Guide to Securing ES

Securing Enterprise Server
Revision History

Revision No.	Date	Author(s)	Brief Description of Change
1.0	Aug 2017	Geoff Collier	First draft
1.1	Sept 14th 2017	Geoff Collier	Incorporated MWW comments, other clarifications, updated summary, added Glossary of Terms. Added esfadmin and esfupdate example commands
1.1.1	2017-09-20	Michael Wojcik	Import into Confluence, with some formatting changes to assist the import process.
1.1.2	2018-10-29	davs	Updated Links into Enterprise Developer 4.0 online documentation.

Table of Contents

Guide to Securing ES 1
01 Scope 3
02 Security Managers and securing MFDS Access 3
Security Managers and the Security Manager List 4
MLDAP ESM Module 4
Micro Focus or Active Directory Users 5
Stacked ESMs and Federation 6
64/32 bit ESM security managers/modules 7
MFDS Security 8
Restrict Admin Access 8
The 'Use default ES Security Manager List' option 8
Default ES Security Options 8
Verify against all Security Managers 8
Allow unknown resources 8
Allow unknown users 8
Use all groups 8
03 Securing a Region for Access and Resources 9
Which Security Manager to use? 9

ES Resources 9
Starting and Stopping a Region 10
Start on System Start and 'Automated Execution Control Enterprise Server Credentials' 10
04 Securing Applications 10
05 Securing the OS 11
MFDS files 11
MFDS repository 11
mfdsacfg.xml 11
Server and Client configuration files 12
Mf-server.dat 12
MF-client.dat 12
Cciusers.dat 12
Dfhdrdat 12
LDIF files 13
06 Maintaining the Security Repository 13
The ESF GUI interface 13
Using MFDS to view and modify Resources 13
07 Default Users and Groups 13
Default users 14
Default groups 15
CAS default groups 15
MFDS default groups 16
08 Securing Communications 16
MFDS and TLS/SSL 17
MFCS Listeners and TLS/SSL 17
Securing other clients and servers with TLS/SSL 17
Configuring a Listener's TLS Protocols and Cipher Suites 18
Storing certificates and keys 18
Some common certificate file formats 18
09 Command Line Utilities 19
10 Caching 20
11 Security Auditing 20
12 Summary and Recommendations 21
13 Glossary of Terms 21

01 Scope

This document will describe the various security-related aspects of an Enterprise Server (ES) installation and how these can be used to 'harden' an Enterprise Server (ES) installation.

It will explain what the different security options are in ES and will provide information about each aspect to enable sensible decisions to be made about ES security.

The intended audience is for customers who want to ensure that their Enterprise Server installation is only accessible to known users and/or who want to use encrypted communications channels to secure username/password information.

It is also for Micro Focus support staff etc when they need to establish a certain level of secure system as required by any current incident or testing activity.

This document will allow clients to configure ES to prevent any unauthorised access, and to secure the communications channels so that passwords etc. are transmitted in an encrypted manner.

The collection of information in this document will provide clients with a single resource which can then be used as a guide to ensuring systems are configured satisfactorily from a security point of view. This document provides a more complete presentation of all the relevant security information compared to the online docs. References to topics in the online documentation are provided where relevant.

Once the information in the document has been digested, it should be possible to configure LDAP-based security for MFDS and production regions with sensible defaults and, having understood the SSL/TLS aspects, it should be possible to secure all communications channels that carry sensitive data.

Operating System aspects are also considered so that certain files and directories can be locked-down and appropriate accounts setup to run ES processes in a controlled manner.

Any un-needed features could be disabled, and this can include some of the default user accounts.

02 Security Managers and securing MFDS Access

External Security Managers (ESMs) are defined in the 'security managers' tab (in MFDS). Many security managers can be defined. MFDS (and the regions) can then make use of one (or more) of these security managers.

The ESM definition includes configuration details appropriate to the specific repository that the particular configuration is for – e.g. Active Directory or LDAP for the MLDAP_ESM type.

Security Managers and the Security Manager List

Once a Security Manager has been defined/configured, it can be used in the 'Security Manager List' and this can be for a particular region or for MFDS or it can be set in the 'Default ES Security' tab – in the latter case, the default ES Security can then be used for any (or all) regions and/or for MFDS.

MLDAP ESM Module

This is the module that enables LDAP repositories (e.g. Microsoft Active Directory – AD/LDS, or OpenLDAP for example on Unix) to be used with Enterprise Server.

The LDAP repository holds the users, groups and in particular the Micro Focus resources which can be used to control access to all aspects of Enterprise Server.

The configuration of an ESM entry using "mldap_esm" requires the username and password of an account that can connect to the LDAP repository.

It is sufficient to use an account that has only read access to the repository and this is recommended for production if this meets the customer's needs.

The following points should be considered when establishing whether a read-only account is sufficient to access the repository:

> The mldap_esm module needs at least read access to the objects that have been put into LDAP: the microfocus-MFDS-User objects, microfocus-MFDS-Group objects, and microfocus-MFDS-Resource objects.
>
> Some optional features, such as setting the last login time, will require write access to microfocus-MFDS-User objects.
>
> If MF-style passwords are being used, the Security Manager needs an account with write access to change passwords, update password history, etc.
>
> If it is required that user's should be able to change their passwords (e.g. from the CICS signon screen), a user with write (update) access to the repository will be required. (When a

user requests a password change the Authorized ID and Password specified in the Edit Security Manager screen are used, rather than the credentials of the actual user requesting the password change.)

If the MFDS administration console is to be used to change user groups and resource access rules in LDAP then the Authorized ID will again need 'update' access to those portions of the repository.

ESF Admin requests that change security data (anything other than listing security information) require write access.

If write/update access to the repository is required, then the account specified in the 'Authorized ID' field of the ESM configuration should be one that is allowed this access. By default when using AD/LDS only "read-only" and "administrator" access accounts are available, these would be accounts in the 'Readers' role or the 'Administrators' role respectively. With a full AD implementation much finer-grained permissions can be set. This is a matter for the customer's LDAP administrator.

The configuration settings in the ESM definition also specify the 'BASE' node in the repository where the Micro Focus LDAP attributes reside. By default this would be:

BASE=CN=Micro Focus,CN=Program Data,DC=local

Micro Focus or Active Directory Users

Part of the configuration of the mldap_esm module is to choose where the users are to be located. These can be Micro Focus users (e.g. SYSAD etc) or they can be Active Directory users (i.e. normal user accounts in the AD domain). In rare cases another LDAP object class might be used.

The 'user class' setting is used to specify which user 'type' is used and this would normally be either 'user' (i.e. Microsoft Active Directory users) or 'microfocus-MFDS-User' (Micro Focus user accounts).

Michael Wojcik: One or two customers have used other LDAP classes for users, such as the standard LDAP inetOrgPerson class.

In conjunction with this, the 'user container' setting would point at where these users are located in the Active Directory, so for 'microfocus-MFDS-User' users, the container would most likely be "CN=Enterprise Server Users", which is where the Micro Focus users will exist by default (after initially configuring the LDAP repository to work with Enterprise Server). If however 'user class' is 'user', then Microsoft users are to be used and so the 'user container' would be set someone outside of the Micro Focus node, e.g. "CN=ADAM Users" (for when AD/LDS on Windows is being used for example).

Also in conjunction with the above the 'Verify' method of authentication will typically change to reflect the type of user being used. For Microsoft (AD) users, typically 'mode=bind' would be used. In this case a 'bind' to Active Directory is done using the appropriate user credentials and the result used to govern the requested access.

When Micro Focus users are used this would be set to 'mode=mf-hash' (which is the default) where a hashing algorithm hashes the provided password to compare with that stored in the user's entry (in Enterprise Server Users in this case).

Example of using Micro Focus (Enterprise Server) users (the default):

```
[LDAP]
BASE=CN=Micro Focus,CN=Program Data,DC=local
user class=microfocus-MFDS-User
user container=CN=Enterprise Server Users
group container=CN=Enterprise Server User Groups
resource container=CN=Enterprise Server Resources
[Verify]
Mode=MF-hash
```

Example of using Microsoft (Active Directory) users:

```
[LDAP]
BASE=CN=Micro Focus,CN=Program Data,DC=local
user class=user
user container=CN=ADAM Users
group container=CN=Enterprise Server User Groups
resource container=CN=Enterprise Server Resources

[Verify]
mode=bind
password type=AD
```

Stacked ESMs and Federation

Multiple ESMs can be enabled for a region/MFDS. Where this is the case each ESM in the Security Manager list is interrogated in turn (in the order in which they exist in the list – which can be altered) to see if a security request can be satisfied.

When Federation is enabled, resources and rules in one ESM can be applied to other resources (users etc) in another ESM. All ESMs effectively act as though all the information was in one ESM.

When Federation is disabled, each ESM acts independently from the other so that rules from or in a specific ESM are the only ones that can apply to a user from or in that particular ESM.

References
Security Federation
Federation in the MLDAP ESM Module
Maxgroups setting

64/32 bit ESM security managers/modules

It is necessary to have the correct bitism for the region or MFDS that is going to use the security manager.

If the region is a 64-bit region, it will require a 64-bit security manager.

Similarly, the security manager used for MFDS must have the same bitism as MFDS.

If MFDS and the region have different bitisms, they cannot use the same ESM definition. They can however use the same security manager LDAP repository but 2 separate ESM definitions would be required – with essentially the same configuration details but one would use a 64bit 'provider' and the other a 32 bit provider.

Provider=*module*

ESM definition 1 (to be used with a 32 bit MFDS and any 32 bit regions):

```
[LDAP]
provider=/usr/lib/libldap_r-2.4.so.2.7.1
BASE=CN=Micro Focus,CN=Program Data,DC=local
user class=microfocus-MFDS-User
user container=CN=Enterprise Server Users
group container=CN=Enterprise Server User Groups
resource container=CN=Enterprise Server Resources

[Verify]
Mode=MF-hash
```

ESM definition 2 (to be used with a 64 bit MFDS and any 64 bit regions):

```
[LDAP]
provider=/usr/lib64/libldap-2.4.so.2.7.1
BASE=CN=Micro Focus,CN=Program Data,DC=local
user class=microfocus-MFDS-User
user container=CN=Enterprise Server Users
group container=CN=Enterprise Server User Groups
resource container=CN=Enterprise Server Resources
```

```
[Verify]
Mode=MF-hash
```

MFDS Security

Restrict Admin Access

- In order to prevent unauthorised access to MFDS, the 'Restrict Administration Access' checkbox can be checked (in the 'MF Directory Server' tab). Once this is enabled, a user will have to log on before access to the MFDS pages is granted.
- The account that can be used to restrict this access (and hence subsequently logon) has to exist in the security repository that has been configured for use by MFDS. The default 'SYSAD' account has the required permissions. E.G. A member of the #DSAdmin group.
- In addition, this account will have to have the relevant resource access rights. It can be configured (restricted) so that only some of the MFDS/administration actions can be performed by a specific user. E.G. to prevent management of user accounts and groups, deny access to "User Administration" in the 'Enterprise Server Administration' resource.

The 'Use default ES Security Manager List' option

- This checkbox exists both in MFDS and in the Region's Security tab.
- By checking this box, the default ES Security manager will be used (e.g. by a region).
- The actual ESM that is used is set in the 'default ES Security' tab

Default ES Security Options

Verify against all Security Managers

- Causes all security managers in the list to be queried, regardless of whether the request could already have been satisfied. The default is to stop querying once the request is initially satisfied (where the security managers are queried in the pre-set order).

Allow unknown resources

- This allows access to resources that are not explicitly 'allowed' or 'denied', in which case a result of 'unknown' will be returned.

Allow unknown users

- Allows unknown users to log in

Use all groups

- This is required when access to a resource is provided by membership of a group other than the user's signon group (which would normally be their default group). When this

option is selected, all the groups that a user is also a member of will be checked for resource access rules as well as their default/signon group. This implementation is similar to the equivalent option in RACF on the Mainframe.
If 'Use All Groups' is not checked, the user can specify another group (that they are a member of) to be their signon group at CICS login time. When 'Use All Groups' is checked, the signon group/field has no effect and the signon group will be their default group.
Reference

03 Securing a Region for Access and Resources

Which Security Manager to use?

In order for a region to be 'secured' it has to be configured to use a security manager (ESM). This is done from the region's 'Security' tab. If the "Use default ES Security Manager configuration" option is checked (which is the default) then the security manager that the region will use will be whatever is set in the 'default ES Security' tab (in MFDS). When this option is unchecked, a particular security manager (ESM) can then be specified directly in the "Security Manager List" on that page. This allows a region to use a different security manager than other regions and in particular then allows the 'Security Manager Administration GUI' interface to be used to manage this particular security manager repository

ES Resources

Once a region has been secured using an ESM, resource access is controlled by Access Control Lists (ACLs) and Access Control Elements (ACEs) in those lists which are stored in the LDAP repository under 'Enterprise Server Resources'.
Third-party LDAP tools (e.g. ADSIedit, jXplorer) can be used to view and modify the Enterprise Server Resources and Users and Groups in the LDAP repository. When the LDAP repository was setup, it would have been populated with all the required resources for CICS, JES and IMS etc in ES (e.g. DATASET, TCICSTRN) and these resources will have been given default access for certain users and or to certain ES Groups that would have also been setup. It is outside the scope of this document to describe all these resources, however a specific user can be allowed or denied access to a resource (either directly or via its group membership) so that only certain users have access to specific transactions or other JES actions and operations for example.
Resource Classes used by Enterprise Server are described at the following link:
https://www.microfocus.com/documentation/enterprise-developer/ed40pu3/ED-VS2017/HHSACHESSA30.html

Starting and Stopping a Region

When a region has been configured to use an ESM, it is necessary to specify a username/password that is valid and appropriate to that ESM. The configuration information section in the ESM definition defines what type of user account is being used by this security manager and where the accounts exists in the LDAP repository, thus an account from this location must be used.
For example if 'Microsoft Users' have been configured and the location of these users specified as 'ADAM users', then a (Microsoft) user that exists under 'ADAM users' (in this example) must be used to start/stop the region.
If 'Microfocus Users' has been specified and the default location of 'Enterprise Server Users' is used, then a user under 'Enterprise Server Users' must be used (e.g. SYSAD).
In both cases the relevant user must be a member of the relevant Microfocus Group(s) or otherwise have access to the Microfocus Resources required to allow a region to be started and stopped (I.E. 'OPERCMDS').

Start on System Start and 'Automated Execution Control Enterprise Server Credentials'

If a region is configured to start when MFDS starts (e.g. at system startup), credentials need to be provided for that region to start successfully. The relevant username and password would be provided in the 'Security' tab in the "Automated Execution Control Enterprise Server Credentials" section. The password is obscured.

04 Securing Applications

Application Security:
By default, an application running in an enterprise server instance has the access permissions of the (login) ID that started the session under which it is running. Thus the user that is running all the processes that form the region (cassi etc) will be the user under which any application code will run – this in turn potentially gives that application access to resources etc in the OS.
The way a region is started determines under which user it runs.
If the 'casstart' command is used to start a region from the command line, all the region's processes will run under the user who issued the casstart command (typically this will be the user who has logged on and has opened a command prompt or terminal session to run the casstart command).
If the 'Start' button in the MFDS GUI is used to start the region, then it is MFDS that is deemed to have started the region processes.

On **Windows**, all the region processes will run under the account that MFDS is configured to run under (which is set in the Windows services entry and is the Local System Account by default).

On **UNIX** it is generally recommended that mfds runs under root, however so that regions don't run as root, a 'normal' user should be configured for the region's processes to run under. This user is configured in MFDS in the following location:

> Options -> General: "Default process user ID",
>
> This would normally be done at installation time but can be altered after the product is installed.
>
> When the start button is used to start a region, this 'Default process user ID' will be used to run the region (and hence all the processes).
>
> Note that it is possible to run mfds as a non-root user in which case all region processes will run under the user that has been used to start mfds when the start button is pressed. (It is not possible to change to the Default Process ID when MFDS is not running as root). One of the other restrictions of running mfds with a non-root user is that a non-reserved port must be used for mfds.

Note that this is concerned with operating system resources and not Micro Focus resources. You can configure security managers to control access to Enterprise Server applications and resources, regardless of the access level that the operating system allows.

05 Securing the OS

It is necessary to consider files that exist in the Operating System that relate to MFDS and Region security. It is important that these files are protected from unauthorised access and/or update. These files are concerned with the security of MFDS or of the regions.

MFDS files

These files are located in the 'MFDS' directory (%ProgramData%\Micro Focus\Enterprise Developer on Windows and in $COBDIR/etc on Unix).

MFDS repository

This is located in an 'mfds' sub-directory under the 'MFDS' directory as follows
%ProgramData%\Micro Focus\Enterprise Developer\MFDS
$COBDIR/etc/mfds
Included in these files are all the region configuration files.

mfdsacfg.xml

This particular file contains various MFDS settings including whether MFDS is secured (Restrict Admin Access) or not and the certificate and keyfile locations together with the keyfile password. It should be protected against unauthorised access and modification via the OS.
It is located as follows:
%ProgramData%\Micro Focus\Enterprise Developer\mfdsacfg.xml
$COBDIR/etc/mfdsacfg.xml

Server and Client configuration files

Mf-server.dat

This file can contain the passphrase (keyfile) required by a secured listener
%TXDIR%\bin\mf-server.dat
$COBDIR/etc/mf-server.dat

MF-client.dat

This file can contain the path to the root signing certificate (CARootcert.pem)
%TXDIR%\bin\mf-client.dat
$COBDIR/etc/mf-client.dat

Cciusers.dat

This file is no longer used.

Dfhdrdat

This is the Resource Definition File and can contain some security information. It is found as follows:
%TXDIR%\etc\cas\dfhdrdat
$COBDIR/etc/cas/dfhdrdat
As well as the file itself, there are some utility programs that access/update this file.
The utilities that can access and/or modify the existing dfhdrdat file require username and password for validation:
Caspcupg
Casrdtup
Casrdtex
(caspcrd simply creates a default dfhdrdat file and does not have any security protection.)

LDIF files

There are also 'ldif' format files (on Windows, *.ldf) that contain the ES users, groups and resources that would populate an LDAP security repository. These files contain the definitions of the different entities and the default passwords (in plain text).
%TXDIR%\bin\es_default_ldap_msuser.ldf

06 Maintaining the Security Repository

The ESF GUI interface

On a region's 'Security' tab, once a particular Security Manager has been added to the Security Manager List (i.e. the region is not using the default ES Security Manager) the option "Enable Security Manager Administration GUI" is available – selecting this (and specifying a port number) creates a new "ESF Administration GUI" listener (of type mfcs-esfadmin). When the region is next restarted, the new listener provides a GUI interface to manage and maintain the repository associated with this ESM. In order to login to the ESF GUI, the user must have access to the 'User Administration' Resource in 'Enterprise Server Administration'.
https://www.microfocus.com/documentation/enterprise-developer/ed40pu3/ED-VS2017/GUID-68104419-C4D5-4778-BC88-78506EC4DAE8.html
In order to secure this ESF GUI interface, its listener needs to be secured in the normal way, by checking "Secure Sockets Layer" and providing the certificate (srvcert.pem) and keyfile (srvkey.pem) locations. When the region is subsequently started, this listener will require the PEM Passphrase before it will start. The relevant passphrase for the keyfile can be entered into mf-server.dat for this listener so that it will then start automatically.
Note that since different regions can be configured to use different ESMs, each ESM (and hence repository) can be managed by its own GUI.

Using MFDS to view and modify Resources

When a security manager is in use by MFDS, it can be selected for 'Edit' (in the Security Managers tab) after which the 'Properties' button can be selected. This allows the users, groups and resources in the security repository to be viewed and modified (with limitations).
If MFDS is already secured for SSL/TLS, then this information will continue to be sent securely (encrypted) using the secure https MFDS port. In addition the 'Restrict Administration Access' option will have previously been checked (which is also necessary to be able to access the repository information via the Edit->Properties button).

07 Default Users and Groups

Initializing LDAP-based security usually involves importing a number of LDIF (LDAP Data Interchange Format) files. These files include LDAP schema changes, LDAP tree additions (container objects), and definitions for a number of users, groups, resource classes, and resource entities.

Default users

LDAP-based security is set up using the sample LDIF files, the following default users will be created as 'Micro Focus user objects' (i.e. microfocus-MFDS-User objects in LDAP).

Name	Comments
SYSAD	CAS administration, e.g. for starting/stopping a region
schemaadmin	MFDS administration
adddelete	limited MFDS administration
modify	limited MFDS administration
administrator	limited MFDS administration
mf_mdsa	used by non-secured servers for CAS to connect to MFDS
mf_dep	used by non-secured servers for web service / EJB deployment
mf_cs	used by non-secured servers for MFCS to connect to MFDS
mfuser	default ESMAC account (see below)
CICSUSER	standard default CICS user
IMSUSER	standard default IMS user
JESUSER	standard default JES user
PLTPISUR	default user for PLI PI
SAFU	sample user for demonstrating security
SAFUIMS	sample user for demonstrating security (for IMS)
FSVIEW	default Fileshare user

There are 4 default users that are used to access the different sub-systems in ES (when no security is enabled for example). The actual default user that is assigned can be set/changed using an environment variable in the region. The following environment variables control this (the default username is shown):

`ES_USR_DFLT_ESMAC=mfuser` (for ESMAC access)
`ES_USR_DFLT_CICS=CICSUSER` (for CICS access)
`ES_USR_DFLT_JES=JESUSER` (for JES access)
`ES_USR_DFLT_IMS=IMSUSER` (for IMS access)

With the above defaults set, when ESMAC is accessed for example, 'mfuser' will be deemed to be the user doing this. In order to prevent this and to require or force a login before ESMAC can be accessed for example, the default users can be disabled. Access to all PCT transactions will then be prevented (apart from IBM category 3 transactions which do not have any security checking).

If the account is disabled by assigning it to a non-existent name (e.g. "NOTEXIST"), there will be no access to transactions but the default account will remain in case the system needs to be reverted back.
https://www.microfocus.com/documentation/enterprise-developer/ed40pu3/ED-VS2017/HHSACHESSA34.html

More information on removing predefined users can also be found here:
https://www.microfocus.com/documentation/enterprise-developer/ed40pu3/ED-VS2017/HHSACHESSA64S019.html

Default groups

The normal LDAP setup process also creates a number of groups. Some of these are defined for use by CAS; the others are used by MFDS.

These groups can be renamed or removed, but take note of the resource access control entries (ACEs) in various resource security definitions that refer to them. The esfadmin listreferences command is one way to find references to a given group. For example:

```
esfadmin -a listreferences group=SYSADM
```

will find all the references to the SYSADM group, including users that belong to it and resource access rules that apply to it. (Additional options for esfadmin may be necessary, depending on your configuration.)

CAS default groups

Many of the CAS default groups exist primarily because they are also present in a typical mainframe RACF installation, and so customers (and customer applications) might expect to find them.

Name	Description	Comments
SYSADM	CAS system administrators	Granted access to many resources
DEVGROUP	developers	Default group for SAFU. Access to CEBR, CDBG, and CRUN transactions.
OPERATOR	operators	Default group for PLTPIUSR. Access to CWTO and other C* transactions and similar system-operator resources.

INTERCOM	users permitted inter-system communication	Access to CPMI and other resources related to ISC.
ALLUSER	all users	Includes all predefined users; new users are not automatically added to it. Default group for CICSUSER, etc. Access to some non-sensitive transactions such as CSGM and CMAP, samples such as ACCT, basic JES operations.
IVPGRP	IMS IVP group	Used by the IMS IVP sample configuration. Default group for SAFUIMS.

MFDS default groups

The MFDS default groups are based on the old MFDS Internal Security. They use names which are not valid on the mainframe, to avoid colliding with groups migrated from a customer's RACF configuration.

Name	Description	Comments
#AllUsrs	All MFDS users	All predefined MFDS users belong to this group
#Modify	MFDS users who can modify object attributes	Limited administrators: can modify but not add or delete objects in MFDS
#AddDel	MFDS users who can add and delete objects	Limited administrators: can modify/add/delete. mf_dep belongs to this group, as deployment involves adding new service and package objects.
#GAdmin	MFDS "general" administrators	Limited administrators: can do most things, but not everything #DSAdmin group can
#DSAdmin	MFDS "directory server" administrators	Full administrators. SYSAD and schemaadmin belong to this group.
#System	MFDS system users	Includes mf_mdsa, mf_dep, and mf_cs (see above)

To do: Clarify which permissions are required by each common MFDS operation.

08 Securing Communications

For the purposes of ES, "secure communications" generally means enabling TLS (formerly SSL) for one or more communications endpoints: MFCS listeners, standalone servers such as MFDS, CICS Web Interface servers, and clients such as Web Services proxies and cassub.

TLS is very complicated, but customers often treat it as a check-off item. Some areas of difficulty with TLS:

- Ensuring both the client and server are in fact attempting to use TLS..
- Configuring appropriate TLS versions and cipher suites.

- Managing certificates (the PKI problem).
- Managing private keys for servers, particularly making them available to servers at startup without leaving them vulnerable to attackers.
- Diagnosing connection failures or examining network traffic.

There are other ways of securing communications, such as VPNs, and in some cases customers may be better off investigating those approaches.

MFDS and TLS/SSL

In order to secure (encrypt) data passed between a browser and MFDS, MF Directory Server can be configured to encrypt its connections. This is done on the 'MF Directory Server' tab by selecting the "Use encrypted connections" and "Use custom server ID certificate" checkboxes.

See "Configuring the MF Directory Server to use TLS Protocols and Cipher Suites": https://www.microfocus.com/documentation/enterprise-developer/ed40pu3/ED-VS2017/GUID-C0F322C1-2CB9-4704-AF51-486A277480A1.html

Once this has been enabled, any attempt to connect to MFDS (e.g. on its non-secure listening port) will result in a redirection to the 'secure logon page' (i.e. the https address using the 'secure port' specified in the MF Directory Server tab).

MFCS Listeners and TLS/SSL

Normal MFCS listeners can be secured to use encrypted communications by checking the "Secure Sockets Layer" option and providing the certificate and keyfile locations.

When the region is restarted, the password can be entered to start the listener, or the password can be provided in the `mf-server.dat` file.

Securing other clients and servers with TLS/SSL

- CWI (and CICS Web Services)
    - https://www.microfocus.com/documentation/enterprise-developer/ed40pu3/ED-VS2017/GUID-6E93D998-D430-4616-A672-2BC1B5A7D7E4.html

Configuring a Listener's TLS Protocols and Cipher Suites

https://www.microfocus.com/documentation/enterprise-developer/ed40pu3/ED-VS2017/GUID-595A02D3-A919-4FAA-9A03-7C33BC122D09.html
Note this requires ED3.0+HF1. In previous versions while TLS can be enabled for listeners, the protocol versions and cipher suites cannot be configured.

Storing certificates and keys

ES keeps certificates and private keys in files. There are a number of file formats in use in the industry, and customers may have to determine what format they have, or convert between formats. Do not rely on certificate file extensions - they often don't mean anything.

Prior to version 4.0, ES essentially only supported PEM files. (It's possible some other types could be made to work but they were untested.) With the 4.0 release, ES supports a much wider variety of file formats. See the product documentation for details.

Some common certificate file formats

- Raw format (rarely seen): A binary dump of the certificate data as used internally in an implementation. Not portable.
- DER format: A certificate represented in ASN.1 using the Distinguished Encoding Rules. (ASN.1 is a nightmarish syntax for data representation, with various sets of "encoding rules" that specify how it's actually represented in bits.) This is a binary format which is the basis for most other certificate file formats. Most TLS implementations can either use DER data directly, or provide some sort of import or conversion utility.
- PEM format: Defined by the RFCs for Privacy-Enhanced Mail in the early 1990s. PEM was a secure email specification that never became popular, but its file formats are widely used in some applications, particularly ones that use OpenSSL. PEM format is DER, encoded with Base64 so it's plain ASCII, with distinctive header and footer lines like `----- BEGIN CERTIFICATE -----`. PEM has a number of advantages:
    - Multiple certificates (and keys) can appear in the same file, simply by concatenating them.
    - Files are easy to view and edit.
    - PEM files can contain a variety of types of objects, including e.g. encrypted private keys.
    - PEM data can be sent in email and other non-binary transports. You can safely cut and paste it.
    - You can put arbitrary text in PEM files; the parser ignores anything not between a header and footer line. So for example you can have a PEM file of certificates with a readable explanation of each certificate.

Because it's so useful, most applications don't support PEM.

- PKCS#7 format: Actually a generic format for encrypted messages, but most often used by CAs to send certificates to customers, and by Windows as a certificate import/export format. Windows usually uses the file extension `.p7b` for this.
- PKCS#8 format: Not a certificate format at all - used to hold private keys (generally encrypted). Sometimes people get confused and think they have a certificate in a PKCS#8 file.
- PKCS#10 format: Not a certificate but a "certificate signing request" (CSR). Sent to a CA to request a certificate.
- PKCS#12, aka PFX, format: A compound file format that can hold certificates, private keys, and arbitrary data, in a hierarchy; objects can be encrypted. Over-engineered and under-specified. PFX was a Microsoft invention, later standardized as PKCS#12. This format has a lot of flaws but is useful for holding both a certificate and its private key in a single file, for example. Browsers often support PKCS#12 for certificate import/export. `.p12` and `.pfx` are the commonly-used Windows file extension.
- Java keystore format: Of *course* Java had to have its own file format. Java keystores can hold certificates and private keys, and can be encrypted.

Note that many applications screw one or more of these up royally, even if they claim to support it; or they invent their own formats. z/OS RACF, for example, will happily export a certificate and private key as a PKCS#12 file, but then Base64-encoded it and put a PEM-style header and footer on it. The result looks like a PEM file, but isn't, and nothing else can parse it. You have to take it apart manually.

Also there are various non-file options for storing keys and certificates. The most common:

- Windows certificate stores. These are what you see if you run the Windows Certificate Manager MMC snap-in or similar tools.
- Other OS-specific key stores, such as Apple keyrings and RACF keyrings (same name, different but functionally similar technology).
- HSMs (Hardware Security Modules), TPMs (Trusted Platform Modules), smartcards, and similar hardware devices.

These introduce their own complications, which I won't go into here.

09 Command Line Utilities

- ESFadmin
    - This command can be used to interrogate or modify the security repository and uses the same configuration as per an ESM configuration entry in MFDS (to establish the correct 'node' in the LDAP repository and what 'users' are being used).
    - It is protected by the need to supply credentials before information can be accessed.

    - Two sets of credentials are required as follows:
        - a) ESF user (-u) the 'user class' and 'mode' settings in the ESM config determine where valid uses would be located in the LDAP repository.
            - (The default would be micro Focus User objects in Enterprise Server Users)
        - b) ESM user (-U) the user used to 'bind' to the ldap server (for example the same user as specified in the ESM configuration 'Authorized ID' field, e.g. CN=MFReader....)
    - Example of an esfadmin command (on Windows) showing the different users:
        - set ESFCMD=esfadmin -uSYSAD -pSYSAD -U"CN=MFReader,CN=ADAM Users,CN=Micro Focus,CN=Program Data,DC=local" -PMF_rdr1:read-only! -Sldap://localhost:50010 -a
        - %ESFCMD% listgroup group="#DSAdmin"
            - Note this assumes that the ES schema additions have been added to the default location in the LDAP repository (CN=Micro Focus,CN=Program Data,DC=local), and that the default 'Mode=MF-hash' is used for the [verify] option. If this is not the case then the '-c' option can be used to specify a configuration file, in which the [ldap] and [verify] parameters can be specified (this would be the same information as in the ESM configuration in MFDS)
- ESFupdate
    - This can be used to enforce an update of the group aspects of users and resources if these have changed. It is equivalent to the 'update all' button in MFDS.
    - It is protected by a user/password for accessing MFDS (for when MFDS is secured/restricted), i.e. credentials for an MFDS administrator if MFDS is to be updated.
    - Example of and esfupdate command on Window:
        - esfupdate -M -a modify -uSYSAD -pSYSAD -m localhost:86 -r CICSDEM1 group NewGroup

10 Caching

- Certain security-related operations can be cached (in the ESF) which may improve results/response times. The following topic explains what can be cached and some of the implications of enabling caching include when the information is refreshed.
- https://www.microfocus.com/documentation/enterprise-developer/ed40pu3/ED-VS2017/GUID-E83C3E4E-BA0C-454A-B803-73BA92D621C2.html

11 Security Auditing

In 3.0, syslog events are used to perform security auditing functions as per the following topic:
https://www.microfocus.com/documentation/enterprise-developer/ed40pu3/ED-VS2017/GUID-21A5B09C-9118-4B76-9B01-782F4E1CF739.html
xxx

12 Summary and Recommendations

This document has described the security features in Enterprise Server and provides sufficient information and detail such that External Security (using an LDAP repository) can be setup and configured to secure the ES installation.
Furthermore, information on securing the communications channels/listeners has been provided to ensure that passwords and other sensitive data are not sent in clear text.
The section on Operating System security provides sufficient knowledge regarding files in the OS that are critical to security so that these files can be protected from unauthorized access using OS utilities.
In summary, it is recommended that the following tasks are reviewed and actioned when securing an ES installation:

- Implement external security for MFDS and the Regions using a LDAP/openLDAP repository and an ES ESM
- Configure this ESM to use either 'Enterprise server Users' (microfocus-MFDS-User objects) or 'Microsoft/Active Directory' users as required
- Restrict administration access to MFDS (so that a login is required)
- Secure the MFDS communications channel
- Secure any listeners that will be passing sensitive data
- Modify the security attributes of the MFDS files (in the OS) so that no unauthorised uses can access or modify them
- Disable any default accounts that are no longer needed for the operation of ES

13 Glossary of Terms

ADAM – Active Directory Application Mode
AD/LDS – Active Directory/Lightweight Directory Services
Bitism – a 64bit or a 32 bit platform
CWI – CICS Web Interface
ES – Enterprise Server
ESF – Enterprise Security Facility
ESM – External Security Manager
ESMAC – Enterprise Server Management and Control
LDAP - Lightweight Directory Access Protocol
LDIF – LDAP Data Interchange Format
MFDS – Micro Focus Directory Server

OS – Operating System
PCT – Program Control Table
SSL – Secure Sockets Layer
TLS – Transport Layer Security