

# Visual COBOL / Enterprise Developer チュートリアル

## デフォルトセキュリティの構成

### 1. 目的

製品バージョン10.0以降をインストールすると、既に設定済の外部セキュリティマネージャー(以降 ESM と称す)が存在しないことを条件に、製品に含まれる VSAM ESM モジュールが提供するセキュリティ機能がデフォルトで有効になります。そのため、実行に関連するすべての操作において、有効な資格情報の認証が必要になります。

本チュートリアルでは Enterprise Developer を例に、この VSAM ESM 機能について説明します。

### 2. 前提

- 本チュートリアルで使用したマシン OS : Windows 11 Pro、Red Hat Enterprise Linux 9.4
- 使用するマシンに Visual COBOL または Enterprise Developer 11.0J がインストールされていること
- Enterprise Server Common Web Administration(以降 ESCWA と称す)、Micro Focus Directory Server(以降 MFDS と称す)、Enterprise Server インスタンスについて理解していること
- ESM について理解していること

### 3. 段階的なセキュリティの設定

ESM は、一番大きな単位である ESCWA、ESCWA で管理する MFDS、MFDS で管理する Enterprise Server インスタンスと、3段階で管理、適用することができます。矛盾が生じないように、同じ ESM を各段階に設定することを強く推奨します。

#### ESCWA のセキュリティ機能

接続方法; ホスト名または IP アドレス: 10086

表示方法; ESCWA メニュー [セキュリティ]



## MFSD のセキュリティ機能)

表示方法;ESCWA メニュー[オペレーション]⇒ナビゲーション[Directory Server]>[Default]⇒MFDS メニュー[セキュリティ]



## Enterprise Server インスタンスのセキュリティ機能)

表示方法;ESCWAメニュー[オペレーション]⇒ナビゲーション[Directory Server]>[Default]>[インスタンス名]⇒インスタンスメニュー[一般]>[セキュリティ]



## 4. デフォルトユーザーと初期パスワードの取得

VSAM ESM のデフォルトユーザーと、インストールごとに生成する8桁の初期パスワードは、製品内部に Secrets Vault として格納されています。これらを製品に付属する Visual COBOL または Enterprise Developer コマンドプロンプト から取得します。

### 実行コマンド)

```
mfsecretsadmin read microfocus/temp/admin
```

## Linux の例)

```
mfsecretsadmin read microfocus/temp/admin
{"mfUser": "SYSAD", "mfPassword": "FeoZmjxQ"}
```

## Windows の例)

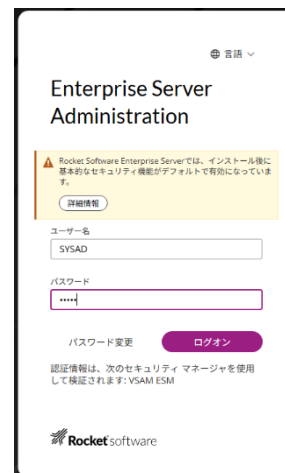
```
C:\> Enterprise Developer コマンドプロンプト (64-bit)
C:\Users\tarot\Documents>mfsecretsadmin read microfocus/temp/admin
{"mfUser": "SYSAD", "mfPassword": "64C4TK80"}
```

上記 Windows の場合、デフォルトユーザーは SYSAD、初期パスワードは 64C4TK80 です。  
この値を利用して各セキュリティ認証を行いますので、内容を記憶しておきます。

## 5. ESCWA ログイン

Web ブラウザーから ESCWA へ接続すると、  
ログイン認証を求められます。

デフォルトユーザーと初期パスワードを入力して[ログイン]、  
もしくは[パスワード変更]をクリックします。



本チュートリアルではデフォルトユーザーのパスワードを  
SYSAD に変更してログインします。  
変更したパスワードは利用者の責任で管理してください。

ユーザー名  
SYSAD

パスワード  
.....

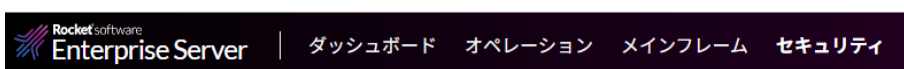
新しいパスワード\* ..... パスワードの確認\* .....

キャンセル **サブミット**

認証情報は、次のセキュリティ マネージャを使用して検証されます: VSAM ESM

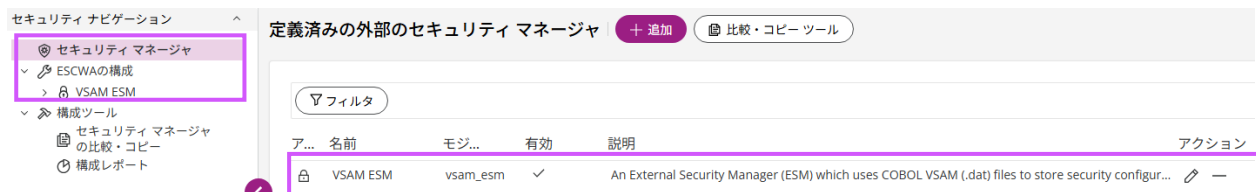
## 6. ESM の登録

ログインに成功すると ESCWA が表示されます。まずは登録されている ESM を確認します。  
上部の ESCWA メニューから[セキュリティ]をクリックします。



次に左側ペイン上部の[セキュリティナビゲーション]から[セキュリティマネージャ]を選択すると、ESCWA などに適用できる ESM 一覧が表示されます。この時点では[定義済みの外部のセキュリティマネージャ]には製品が提供する VSAM ESM が登録されていますが、他の ESM を登録したい場合は、[+ 追加]ボタンをクリックして接続内容を入力すると一覧に表示されます。内容を変更する場合には SYSAD ユーザーで認証を行ってください。

## ESCWA セキュリティ設定



[説明]に表示されているように、VSAM ESM はその名の通り、VSAM (\*.dat) ファイルにセキュリティ構成情報を保存する製品独自の ESM を指します。これらの VSAM ファイルは製品インストールフォルダまたはディレクトリにある etc フォルダまたはディレクトリ配下に保存されています。

## 7. ESCWA セキュリティの構成

左側ペイン上部の[セキュリティナビゲーション]から[ESCWA の構成]を選択すると、ESCWA に適用されている ESM 一覧が表示されます。この時点では[セキュリティマネージャリスト]には VSAM ESM が登録されていますが、他の ESM を適用したい場合は、[+ 追加]ボタンをクリックして適用可能な ESM を選択すると一覧に表示されます。内容を変更する場合には SYSAD ユーザーで認証を行ってください。

## ESCWA セキュリティ設定



ESCWA のセキュリティに ESM を適用すると、ESM に定義されているユーザー、グループ、リソースなどをメンテナンスすることができます。

## ユーザー設定)

セキュリティナビゲーション

- セキュリティ マネージャ
- ESCWA の構成
  - VSAM ESM
    - ユーザー**
    - グループ
    - リソース
    - リレーション
    - ロール
  - 構成ツール
    - セキュリティ マネージャの比較・コピー
    - 構成レポート

▼ フィルタ

ア...	アカウン...	名前	デフォルト ...	説明	アクション
		CICSUSER	ALLUSER	Default CICS User	 
		IMUSER	ALLUSER	Default IMS user	 
		JESUSER	ALLUSER	Default JCL user	 
		PLTPISUR	OPERATOR	CICS User for PLTPI	 
		RFAUSER	RFAUSER		 
		SAFU	DEVGROUP	Test security user	 
		SAFUIMS	IVPGRP	ES IMS User	 
		SYSADM	SYSADM	Administrator (added by mfseconv)	 

## リソース設定)

セキュリティナビゲーション

- セキュリティ マネージャ
- ESCWA の構成
  - VSAM ESM
    - ユーザー
    - グループ
    - リソース**
    - リレーション
    - ロール
  - 構成ツール
    - セキュリティ マネージャの比較・コピー
    - 構成レポート

セキュリティリソースナビゲーション

- JESJOBS
  - CANCEL.\*\*
  - SUBMIT.\*\*
  - JESSPOOL

▼ フィルタ

ア...	名前	説明	ACL	アクション
	CANCEL.**	Allow job cancellation for SYSADM and ALLUSER groups	ALLOW-SYSADM GROUP:alter;ALLOW-ALLUSER GROUP:alt...	 
	SUBMIT.**	No Limit on job Submissions by Jobname, Jobnumber, etc.	ALLOW-SYSADM GROUP:alter;ALLOW-ALLUSER GROUP:alt...	 

左側ペイン上部の[セキュリティナビゲーション]から[ESCWA の構成]>[VSAM ESM]>[リレーション]を選択して SYSAD が属するグループを確認します。右側ペインで[タイプ]にユーザーを、[名前]に[SYSAD]を選択後、[サブミット] ボタンをクリックしてリレーションを表示すると、すべてのグループに属していることがわかります。

## SYSAD ユーザーのリレーション)

セキュリティナビゲーション

- セキュリティ マネージャ
- ESCWA の構成
  - VSAM ESM
    - ユーザー
    - グループ
    - リソース
    - リレーション**
    - ロール

▼ フィルタ

ア...	名前	説明	ACL	アクション
	CANCEL.**	Allow job cancellation for SYSADM and ALLUSER groups	ALLOW-SYSADM GROUP:alter;ALLOW-ALLUSER GROUP:alt...	 
	SUBMIT.**	No Limit on job Submissions by Jobname, Jobnumber, etc.	ALLOW-SYSADM GROUP:alter;ALLOW-ALLUSER GROUP:alt...	 

© Rocket Software, Inc. or its affiliates 1990–2025. All rights reserved. Rocket and the Rocket Software logos are registered trademarks of Rocket Software, Inc. Other product and service names might be trademarks of Rocket Software or its affiliates.

5

一方、CICSUSER を確認すると2つのグループにのみ属していることがわかります。

### CICSUSER ユーザーのリレーション

リレーションの表示

タイプ

ユーザー

名前

CICSUSER


サブミット

ダウンロード

フィルタ

フィルタ テキスト

☐ ルール
 ☐ ACE
 ☒ グループ
 ☐ ユーザー



リレーションの表示では、[ユーザー]の他に[グループ]、[リソース]をタイプとして選択することができます。

次にリソースを確認してみます。左側ペイン上部の[セキュリティナビゲーション]から[ESCWA の構成]>[VSAM ESM]>[リソース]をクリックします。

左側ペイン下部に展開された[セキュリティリソースナビゲーション]>[Common Web Administration]>[Security Configuration]を選択して ESCWA のセキュリティ構成にかかわる権限を右側ペインの[リソースオプション(Security Configuration)]で確認すると、変更権限を持つのは#DSAdmin に属するユーザーのみとなっています。上記ユーザーの例では SYSAD は更新権限を持ち、CICSUSER は参照権限のみを持つことになります。

### リソースオプション

セキュリティ ナビゲーション

セキュリティ マネージャ

ESCWA の構成

VSAM ESM

ユーザー

グループ

リソース

リレーション

ロール

構成ツール

セキュリティ マネージャの比較・コピー

構成レポート

セキュリティ リソース ナビゲーション

Common Web Administration

Communications

Server Log

Configuration

Control

ESCWA Configuration

K8s Configuration

Logon

MFDS Configuration

Managed Access

Native Access

Scale-out Configuration

Security Access

Security Configuration

リソース オプション

\* クラスの新規作成

Security Configuration

適用

削除

\* 入力必須の項目です

名前

Security Configuration

説明

Allow access to security configuration properties for the Common Web Administration Server

ACL

ALLOW:\*:read;ALLOW:#DSAdmin GROUP:update,add,delete

- セキユティ・リソースナビゲーション
- > ACISCPCT
- > AdminAPI
- > CCMCDMD
- > CIMS
- > Common Web Administration
- > Communications Server
- > DATASET
- > DBCENTRY
- > DCBREFD
- > DICSICPCT
- > Enterprise Server Administration
- > Enterprise Server Web
- > FICSCFCT
- > FIMS
- > FIMS
- > FICJSCFCT
- > JESHPUT
- > JESJOB
- > JESSPOOL
- > LIMS
- > MICSFPCFCT
- > MPEMADAC
- > MQADMN
- > MQQCON
- > MQPRQC
- > MQMQQUE
- > QIM
- > OPERCMDS
- > PCICSP5B
- > PIMS
- > PICSRES
- > SCICSTST
- > SIMS
- > SURROGAT
- > Surrogate Services
- > TCISGTRN

## 8. MFDS セキュリティの構成

① **MFDS:定義済みの外部のセキュリティマネージャ**

MFDSに適用可能なESMの一覧が表示されます。VSAM ESMが表示されていない場合や他のESMを適用したい場合は以下の手順で追加することができます。既にVSAM ESMが表示されている場合は内容を確認します。

① MFDS:定義済みの外部のセキュリティマネージャ

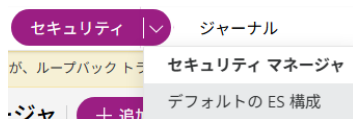
追加する ESM の内容)

### 外部のセキュリティ マネージャ構成

名前*	VSAM ESM	モジュール*	vsam_esm
<input checked="" type="checkbox"/> 有効			
接続パス			
認証ID			
パスワード	パスワードを入力してください		

## ② MFDS:デフォルトの ES 構成

MFDS が管理する Enterprise Server インスタンスに適用するデフォルトのセキュリティを設定します。MFDS メニューの[セキュリティ]>[デフォルトの ES 構成]を選択します。既に VSAM ESM がリストに表示されている場合は追加せずに、内容を確認します。



追加する場合は、右側ペインに表示された[セキュリティマネージャリスト]の[+追加]ボタンをクリックします。

### デフォルトの ES セキュリティ機能の構成

**適用**

\* 入力必須の項目です

☐ 全てのセキュリティ マネージャを検証 ☐ 不明なリソースを許可 ☐ 不明なユーザーを許可

☐ 監査イベントを作成する ☒ 全てのグループを使用

キャッシュTTL 0 秒      キャッシュ上限 0 kB

### セキュリティ マネージャ リスト

**+ 追加**   **定義の表示**

[定義済みの外部のセキュリティマネージャ]一覧には MFDS に適用できる選択肢が表示されます。

[VSAM ESM]にチェックして[選択]ボタンをクリックすると、デフォルトの ES セキュリティ機能として VSAM ESM が適用され、[セキュリティマネージャリスト]に表示されます。

### 定義済みの外部のセキュリティ マネージャ

VSAM ESM ×

フィルタ

☒ VSAM ESM



### セキュリティ マネージャ リスト

**+ 追加**   **定義の表示**

1 ✓ VSAM ESM

最後に画面上部の[適用]ボタンをクリックして ESM を適用します。ユーザー認証が求められる場合は、SYSADユーザーを使用して認証します。

### デフォルトの ES セキュリティ機能の構成

**適用**



### ③ MFDS:Directory Server の構成

MFDS 操作に関連するセキュリティ設定を行います。MFDS メニューの[セキュリティ]>[Directory Server の構成]を選択します。既に設定されている場合は内容を確認します。



ここでは前述で設定した[ES デフォルトセキュリティマネージャを使用]にチェックし、MFDS に適用する ESM を指定します。また、MFDS アクセス時にユーザー認証を求める場合は、[Directory Server アクセスを制限する]にチェックし、最後に画面上部の[適用]をクリックします。

Directory Serverのセキュリティ機能の構成 **適用**

\* 入力必須の項目です

☒ Directory Server アクセスを制限する ⓘ ☐ すべてのセキュリティ マネージャを検証 ⓘ ☐ 不明なリソースを許可 ⓘ

☐ 不明なユーザーを許可 ⓘ ☐ 監査イベントを作成する ⓘ ☒ すべてのグループを使用 ⓘ

☐ セキュリティ マネージャのプロパティが変更されたら更新する ⓘ

キャッシュTTL ⓘ  秒  秒

キャッシュ上限 ⓘ  kB

**セキュリティ マネージャ リスト**

☒ ES デフォルト セキュリティ マネージャを使用 ⓘ

+ 追加 ⓘ 定義の表示 ⓘ

セキュリティ設定の更新に伴い認証が求められますので、SYSAD ユーザーを使用して認証します。

#### 管理者ユーザーの認証情報の更新

セキュリティ構成が更新され、アクセスが制限されています。Enterprise Server Administration リソースクラスの「ユーザー管理」リソースの権限のある既存のIDとパスワードを指定する必要があります。

ユーザー名\*

SYSAD

パスワード\*

.....

\* 入力必須の項目です

**ログイン** 戻る

MFDS 操作に関するセキュリティマネージャリストに VSAM ESM が適用され、表示されます。

#### セキュリティ マネージャ リスト

☒ ES デフォルト セキュリティ マネージャを使用 ⓘ

+ 追加 ⓘ

定義の表示 ⓘ

1 ✓ VSAM ESM

MFDS アクセスに制限をかけることで、左側ペインに表示されている MFDS のアイコンが変化します。



## 9. Enterprise Server インスタンスセキュリティの構成

Enterprise Server インスタンスのセキュリティ設定を確認します。左側ペイン上部の[ナビゲーション]より、セキュリティを設定する Enterprise Server インスタンスを選択後、Enterprise Server インスタンスメニューの[一般]>[セキュリティ]を選択すると、右側ペインに[リージョンのセキュリティ機能の構成]が表示されます。ここでは VSAM ESM を追加する例を示しますが、既に適用されている場合は内容を確認します。



前項の MFDS セキュリティで[デフォルトの ES 構成]として設定した VSAM ESM を Enterprise Server インスタンスに適用します。

[デフォルトのセキュリティ機能の構成を使用]にチェックし、[適用]をクリックすると、[セキュリティマネージャリスト]には VSAM ESM が表示されます。



本チュートリアルでは[デフォルトのセキュリティ機能の構成を使用]を指定しますが、他の ESM を指定する場合にはこれにチェックをせずに、[+ 追加]ボタンをクリックし、一覧に表示されたESMから選択することで、個別に ESM を指定することもできます。

### [定義済みの外部のセキュリティマネージャ]の選択肢)

定義済みの外部のセキュリティ マネージャ すべてクリア

VSAM ESM
×

▼ フィルタ

✓ VSAM ESM

### デフォルト以外のセキュリティ使用時の一覧表示例)

	CICS2	Region	Stopped	✓	✓	デフォルト以外			
--	-------	--------	---------	---	---	---------	--	--	--

### デフォルトセキュリティ使用時の一覧表示例)

	CICS2	Region	Stopped	✓	✓	デフォルト			
--	-------	--------	---------	---	---	-------	--	--	--

前項からの設定例では、ESCWA、MFDS、Enterprise Server インスタンスには同じ VSAM ESM が設定されます。

## 10. Enterprise Server インスタンスセキュリティの除去

ESM を除去する場合は前項までの設定を遡り、小さい単位から大きい単位へと無効化していきます。VSAM ESM 以外の ESM を除去する際も後述の[デフォルトセキュリティの無効化コマンド]を除いて、同じ手順を踏みます。

### [デフォルトのセキュリティ機能の構成を使用]を指定していない場合)

セキュリティを無効化する Enterprise Server インスタンスを選択後、Enterprise Server インスタンスメニューの[一般]>[セキュリティ]を選択し、[リージョンのセキュリティ機能の構成]を表示します。

個別に指定した ESM が表示されている行の右端の除去アイコンをクリック後、[適用]をクリックします。

リージョンのセキュリティ機能の構成
適用

\* 入力必須の項目です

☐ デフォルトのセキュリティ機能の構成を使用

☐ 不明なリソースを許可

☐ 不明なユーザーを許可

☐ すべてのセキュリティ マネージャを検証

☒ すべてのグループを使用

☐ 監査イベントを作成する

キャッシュTTL

秒

キャッシュ上限

kB

**セキュリティ マネージャ リスト**

+ 追加
定義を表示

1	✓	VSAM ESM	
---	---	----------	--

一覧から削除されます。

## セキュリティ マネージャ リスト

[+ 追加](#) [定義の表示](#)

構成情報 ⓘ

[デフォルトのセキュリティ機能の構成を使用]を指定している場合)

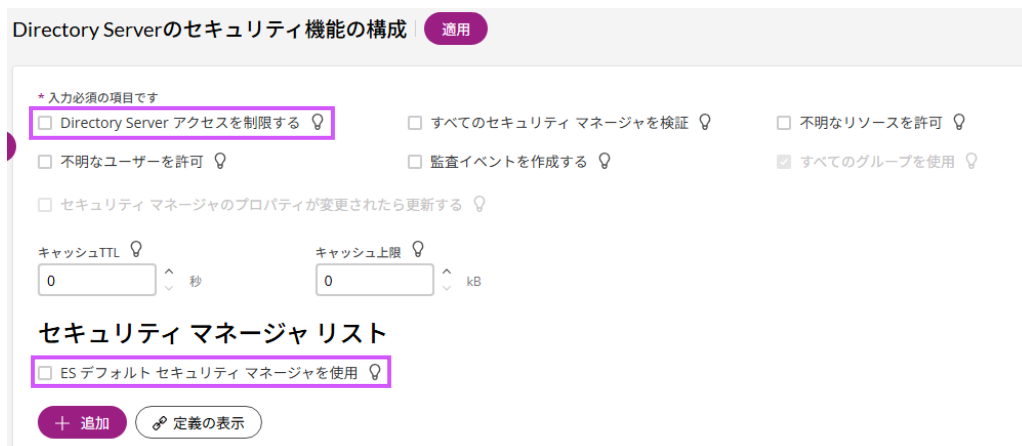
この除去を実施する必要はありません。

## 11. MFDS セキュリティの除去

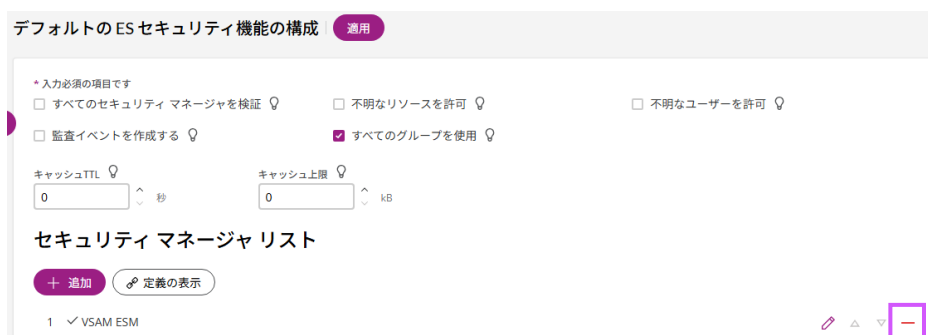
ESCWA メニューから[オペレーション]をクリックした後、左側ペイン上部の[ナビゲーション]より[Directory Server] > [Default]をクリックして MFDS メニューを表示します。



MFDS メニューの[セキュリティ] > [Directory Server の構成]を選択し、[Directory Server アクセスを制限する]と [ES デフォルトセキュリティマネージャを使用]からチェックを外した後、画面上部の[適用]をクリックします。



次に、MFDS メニューの[セキュリティ] > [デフォルトの ES 構成]を選択し、VSAM ESMが表示されている行の右端の除去アイコンをクリック後、[適用]をクリックすると、[セキュリティマネージャリスト]から VSAM ESM が削除されます。



Enterprise Server インスタンスに[デフォルトのセキュリティ機能の構成を使用]を指定した場合は、MFDS の[デフォルトの ES セキュリティ機能の構成]から VSAM ESM を除去した時点で、下記の画像のように Enterprise Server インスタンスからも除去されます。

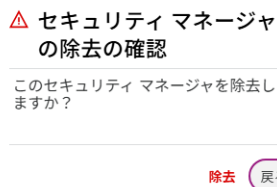
## Enterprise Server インスタンスのセキュリティ設定



MFDS メニューの[セキュリティ]を再度クリックして、[定義済みの外部のセキュリティマネージャ]に表示されている VSAM ESM 行の除去アイコンをクリックします。



確認メッセージが表示されますので、[除去]をクリックします。

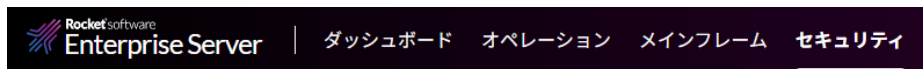


一覧から削除されます。



## 12. ESCWA セキュリティの除去

[ESCWA セキュリティ機能の構成]から VSAM ESM を除去します。ESCWA メニューの[セキュリティ]をクリックします。



左側ペイン上部の[セキュリティナビゲーション]より[ESCWA の構成]を選択し、右側ペインの[ESCWA セキュリティ機能の構成]に表示された VSAM ESM 行の[除去]アイコンをクリックします。



画面上部の[適用]をクリックすると、セキュリティ設定の更新に伴い認証が求められますので、SYSAD ユーザーを使用して認証します。

### 現行の管理者ユーザーの認証情報

セキュリティ構成が更新中です。ユーザーIDとパスワードを再入力してください。

ユーザー名\*

SYSAD

パスワード\*

\*\*\*\*\*

\* 入力必須の項目です

[ログオン](#) [戻る](#)

セキュリティマネージャリストから除去されます。

### セキュリティ マネージャ リスト

[+ 追加](#) [定義の表示](#)

構成情報 

最後に、デフォルトセキュリティの無効化を各種設定ファイルに反映します。

製品に含まれている Visual COBOL または Enterprise Developer コマンドプロンプトを起動し、次のコマンドを実行します。コマンドは、Linux/UNIX では製品インストールパスにある commonwebadmin.json などのファイルを変更する権限を、Windows ではサービスの停止と開始を行う権限を持つユーザーで実行してください。

### Linux/UNIX の実行コマンド)

DisableESDefaultSecurity.sh

#### セキュリティ除去後の Linux/UNIX の実行例)

```
#DisableESDefaultSecurity.sh
Rocket Software DisableESDefaultSecurity utility: Version 1.0.0

MFDS is not using ES Default Security.
ESCWA is not using ES Default Security.
No changes made.
```

### Windows の実行コマンド)

DisableESDefaultSecurity.cmd

#### セキュリティ有効時の Windows の実行例)

```
C:\Users\%tarot%\Documents>DisableESDefaultSecurity.cmd
Rocket Software DisableESDefaultSecurity utility: Version 1.0.1

MFDS is using ES Default Security, attempting to disable.
MFDS mfdscfg.xml backup file created C:\ProgramData\Micro Focus\Enterprise Developer\20260109174809_mfdscfg.xml
MFDS esm.dat backup file created C:\ProgramData\Micro Focus\Enterprise Developer\20260109174809_des_esm.dat
MFDS is no longer using ES Default Security.
ESCWA is using ES Default Security, attempting to disable.
ESCWA commonwebadmin.json backup file created C:\ProgramData\Micro Focus\Enterprise Developer\20260109174809_commonwebadmin.json
ESCWA is no longer using ES Default Security.
Backed up secret "microfocus#temp#admin" to "microfocus#temp#admin.disabled".
Backed up secret "microfocus#common#readonly" to "microfocus#common#readonly.disabled".
```

構成の変更を反映させるために、ESCWA および MFDS を再起動します。

## 13. ESM の除去

ESCWA、MFDS、Enterprise Server インスタンスに適用できる ESM の登録を除去したい場合は、ESCWA メニューの [セキュリティ] をクリックし、左側ペイン上部の [セキュリティナビゲーション] より [セキュリティマネージャ] を選択します。右側ペインの [定義済みの外部のセキュリティマネージャ] に表示された ESM 行の [除去] アイコンをクリックします。



画面上部の[適用]をクリックすると、確認メッセージが表示されますので、[除去]をクリックします。

### △ セキュリティ マネージャ の除去の確認

このセキュリティ マネージャを除去しますか？

除去

戻る

ESM が除去されます。

定義済みの外部のセキュリティ マネージャ

+ 追加

🔍 比較・コピー ツール

🔍 フィルタ

ア...	名前	モジュ...	有効	説明	アクション
------	----	--------	----	----	-------

## 14. 免責事項

本チュートリアルは機能説明を目的としており、無謬性を保証するものではありません。本チュートリアルに関わる全てを対象として、二次的著作物に引用する場合は著作権法に基づき適切な扱いを行ってください。

本チュートリアルで学習した技術の詳細については製品マニュアルをご参照ください。