User Management User Guide

Kinetic - Edge & Fog Processing Module (EFM) 1.7.0

Revised: July 18, 2019

Table of Contents

Introduction

The User management is a component that allows managing users, groups, permissions and roles for the EFM Web based components EFM System Administrator, EFM System Monitor, EFM Dataflow Editor, EFM Manager and the User Management itself. Not only does the User Management system authenticate, but through the use of roles, it authorizes the specific use of the EFM applications and rights. In this manner it is possible to define administrators, developers and operators with access to different applications based upon their functions.

The User Management system comes configured as a standalone environment using a local database, but it can allow the integration of a variety of external federated systems such as LDAP and Active Directory to provide Single Sign On functionality for EFM.

This guide helps you get started with EFM User Management system. It covers server configuration, user and roles as well as backup and restoration processes. Advanced deployment options are not covered. For additional configuration details, refer to the Additional References section.

User Management overview

The user interface of the Kinetic–EFM User Management starts with the login page. This is the same for all applications and provide a single sign on once authenticated.

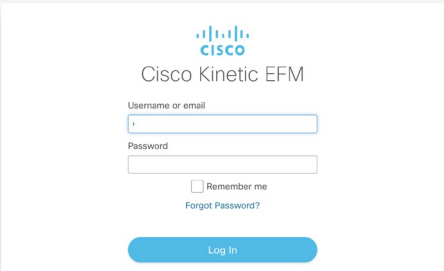

Figure 1. Cisco Kinetic EFM Single Sign-On Login

At first time use, the user credentials are those defined at installation. Once the user name and password are introduced, the EFM applications menu will appear. By selecting User Management, we will enter the specific application for identity and authentication management.

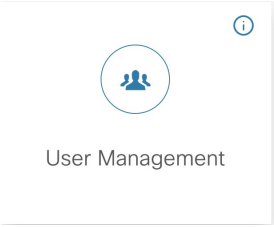

Figure 2. EFM User Management landing page selection

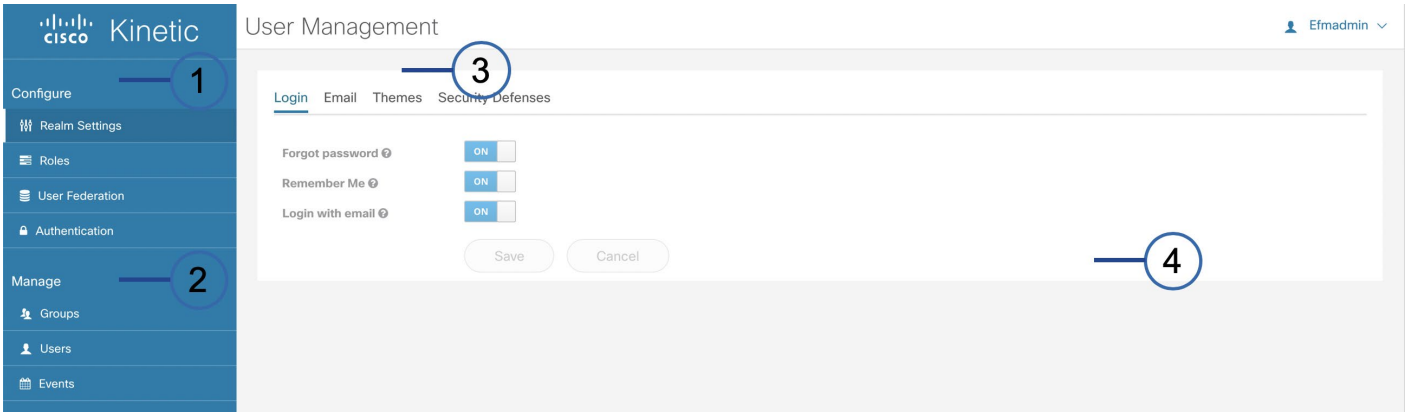

Figure 3. User Management Window

1	Configure tasks	**2**	Manage tasks
3	Task header (if any)	**4**	Task input fields

The user management system is divided into two major headers. Each section also has options below that are specific to a function.

1. **Configure** – General server configuration and operation. This section is prepopulated for the EFM applications.
2. **Manage** – Detailed management of groups, users and logging information.

Configure Actions

General server configuration and operation.

Realm Settings

This feature defines general user management realm settings and has the following tabs:

- Login
    - Forget Password – Show a link on the login page to click on when they have forgotten their credentials. Prerequisites: Follow instruction given in Email configuration tab to setup email correctly. Ensure that "Forgot password" switch is set to On in Realm Settings/ Login Tab. Also ensure that email ID is set for user whose password requires a reset.
    - Remember Me – Show check box on login page to allow user to remain logged in between browser restarts until session expires.
    - Login with email – Allow users to login with their email address. Prerequisites: Ensure that the Login with email switch is On in Realm Settings/Login and that the user is available whose email ID is set.
- Email – Configuration of the SMTP email server. The following fields are used to define the server:
    - Host (mandatory) – SMTP host
    - Port – SMTP Port (default 25)
    - From Display Name – Display name for sender email address
    - From (mandatory) – Sender email address
    - Replay to Display Name – Display name for reply to email address
    - Reply to – Reply to email address
    - Envelope From – Sender envelope email address
    - Enable SSL – On/Off
    - Enable StartTLS – On/Off
    - Enable Authentication – On/Off
- Themes – User Management Admin Console Theme selection. Options are cisco_efm_theme (default) and keycloak.
- Security Defenses – Ability to define security defenses. The following fields are used for configuration of Brute Force Detection
    - Enabled – On/Off.

- Permanent Lockout – Lock the user permanently when the user exceeds maximum login failures.
- Max Login Failures – Number of failures before wait is triggered.
- Wait Increment – When a failure threshold has been met, defines how much time should the user be locked out.
- Quick Login Check Milliseconds – If a failure happens concurrently within the defined value, lock the user.
- Minimum Quick Login Wait – Length of time to wait for quick login failure.
- Max Wait – Maximum time for a user to be locked out.
- Failure Reset Time – Length of time to reset failure count.

Roles

This feature provides possibility to restrict the access of the user to various applications by using the Roles in the authentication server. The following are the roles which are available out of the box from the installation of the Product.

Realm Roles – List of all available roles that can be assigned, allows for editing and deletion.

Role Name	Role Description / Comment
:config	Role similar to: config in EFM
admin	Admin Role for the realm (This encompasses all roles defined below)
sys-has-user-management- access	Provides access to Admin Console
sys-has-efm-manager-access	Provides access to EFM Manager
sys-has-efm- admin-access	Provides access to EFM Admin
sys-has-efm- monitor-access	Provides access to EFM Monitor
sys-has-dataflow-access	Provides access to Dataflow Editor (This role along with: config or any other permission giving role will make sure to give required access to dataflow, else only dataflow can be viewed and no action could be taken on it)

Default Roles – Defines realm level roles that are assigned to new users.

User Federation

This feature provides support for external user databases. The configuration options that can be selected are:

- Kerberos
- LDAP

Adding a Kerberos provider

By selecting Kerberos, the Kerberos required settings page will appear. The following fields are defined, some being as mandatory:

Required Settings:

- Enabled (toggle) – On/Off. Enable/Disable this Kerberos provider. If disabled it will not be considered for queries and managed users will be disabled and read-only until the provider is enabled again.
- Console display name – name of the provider when linked
- Priority – Priority of the provider when doing a user lookup. Lowest first.
- Kerberos Realm (mandatory) – Name of Kerberos realm. For example, FOO.ORG.
- Server Principal (mandatory) – Full name of the sever for HTTP service, including the server and domain name. For example, HTTP/host.foo.org@foo.org.
- KeyTab (mandatory) – location of the Kerberos KeyTab file containing the credentials of the server principal. For example, /etc/krb5.keytab.
- Debug (toggle) – On/Off. Enable/disable debug logging to standard output for Kbr5LoginModule.
- Allow Password Authentication (toggle) – On/Off. Enable/disable the possibility of username/password authentication against Kerberos database.
- Update Profile First Login (toggle) – On/Off. Update profile on first login.

Cache Settings:

- Cache Policy – Cache policy for this storage provider. “DEFAULT” is whatever the default settings are for the global cache. “EVICT_DAILY” is the time of day every day that the cache will be invalidated. “EVICT_WEEKLY” is the day of the week and time the cache will be invalidated. “MAX-LIFESPAN” is the time in milliseconds that will be the lifespan of the cache entry.

Adding an LDAP provider

- By selecting LDAP, the LDAP required settings page will appear. The following fields are defined, some being as mandatory:

Required Settings:

- Enabled (toggle) – On/Off. Enable or disable this ldap provider. If disabled it will not be considered for queries and imported users will be disabled and read-only until the provider is enabled again.
- Console display name – name of the provider when linked
- Priority – Priority of the provider when doing a user lookup. Lowest first.
- Import Users – On/Off. If enabled, LDAP users will be imported into User Management DB and synced via the configured sync policies.
- Edit Mode – READ_ONLY is a read-only LDAP store. WRITABLE means data will be synced back to LDAP on demand. UNSYNCED means user data will be imported, but not synced back to LDAP.
- Sync Registrations – On/Off. If enabled, newly created users be created within the LDAP store.
- Vendor (mandatory) – LDAP vendor (provider)
- Username LDAP attribute (mandatory) – Name of LDAP attribute, which is mapped as the User Management username. For many LDAP server vendors, it can be "uid". For Active Directory it can be "sAMAccountName" or "cn". The attribute should be filled for all LDAP user records you want to import from LDAP to the User Management system.
- RDN LDAP attribute (mandatory) – Name of LDAP attribute, which is mapped as RDN (top attribute) of typical user DN. Usually it's the same as Username LDAP attribute, however it's not required. For example, Active Directory it's common to use "cn" as RDN attribute when username attribute might be "sAMAccountName".
- UUID LDAP attribute (mandatory) – Name of LDAP attribute, which is used as unique object identifier (UUID) for objects in LDAP. For many LDAP server vendors, it's "entryUUID" however some are different. For example, Active Directory it should be "objectGUID". If your LDAP server really doesn't support the notion of UUID, you can use any other attribute, which is supposed to be unique among LDAP users in the tree. For example, "uid" or "entryDN".
- User Object Classes (mandatory) – All values of LDAP objectClass attribute for users in LDAP separated by comma. For example, "inetOrgPerson, organizationalPerson". Newly created User Management users will be written to LDAP within all those object classes and existing LDAP user records are found just if they contain all those objects classed.
- Connection URL (mandatory) – Connection URL to your LDAP server.
- Users DN (mandatory) – Full DN of LDAP tree where your users are. It could be for example "ou=users,dc=com" assuming that your typical user will have DN like "uid=john,ou=users,dc=example,dc=com".
- Authentication Type (mandatory) – LDAP Authentication type. Right "none" (anonymous LDAP authentication) or "simple" (Bind credential + Bind password authentication) mechanisms are available.
- Bind DN (mandatory) – DN of LDAP admin, which will be used by the User Management to access LDAP server.

- Bind Credential (mandatory) – Password of LDAP admin.
- Custom User LDAP Filter – Additional LDAP filter for filtering searched users. Leave this empty if you don't need an additional filter. Make sure it starts with "(" and ends with ")".
- Search Scope – For one level, we search for users just in DN specified by User DNs. For subtree, we search in the whole of their subtree.
- Validate Password Policy – On/Off. If enabled, the User Management validates the password with the realm password policy before updating it.
- User Truststore SPI – Specifies whether LDAP connections will use the truststore SPI with the truststore configured in standalone.xml/domain.xml. "Always" means that it always uses it. "Never" means that it won't use it. "Only for ldaps" means it will use it if the connection URL uses ldaps. Note that even if standalone.xml/domain.xml is not configured, the default Java cacerts or certificate specified by "javax.net.ssl.trustStore" property will be used.
- Connection Pooling – On/Off. If enabled, the User Management uses connection pooling for accessing the LDAP server.
- Connection Timeout – LDAP connection timeout is in milliseconds.
- Read Timeout – LDAP Read timeout is in milliseconds. This timeout applies for LDAP read operations.
- Pagination – On/Off. If enabled, the LDAP server supports pagination.

Kerberos Integration Settings:

- Allows Kerberos authentication – On/Off. If enabled, uses HTTP authentication of users with SPNEGO/Kerberos tokens. That data about authenticated users will be provisioned from this LDAP server.
- Use Kerberos for password authentication – On/Off. If Enabled, uses Kerberos login to authenticate username/password against the Kerberos server instead of authenticating against LDAP server with Directory Service API.

Sync Settings:

- Batch Size – Count of LDAP users to be imported from the LDAP to User Management within a single transaction.
- Periodic Full Sync – On/Off. If enabled, uses periodic synchronization of LDAP users to User Management.
- Periodic Changed Users Sync – On/Off. If enabled, periodic synchronization of changed or newly created LDAP users to User Management.

Cache Settings:

- Cache Policy – Cache policy for this storage provider. "DEFAULT" is whatever the default settings are for the global cache. "EVICT_DAILY" is the time of day every day that the cache will be invalidated. "EVICT_WEEKLY" is the day of the week and time the cache will be invalidated. "MAX-LIFESPAN" is the time in milliseconds that will be the lifespan of the cache entry.

Authentication

This feature defines general user authentication management policy settings and has the following tabs.

- Required Actions
    - Configure OTP
    - Term and Conditions
    - Update Password
    - Update Profile
    - Verify Email
- Password Policy definitions (optional) – Minimum password length is defined, but allows for removal, updating or addition of other policies that include password expiration, hashing iterations, special characters, not recently used, uppercase characters, lowercase characters, password blacklist, regular expression, digits, not username and hashing algorithm.
- OTP Policy definition
    - OTP type – Time based/counter based. Time based is Time-Based One-Time Password. Counter based is One Time Password in which the server keeps a counter against the agent.
    - OTP Hash Algorithm – Hashing algorithm used to generate the OTP.
    - Number of Digits – Number of digits the OTP should have.
    - Look Ahead Windows – Defines how far ahead should the server look in the case that the token generator and server are out of time sync or counter sync.
    - OTP Token Period – Defines how many seconds should the OTP toke be valid.
    - Supported Applications – FreeOTP, Google Authenticator

Manage Actions

Groups

This feature allows for looking up and creating groups. It also allows for looking up and managing default groups.

Groups creation and editing allow for the following:

- Setting name of the group
- Realm role mapping
- Group members (See Users section to add members to a group)

Users

This feature allows for looking up users and updating credentials.

Adding a user

Select the Add User button and the following fields

- ID (system generated uinique ID)
- Username (mandatory) – unique for the user
- Email – user email
- First Name
- Last Name
- User enabled – On/Off. If enabled, the user it will be active
- Email verified – On/Off. If enabled, the user's email has been verified.
- Required user actions

Select **Save**. Check the message as Success on top.

Select the "Credentials" tab, and ensure the Temporary is ON (which indicates the user needs to change password on login).

- Introduce the new password and confirmation.

It is also possible to assign a new password by the administrator and turn off the Temporary toggle. Click " Reset password" and select " Change Password" button. Check for the success message as well. Upon first login, if Temproary password toggle is on, the new user will be required to change password before proceeding.

Select the "Role Mapping" tab,

- If the user needs access to one or more EFM applications, then select the specific role for that application. See the Roles section for more detail.

Select the “Groups” tab to add or remove the user from a group.

Select the “Sessions” to view a list of current session by the user.

Adding a user example:

1. Login with an Administrator user
2. Select the User Management card
3. Go to Users Tab and click Add user button
4. Specify username as " efmtest" , all the other fields need not be touched, Click save
5. Check the message as Success on top.
6. Open Credentials Tab and set password for the user. Make sure the Temporary is ON (which indicates the user needs to change password on login).
7. Click " Reset password" and select " Change Password" button. Check for the success message as well.
8. Go to Role mapping tab, select sys-has-dataflow-access from Available roles and click " Add selected" button. Check for Success message
9. Select Sign Out from top right after selecting the user.
10. Check the Login page is displayed.
11. Login with efmtest user and the temporary password created.
12. The Warning Message is shown " You need to change your password to activate your account." . Give a password and confirm the password
13. On the Landing Page, only Dataflow editor card must be shown and on clicking the card, the dataflow editor would be opened without any further logins
14. The user can just see the dataflow editor but cannot do any other activity than viewing the links and system attributes.
15. To give full access to the dataflow options login as admin
16. Assign " :config" role to user – " efmtest" with step as explained in point 8.
17. Save and logout
18. Login as efmtest again and open the dataflow card again.
19. The user now will have authority to restart server, assign variables, start links, etc.,

20. Repeat step 8 for the selected user to give access to different roles.

Events

Allow to view and configure logging of login events. Events allow for the following:

- Login events viewing and filtering.
- Admin events viewing and filtering.
- Config allows for clearing Login and Admin event history.

Backup and restore of EFM User Management

The vital information from Authentication server can be backed up and restored. There are shell scripts developed which takes backup and restore if required. The following is the Process by which it could be achieved.

Prerequisites: Installation of authentication server rpm and asset manager config rpm.

Backup

Stop authentication server if already running

```
service authentication-server stop
```

Execute the `data-backup.sh` script with the parameter as file name to be backed up to. For example:

```
/opt/cisco/kinetic/efm_authentication_server/bin/data-backup.sh data--test-backup.tar.gz
```

The extension of tar.gz will be appended by code if not provided in the parameter. If the file to be created already exists, the code will exit, and the existing file will not be modified.

Restore

Stop authentication server is already running - `service authentication-server stop`

Execute the script `data-restore.sh` with the parameter as file from which the restore should happen. For example:

```
/opt/cisco/kinetic/efm_authentication_server/bin/data-restore.sh data--test-backup.tar.gz
```

The Code will exit if the file does not exist.

The Code will create backup of data folder, if it already exists.

After restoring is completed, run the following script to update the required configuration with latest ID. Do not change any configuration when asked during script execution.

```
/opt/cisco/kinetic/efm_authentication_server/bin/configure_asset_manager.sh
```

References

The Cisco EFM User Management system uses the Keycloak system as a core component for identity and access management. For more information on full functionality and capabilities, more information can be found at https://www.keycloak.org/.

For more a more advanced configuration of the EFM User Management, also refer to the Keycloak documentation at https://www.keycloak.org/documentation.html .

Obtaining documentation and submitting a service request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.