, select the directory you want to use to search for users and groups.

From the Type drop down list, choose whether you are searching for a group or a user.

5. In the Filter field enter appropriate search criteria.
5. The asterisk (*) *is a wildcard character that, when used by itself, says find all users or groups. To narrow your search results you can use the asterisk in conjunction with other characters. For*

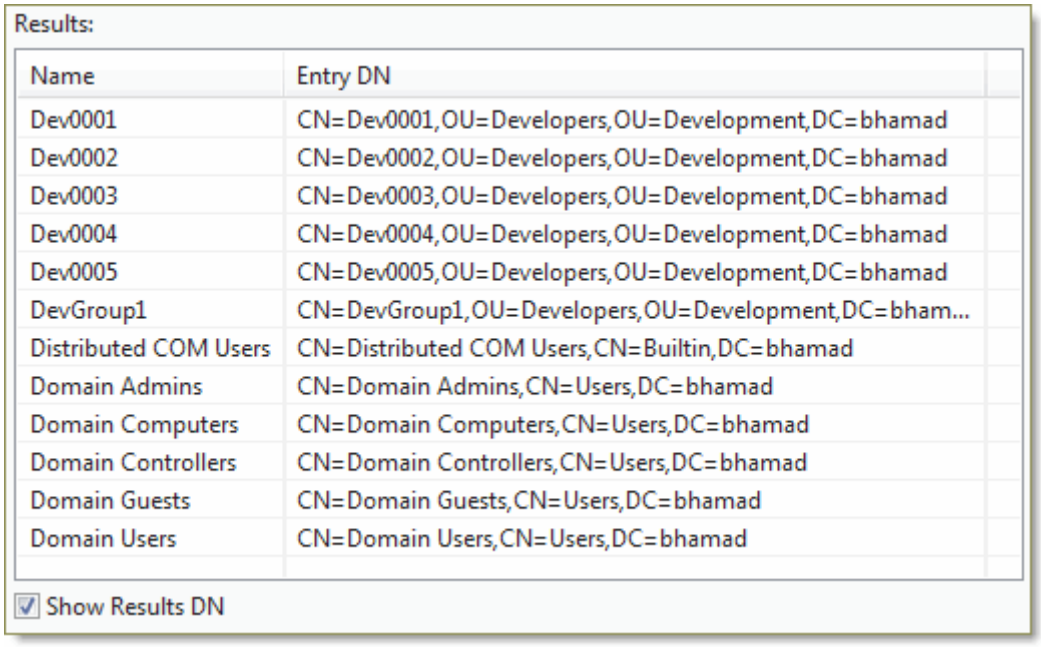
example, if you have a filter "B", then your search results will contain all elements that start with the letter "B".

6. Click Search to search the chosen directory with the given criteria.
6. If searching for users the search results will contain all elements in which the Entry Name attribute and the Login Name attribute match the search criteria. The entry name displays in the search results field, but the login name is added to the authorization profile.
7. In the Results field, locate the group or users you want to add. You can select multiple entries.

Click Add to add the selected users or groups to the authorization profile. The added members display in the Member pane of the Administrative Console.

Click Reset to clear the search results and continue searching for additional members to add.

Select **Show Results DN** to have the Entry DN display in the results table. The Entry DN is the distinguished name of the entry in the LDAP directory. For example, results with this option selected:



The last element of the DN is the name of the directory. You can determine the full DN of this entry by looking at the Base DN configured for the directory.

For example, if the Entry DN shows **CN=Domain Admins,CN=Users,DC=micro-focus** and the directory called Micro Focus has a Base DN property **DC=micro-focus-ldap,DC=com**, then the full DN for the entry would be **CN=Domain Admins,CN=Users,DC=micro-focus-ldap,DC=com**.

You cannot add users and groups to an authorization profile until either a directory has been added or OSGroups have been enabled in the Directories perspective. If you select OSGroups in the Directories list, then only groups are searched for and the **Show Entry DN** option cannot be selected.

More information

Using Authorization and Authentication

What is a Directory?

4. Legal Notice

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.