Host Access Management and Security Server Administrative Console
Users Guide
August 2016
## Contents

### About the Administrative Console

5

### 1 Using the Session Manager

7

- Add a session. ................................................................. 7
- Edit a session ................................................................. 8
- Export a session. ............................................................. 8
- Launch Session Manager ................................................ 10

### 2 Using the Access Mapper

11

- Map sessions to users ...................................................... 11
  - Selecting sessions ....................................................... 12

### 3 Setting Access Control Options

15

- Choose Authorization Method ........................................... 15
- LDAP Configuration .......................................................... 15
  - LDAP server ............................................................... 16
  - Search base and groups/folders ...................................... 17
  - Authentication of end users .......................................... 18
  - Advanced settings ....................................................... 18
- SiteMinder Configuration .................................................. 18
About the Administrative Console

The Host Access Management and Security Server provides a browser-based central point of administration so you can quickly configure and deliver terminal sessions to your users and leverage your existing user and group directories to control terminal access.

The Management and Security Server Administrative Console consists of a navigational panel and various components: the Session Manager, Access Mapper, and Access Control Setup.

Getting started with the Administrative Console

From the Start menu, select Micro Focus Host Access Management and Security Server, and then Administrative Server to open the Administrative Console.

Use the Administrative Console to:

- View sessions that reside on supported session servers.
- Add, edit, and delete sessions.
- Configure client authentication and authorization using your existing identity management system, such as LDAP.
- Map sessions to users.
1 Using the Session Manager

The Session Manager provides a view of all your sessions. Use the Session Manager to create and modify terminal sessions. If you have not added any sessions, use the Add Session panel to configure and add a session.

Once you have added a session, it is presented in a table to which other sessions can be added, edited, renamed, copied, or deleted. You can customize the table, choosing columns to display or hide, depending on what works best for you.

From the Session Manager Action menu, you can also export sessions from one type to another. Currently you can export a Reflection for the Web session and create a Reflection ZFE session.

To assign users to a session

The Administrator assigns users or groups to specific sessions using the Access Mapper.

From the left panel, open the Access Mapper. Use the options to specify the sessions that appear on your users’ session list. Use the Session Manager to add new sessions.

Related Topics
- Edit a session
- Add a session
- Export a session
- Setting Access Control Options
- Using the Access Mapper

Add a session

Required fields are marked by an asterisk.

1. From the Session Manager, click Add.
2. Choose the type of session you want to add.
3. Enter a name for the session. Session names must be unique and cannot exceed 64 characters. Quotation marks (" ") are not valid characters and cannot be used in the session name.
4 Enter the address for the session server. For example, http://zfe-ci.mycompany.com:7070/zfe, where the port and server name identifies the server where the session resides.

5 Click Launch to start the session in administrator mode in a separate window and configure the session.

In the Administrative Console, after you’ve saved the session settings, you can open the Access Mapper to make the session available to end users or return to the Session Manager to add or edit more sessions.

Related Topics
- Setting Access Control Options
- Using the Access Mapper
- Edit a session
- Export a session

**Edit a session**

1 Select the session you want to edit.
2 Open the Actions menu and choose Edit or alternatively you can click the session name from within the Session Manager table.
3 Information on the session is available for you to edit. The Description field is a read only field and cannot be edited.
4 Click Submit.

Related Topics
- Setting Access Control Options
- Using the Access Mapper
- Add a session
- Export a session

**Export a session**

You can export one type of session and create a different session type using the Export option available from either the Actions menu or from the right-click context menu. After a session is exported, the original session remains unchanged in the session list. Currently you can export Reflection for the Web sessions and create Reflection ZFE sessions.
In the Session Manager, choose the session you want to export. Session types are identified by an icon in the Type column. In the image above the selected session is a Reflection for the Web session.

Reflection ZFE sessions are denoted by the Reflection ZFE icon . Currently you can export and change Reflection for the Web sessions to Reflection ZFE sessions.

From the Actions menu, choose Export or alternatively right-click on the selected session and choose Export.

On the Export panel, type the name of the exported session and the address of the Reflection ZFE Session Server that will host the session. These are both required fields marked by an asterisk.

Click Create. The new session is now available in the Session Manager list to be assigned to users.

The original session is unchanged and remains available in the session list.

**Related Topics**

- Setting Access Control Options
- Using the Access Mapper
- Add a session
- Edit a session
Launch Session Manager

After you launch your session and complete the session configuration in a separate browser window, you can return to the Administrative Console and continue to add or edit sessions. You can also use the Access Mapper to make sessions available to end users.

**TIP:** The recommended work flow is to always complete your session configuration and select Exit in the left navigation panel before continuing to make any changes in the Administrative Console.

**Related Topics**

- Setting Access Control Options
- Using the Access Mapper
- Add a session
Using the Access Mapper

Use the Access Mapper to make sessions available to users. The user can easily access these sessions from the list of sessions which are presented to them after they log in.

If you are using LDAP to authorize sessions, you can search for a specific user or group and then map that user to the available sessions that display in the Sessions panel.

If you are not using LDAP to authorize session access, the Access Mapper lists the terminal sessions you configured in the Session Manager. You can then select those sessions you want to be made available to your users’ session list.

Using Automated Sign-On for the Mainframe

Automated Sign-On for the Mainframe is an add-on product for Management and Security Server that enables an end user to authenticate to a terminal emulation client and be automatically logged on to a host application on the z/OS mainframe.

There is additional configuration necessary when you are mapping sessions to your end users to implement Automated Sign-On.

NOTE: Before you can configure user mappings for Automated Sign-On:

- The Automated Sign-On add-on must be installed and configured on the Host Access Management and Security Server. For information on how to install and configure the Automated Sign-On feature, see Automated Sign-On for Mainframe Administrator Guide.

Related Topics

- Map sessions to users
- Using the Session Manager

Map sessions to users

1. Select Users or Groups from the list.
2. Enter a user or group name, the asterisk (*) wildcard, or a combination of * and letters in the text box.
3. Click Attributes to narrow your search using the available filter attributes. There are a default set of attributes that are already selected, but you can select or clear attributes to refine your query.
4. Enter your search value in the search field and press Enter. The search results display in the left panel. Use the arrows at the bottom of the panel to page through the list.
Selecting sessions

Check the terminal sessions that you want to make available to your users. If you selected LDAP authorization, the sessions that you select appear on the session list for the specified user or for the users within a specified group.

The Administrative Server does not support mapping sessions to Active Directory primary groups (for example, Domain Users).

An asterisk denotes that a user has inherited access to that session by having membership in a group. For example, if you map a session to a group of which User 1 is a member, then that session is listed with an asterisk (*) denoting the session is inherited. If a session is inherited, you can remove access to that session by clearing the “Allow user to inherit access to sessions” option.

**NOTE:** Granting access to all users means that you are granting access to the search base, and all users inherit that access. Such access is only extended to users when the “inherit access” option is checked.

Mapping user names for Automated Sign-On

After the Automated Sign-On add-on has been installed and configured on the Management and Security Server, set authorization by mapping access for all your users and groups to their sessions.

Mapping users’ access to the sessions you created specifies the session URLs available to each user. You can map access by individuals or groups.

1. For the selected user or group, select the sessions in the Sessions panel they are entitled to access.
2. Click **Edit**. The Edit option is only available if the Management and Security Server is correctly installed and configured, the session is mapped, and access to the session is not inherited from a group to which the user belongs.
3. On the **User Mapping** panel, choose the method you configured for determining the user’s name or group’s mainframe username:
   - **Not set**
     
     The default must be changed for automated sign-on.
   - **Literal value**
     
     This option is available for sessions mapped to users, but not groups. Enter a value that meets these criteria:
     
     - up to eight alphanumeric characters
     - no spaces
     - no other characters
   - **Derive from UPN**
     
     Select this option to request a passticket from DCAS by deriving the mainframe username from the User Principal Name (UPN) of the user. The UPN is typically available from a smart card or client certificate, and is a standard attribute in Active Directory servers. A UPN is formatted as an Internet-style email address, such as userid@domain.com, and Management and Security Server derives the mainframe username as the short name preceding the ’@’ symbol.
   - **Get LDAP attribute value from authenticating directory**
     
     Select this option to perform a lookup in the LDAP directory (defined in Access Control Setup) and return the value of the entered attribute as the mainframe username.
All LDAP attributes must meet these criteria:

- must begin with an alpha character
- no more than 50 characters
- any alphanumeric character or a hyphen is permitted

Get LDAP attribute value from secondary directory using search filter

Select this option to use the search filter to find the user object in the secondary LDAP directory; then return the value of the entered attribute as the mainframe username.

4. Click OK.

Other options

These options are available only if you selected LDAP authorization.

- Access to Administrative Console
  Select this option to make the Administrative Console available to this user or to users within the specified group.

- Allow user to inherit (*) access to sessions
  Select this option to have session access inherited from groups to which the user belongs. Clearing this option removes the group mappings for inherited sessions.

Related Topics

- Setting Access Control Options
- Using the Session Manager
Setting Access Control Options

You can use access control features to validate a user’s identity (authentication) and to assign a session to specific users or groups (authorization).

Authentication validates the user’s identity based on some credentials, for example, a username/password combination or a client certificate. You can use any of the following methods to authenticate users:

- **None** - Management and Security Server does not present a login screen. Any user can access their assigned sessions without being prompted for credentials. Session authorization is not available.

  **NOTE:** If you set the authorization method to None, be aware that all users are logged in as Guest. During session configuration, it is best not to allow users to modify their session settings (User Preference Rules), as they can overwrite each other’s choices.

- **LDAP** - Management and Security Server makes a read-only connection to your existing LDAP (Lightweight Directory Access Protocol) server to verify usernames and passwords. You can also use LDAP to authorize session access. LDAP is an industry standard application protocol for accessing and maintaining distributed directory information services over a network.

- **SiteMinder** - To implement this option on a Windows system, install both the Administrative Server and a SiteMinder web agent on the same machine as IIS, and set up the server to use your IIS web server.

The access control setup options will vary based on your selection.

Choose Authorization Method

- **Allow authenticated users to access all published sessions**
  
  The Access Mapper presents a list of sessions that you can choose to publish to end users.

- **Use LDAP to restrict access to sessions**
  
  The Access Mapper allows you to map sessions to LDAP users or groups. Logon userids must match those in the LDAP directory. After you publish or map sessions, they appear in the authorized end users' list of available sessions.

LDAP Configuration

Use the options on this page to configure Management and Security Server to use your LDAP server to regulate access to terminal sessions. The LDAP administrator for your organization can give you more information about how to configure these options.
LDAP server

Describe your LDAP server using these settings.

- **Server type**
  
  Select the type of LDAP server you are using from the list. The options on this page change depending on the LDAP server type you select. If you do not see your specific LDAP server in the list, select **Generic LDAP Compliant Directory Server (RFC 2256)**.

- **Security options**
  
  Data can be passed between the Administrative Server and the LDAP server in clear text or encrypted. The type of encryption used depends on your LDAP server. Kerberos v. 5 is available for Windows Active Directory, and TLS/SSL for all other servers.

  By default, Management and Security Server transmits data between the Administrative Server and the LDAP server in clear text. If you choose this option, you should prevent users from accessing the network link between these two servers.

<table>
<thead>
<tr>
<th>Encryption type</th>
<th>Description</th>
</tr>
</thead>
</table>
  | Kerberos v.5    | When you select Windows Active Directory with Kerberos, you must enter the name of the Kerberos key distribution centers. Multiple key distribution centers, delimited by commas or spaces, can be used. If you do not know the name of the Kerberos key distribution center, enter the fully-qualified DNS name of the Active Directory server.

  The option under the key distribution center name field allows you to encrypt all data transmitted over the Kerberos connection. By default, only user names and passwords are passed securely between the Administrative and LDAP servers using Kerberos. Encrypting all data is more secure, but may increase performance overhead.

  TLS/SSL

  When you select TLS/SSL security, the Administrative Server negotiates a TLS or SSL v3 protocol version for the connection with the LDAP server. The protocol version negotiated with the LDAP server depends in part on the TLS and SSL protocol versions allowed by that server. The Administrative Server supports SSL v3 for backwards compatibility with older LDAP servers; however, use of SSL v3 is not recommended. If there are some TLS or SSL protocol versions that you do not want to use for LDAP connections, you should disable those protocol versions on the LDAP server.

  To configure security for TLS/SSL connections, you must first import the server’s trusted certificates into the JRE’s default trusted keystore:

  1. Import the certificate to the JRE’s keystore file named "cacerts", located in 
     [Management and Security Server Install \jre\lib\security].

     Example: C:\Program Files\Micro Focus\MSS\jre\bin>keytool -import -trustcacerts -alias myHost -file myHost.cer -keystore ..\lib\security\cacerts

     For more information, see the Java SE 8 documentation for the `keytool` security tool.

  2. Enter the Java keystore’s default password: `changeit`

  3. Restart the Administrative Server.

- **Server name**
Enter the LDAP server name as either a name or a full IP address. If you selected TLS/SSL above, this LDAP server name must exactly match the Common Name on the LDAP server's certificate. Multiple server names, delimited by commas or spaces, can be used for failover support. If an LDAP server is down, the next server on the list will be contacted. In this case, all fields specified on this page that are used for LDAP connections should be available on all the LDAP servers, and should have identical configurations.

- **Server port**

  Enter the port used by your LDAP server. The default is 389 for plain text or 636 for TLS/SSL. If you are using Active Directory, you may wish to set the server port to the global catalog port, which is 3268 (or 3269 over TLS/SSL). Global catalog searches can be faster than referral-based cross-domain searches.

- **Username and password**

  Provide the username and password for an LDAP server account that can be used to access the directory in read-only mode. Generally, the account does not require any special directory privileges but must be able to search the directory based on the most common directory attributes (such as cn, ou, member and memberOf). Type in the password again in the Password confirmation box.

  If this account password changes and the Administrative Server's configuration is not updated to use the new password, your users will get error messages when trying to authenticate. To resolve the problem, update the account password here and save your new settings. To avoid this problem, you may wish to set up an account that is not subject to automatic password aging policies, or that will not have the password changed by other administrators without notice.

  **NOTE:** The user name must uniquely identify the user in the directory. The syntax depends on the type of LDAP server you are using.

  - If you selected Windows Active Directory and Kerberos, enter the userPrincipalName (e.g., username@exampledomain.com). The userPrincipalName is case sensitive. Case sensitivity does not apply to end user logins.
  
  - If you selected Windows Active Directory with Plain Text, enter the NetBIOS domain\samAccountName (e.g., exampledomain\username), userPrincipalName (e.g., username@exampledomain.com), or distinguished name (e.g., uid=examplename,DC=examplecorp,DC=com).
  
  - If you selected any other LDAP server type, enter the distinguished name (for example, uid=examplename,DC=examplecorp,DC=com).

- **Search base and groups/folders**

  - **Directory search base**

    Enter the distinguished name of the node in the directory tree you want to use as the base for Administrative Server search operations. Examples: DC=my_corp,DC=com or o=my_corp.com. For more information about how to describe the search base, see the LDAP administrator for your organization.

  - **Groups or folders**

    You can map sessions directly to users in the directory. You can also map sessions to either logical groups or folders. The choice of whether to use groups or folders should reflect the way the data in your directory is organized. In Management and Security Server, the term "folder" is used to describe both organizational units and containers. Most directories have an organizational structure that uses logical groups, for example, groupOfNames and groupOfUniqueNames.
Authentication of end users

LDAP attribute for identifier

The default LDAP attribute to use as an identifier is available when you select an LDAP server type.

**Table 3-1 Default LDAP identifiers**

<table>
<thead>
<tr>
<th>Server type</th>
<th>Default user identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenLDAP Directory Server</td>
<td>cn</td>
</tr>
<tr>
<td>Generic LDAP Compliant Directory Server (RFC 2256)</td>
<td>cn</td>
</tr>
<tr>
<td>RACF Directory Server</td>
<td>racfid</td>
</tr>
<tr>
<td>Oracle LDAP Directory Server</td>
<td>uid</td>
</tr>
<tr>
<td>IBM Tivoli Directory Server</td>
<td>cn</td>
</tr>
<tr>
<td>Windows Active Directory</td>
<td>List of domains**</td>
</tr>
<tr>
<td>NetIQ eDirectory</td>
<td>cn</td>
</tr>
<tr>
<td>Windows Active Directory with LDAP login form</td>
<td>cn</td>
</tr>
</tbody>
</table>

**When you select Active Directory as your LDAP server and the Kerberos security option, you must enter a list of Kerberos realms (e.g., domain@example.com). If you are using Active Directory with plain text, enter a list of NT domains (e.g., MYCOMPANY, SALES).**

When an end user requests the list of sessions, the login page prompts for a username and password and displays available domains or realms in a drop-down list. If you have more than one domain or realm, separate the entries with commas (for example, 1stDomain, 2ndDomain, 3rdDomain).

Advanced settings

Maximum nested level for groups

This number determines how mapped sessions are inherited. If Group A contains Group B of which User 1 is a member, and you map a session to Group A, User 1 will also have access to that mapped session. If users do not inherit sessions as you expect, increase this number. Do not raise this level more than necessary because too high a number can impair performance if you have a large number of users. The default is 5.

SiteMinder Configuration

Management and Security Server uses Microsoft IIS to integrate with SiteMinder. For instructions on how to integrate IIS with MSS and if needed, Reflection ZFE, see:

- Technical Note 2591 - Integrating Reflection for the Web with SiteMinder
- Technical Note 2859 - Using the IIS Reverse Proxy with Reflection ZF

If you have selected SiteMinder as your authentication method, complete the configuration:

- Agent version

  Some configurations vary depending on the version you select.
• Agent name
The name of the SiteMinder agent that is used by IIS. This is the Name of the agent configured to
work with IIS that is integrated with the Management and Security Server.

• Shared secret (version 4)
The secret used by the policy server to verify the agent. This is the Shared secret that was
created in the SiteMinder Administration tool under System Configuration > Agents.

• Policy server host (version 4)
The IP address (preferred) or DNS name of the host on which the SiteMinder policy server is
installed.

• Authentication port (version 4)
The SiteMinder policy server’s authentication port. The default for this port is 44442. To check
the port number, open the SiteMinder Policy Server Management Console, click the Settings tab,
and look for the Authentication port number under Access Control. If other SiteMinder port
numbers were changed from their defaults, you must reset the corresponding port numbers in
the Management and Security Server PropertyDS.xml file, located in the MSSData folder.

• Configuration file (version 5+)
Provide a full path to the SiteMinder host configuration file. This is typically SmHost.conf and
resides in the config directory in the SiteMinder web agent installation directory.

• User identity
Determines which SiteMinder user attribute is displayed in the list of sessions and used for
LDAP authorization.

• User identity LDAP search attribute (optional)
When the Administrative Server is configured to use authorization, use this field to specify the
LDAP attribute used by the Administrative Server to perform an LDAP search request for the
user's distinguished name (DN). During authorization, the Administrative Server issues an LDAP
search request to obtain the user's LDAP DN. The LDAP search request's filter uses the attribute
specified in this field.

For example, if you enter the value "uid" into this field, then the LDAP search filter will look like:
(uid=<SiteMinder username>) where <SiteMinder username> is the value of the SiteMinder
user's name, obtained from the SiteMinder session token, using the ATTR_USERNAME key.
Example: (uid=johns)

NOTE: When the Administrative Server is not configured for authorization, any value entered in
this field is ignored.

SiteMinder and 64-bit systems
If you’re using a 64-bit operating system, check to ensure that the SiteMinder installer has placed the
path to the 64-bit libraries before the path to the 32-bit libraries in the PATH variable. To confirm this,
open a command window and type: echo %PATH%.

If the 64-bit libraries are not first in the path, then edit the PATH variable so that the path to the 64-bit
libraries comes before the path to the 32-bit libraries.

Related Topics
• Using the Access Mapper
• Using the Session Manager