opentext™

Open Enterprise Server 24.4
Unified Management Console
Administration Guide

January 2025

Legal Notice

Copyright 2022 - 2025 Open Text

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

Contents

About This Book 5

1 Overview of Unified Management Console 7

Consolidation of Management Consoles . . . 8
Web-Based Access . . . 8
UMC SDK (REST API) . . . 8
Highly Responsive UI/UX . . . 8
Simplified Workflows . . . 8
Secure Platform . . . 9
Hybrid Management . . . 9
New Core Build Ground Up . . . 9
Transition from iManager to UMC . . . 9

2 UMC Architecture 11

User Authentication . . . 11
Auto-Population of Tree Name . . . 12
Unified Management Server . . . 12
User Permissions . . . 12
- UMC Server . . . 12
- Storage Management . . . 12

UMC Agents . . . 13
UMC communication with eDirectory and UMC agents . . . 13
Database Servers . . . 13
- Management Activities via Web Console . . . 13
- Temporary User Tokens . . . 13
- User Profiles . . . 13
- eDirectory Tree Details . . . 14

UMC Ports . . . 14

3 Configuring and Upgrading UMC 17

Support Matrix for Managing OES Services . . . 17
Prerequisites . . . 18
Configuring UMC During OES Installation . . . 18
Configuring UMC Post OES Installation . . . 19
Installing and Configuring Identity Console . . . 19
- Error Message: “Login Error. Invalid Credentials” . . . 20

Upgrading UMC . . . 20

4 Accessing UMC 21

Login to UMC . . . 21
Home Page . . . 22

About This Book

The guide describes the architecture of Unified Management Console and how it is used to manage OES services.

- Chapter 1, “Overview of Unified Management Console,” on page 7
- Chapter 2, “UMC Architecture,” on page 11
- Chapter 3, “Configuring and Upgrading UMC,” on page 17
- Chapter 4, “Accessing UMC,” on page 21

Audience

This admin guide is intended for network administrators who are planning to use Unified Management Console (UMC) to manage the OES services.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the `comment on this topic` feature at the bottom of each page of the online documentation.

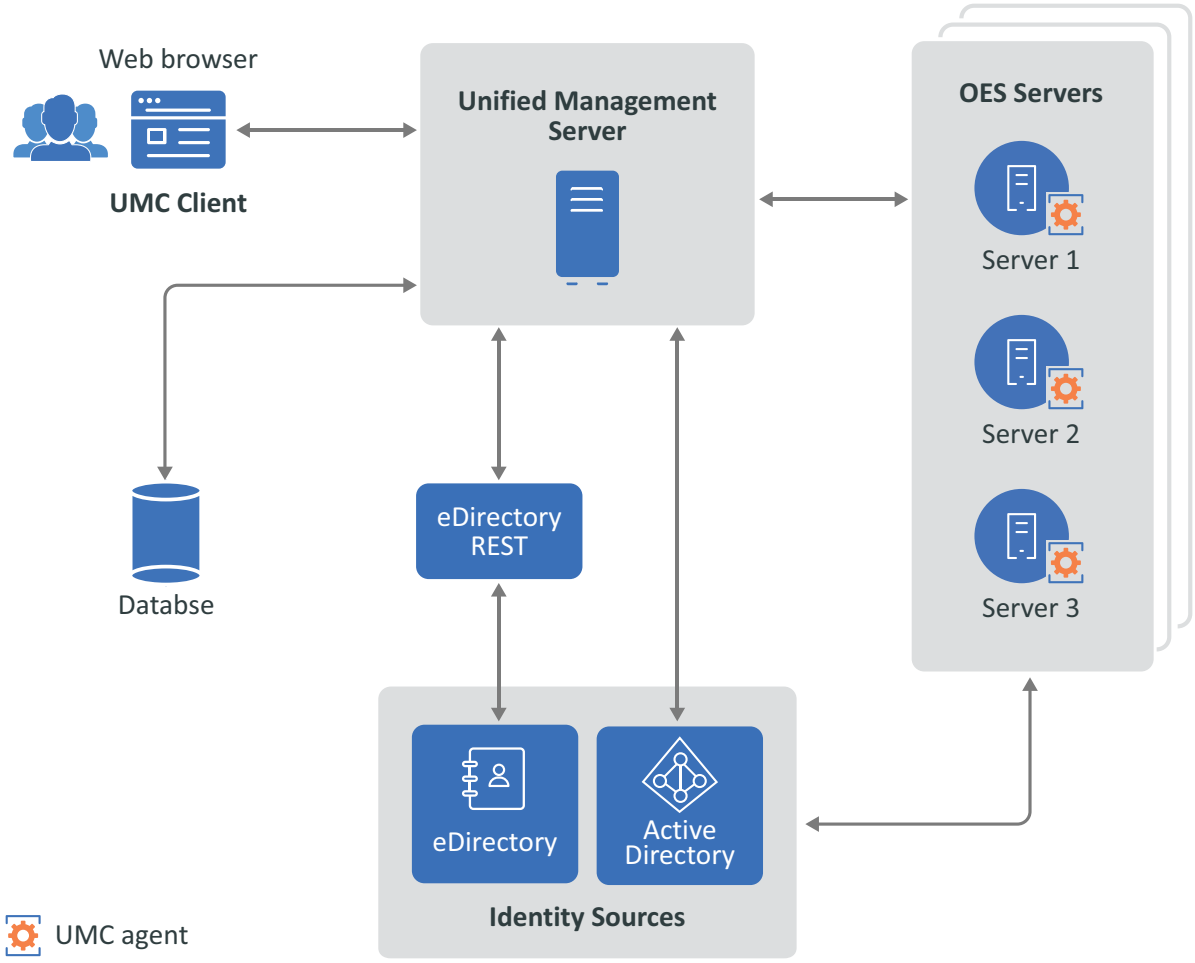
Additional Documentation

For more information about	See
Frequently asked questions on the tasks performed through the Unified Management Console	*Unified Management Console*
UMC REST APIs that can be customized for managing OES services	UMC Server API (https://www.microfocus.com/documentation/open-enterprise-server/24.4/resources/umc-server-api/)

1 Overview of Unified Management Console

The Unified Management Console (UMC) is a web-based remote management tool designed for both small and large OES deployments. Its completely overhauled user interface provides a seamless experience for managing multiple servers or clusters simultaneously. With comprehensive workflows, intuitive dashboards, and advanced operations, UMC ensures efficient and streamlined management of your entire system.

Figure 1-1 *UMC Overview*



The highlights of UMC are:

- “Consolidation of Management Consoles” on page 8
- “Web-Based Access” on page 8
- “UMC SDK (REST API)” on page 8
- “Highly Responsive UI/UX” on page 8
- “Simplified Workflows” on page 8

- "Secure Platform" on page 9
- "Hybrid Management" on page 9
- "New Core Build Ground Up" on page 9
- "Transition from iManager to UMC" on page 9

Consolidation of Management Consoles

UMC is designed to replace multiple existing management consoles, including iManager, iMonitor, and Remote Manager. This consolidation simplifies the management of OES services, making it more user-friendly.

Web-Based Access

Users can enjoy the convenience of accessing the management console from any web browser-enabled device, ensuring flexibility and ease of access. This feature empowers administrators to efficiently manage OES services from virtually anywhere. Moreover, it utilizes the standard HTTPS port (443), eliminating the requirement to open additional administrative ports for remote access. Best of all, there is no need to download or maintain a separate administrative client, streamlining the process even further.

UMC SDK (REST API)

The UMC SDK offers a range of REST APIs and examples for managing OES services. It enables your applications to interact with the client-based application by using UMC capabilities, including token generation for authorization and login to the UMC server. This SDK is designed for developers interested in creating new applications or integrating existing ones with the UMC's standards-based security architecture. For more information, see UMC Server API Documentation (https://www.microfocus.com/documentation/open-enterprise-server/24.4/resources/umc-server-api/).

Highly Responsive UI/UX

Built through strategic utilization of the Angular framework, leveraging its robust capabilities, in tandem with the thoughtful incorporation of UX Aspects, to ensure a highly tailored and user-centric development approach.

Simplified Workflows

The platform offers end-to-end workflows, enabling administrators to efficiently manage multiple servers simultaneously. It features a versatile dashboard that provides both basic and advanced analytics, giving users valuable insights into system performance.

Secure Platform

Provides comprehensive security through a token-based authentication system, supported by enhanced authentication methods. These measures work in synergy to ensure robust security protocols, safeguarding user access and data integrity while streamlining the authentication process for a seamless user experience.

The UMC environment utilizes public-key cryptography. If your company's security policy requires you to regenerate the security keys, there is no need to reconfigure UMC. The UMC server publishes the public key to all clients through an API with a static URL stored in the `umcConfig` object.

Hybrid Management

Utilize effective and efficient management capabilities for maintenance of file and print services, seamlessly supported by the robust eDirectory system. Manage files that have been meticulously integrated with the versatile Active Directory infrastructure.

New Core Build Ground Up

A centralized REST-based API server, which serves as a lightweight and efficient management service for OES servers. This integrated solution facilitates streamlined server management tasks, promoting efficiency and ease of use for system administrators.

Transition from iManager to UMC

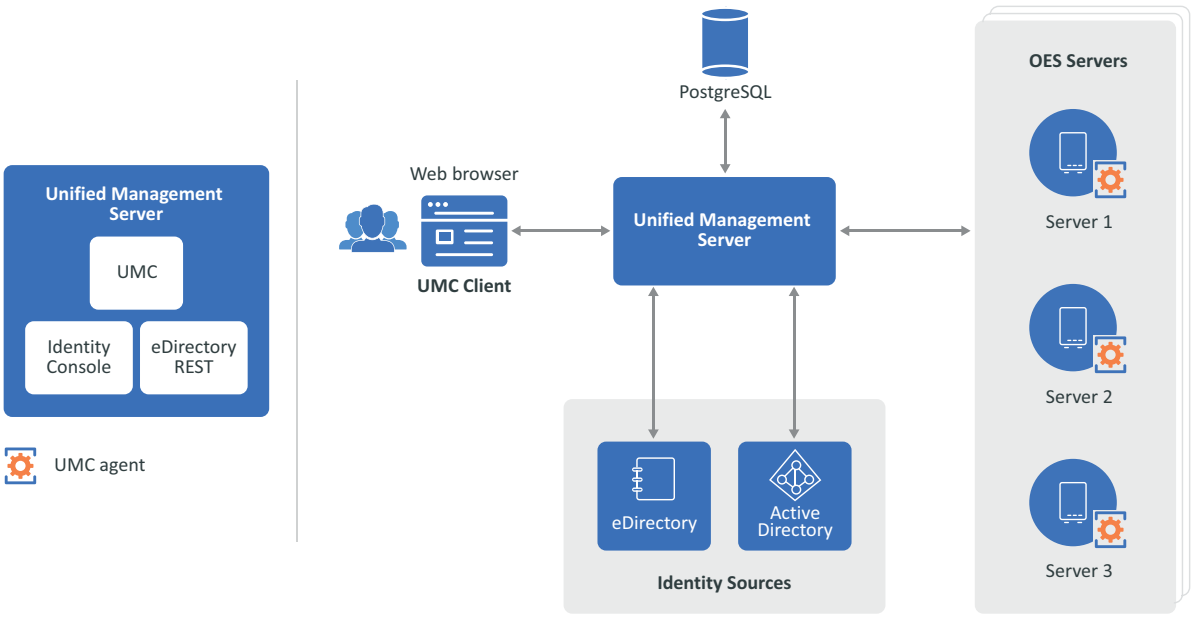
iManager has reached End Of Life (EOL) and comes with limited support for managing OES services. UMC is a replacement for iManager, which will manage all the OES services in the upcoming releases. For managing the directory services, we recommend you to use Identity Console.

2 UMC Architecture

This chapter describes the simple deployment and high-level architecture involved in the UMC environment.

- “User Authentication” on page 11
- “Auto-Population of Tree Name” on page 12
- “Unified Management Server” on page 12
- “User Permissions” on page 12
- “UMC Agents” on page 13
- “UMC communication with eDirectory and UMC agents” on page 13
- “Database Servers” on page 13
- “UMC Ports” on page 14

Figure 2-1 *Simple Deployment of UMC*



User Authentication

To access the UMC management console, users need to provide their credentials. This ensures that only authorized personnel can access and make changes to OES services.

Auto-Population of Tree Name

The management console simplifies the login process by automatically populating the tree name, which is derived from the eDirectory tree name specified during OES configuration. This feature streamlines the login process and reduces the chance of user error.

Unified Management Server

The Unified Management server is an OES server that is configured with UMC and Identity Console. Identity Console is bundled with UMC. The packages are installed automatically during the UMC installation and no separate installation is required.

For managing OES services and directory services, use the following:

- UMC to manage OES services

  To access UMC server, use `https://<umc_server_ip>/umc/`
- Identity Console to manage directory services

  To access Identity console, use `https://<umc_server_ip>:<eDir_api_port>/identityconsole/login.html`

User Permissions

UMC Server

The user permissions required to deploy UMC vary between the first and second instances of UMC.

- The first instance of UMC:

  You must have `Supervisor` rights or admin-equivalent tree-level rights to the tree root.
- Successive instances of UMC:

  You must have `Write` permission on the `All Attributes Rights` property of the `umcConfig` object under the security context.

Storage Management

- Logged-in users must have `Supervisor` rights on the NCP server object where the pools and volumes are mounted for storage management.
- The Compare, Read, and Write permissions on **All Attributes Rights** and Browse permission on **Entry Rights** are required at the tree level for the logged-in users to browse through the eDirectory tree.

UMC Agents

The OES servers hosting services, such as NSS, act as agents for the UMC server. When upgrading to OES 2023 or later, a UMC agent is automatically deployed on the server and must be active to perform management tasks.

The OES server auto-discovers the UMC server in the eDirectory tree and reads the `umcConfig` object in the security context to establish a connection with the UMC server.

UMC communication with eDirectory and UMC agents

- The UMC server and the eDirectory API server employ REST API authentication for users to login to the web console.
- Both the UMC server and UMC agents for OES utilize token-based authentication (OAuth2 with JWT) for the management of OES services (e.g., NSS). The tokens remain active (as per the set lifetime of the token) even if the UMC server restarts or undergoes upgrades.

Database Servers

Postgres is the default database used for UMC. The default port number is 5432 and can be modified.

The PostgreSQL database offers the following features:

- "Management Activities via Web Console" on page 13
- "Temporary User Tokens" on page 13
- "User Profiles" on page 13
- "eDirectory Tree Details" on page 14

Management Activities via Web Console

PostgreSQL stores data related to management activities performed through UMC. This data could include logs, user actions, configurations, and other information related to the management of the system.

Temporary User Tokens

Stores temporary user tokens, such as access tokens, refresh tokens, and CSRF tokens, for authentication and security purposes. These tokens are used to validate and authenticate users and protect against cross-site request forgery (CSRF) attacks.

User Profiles

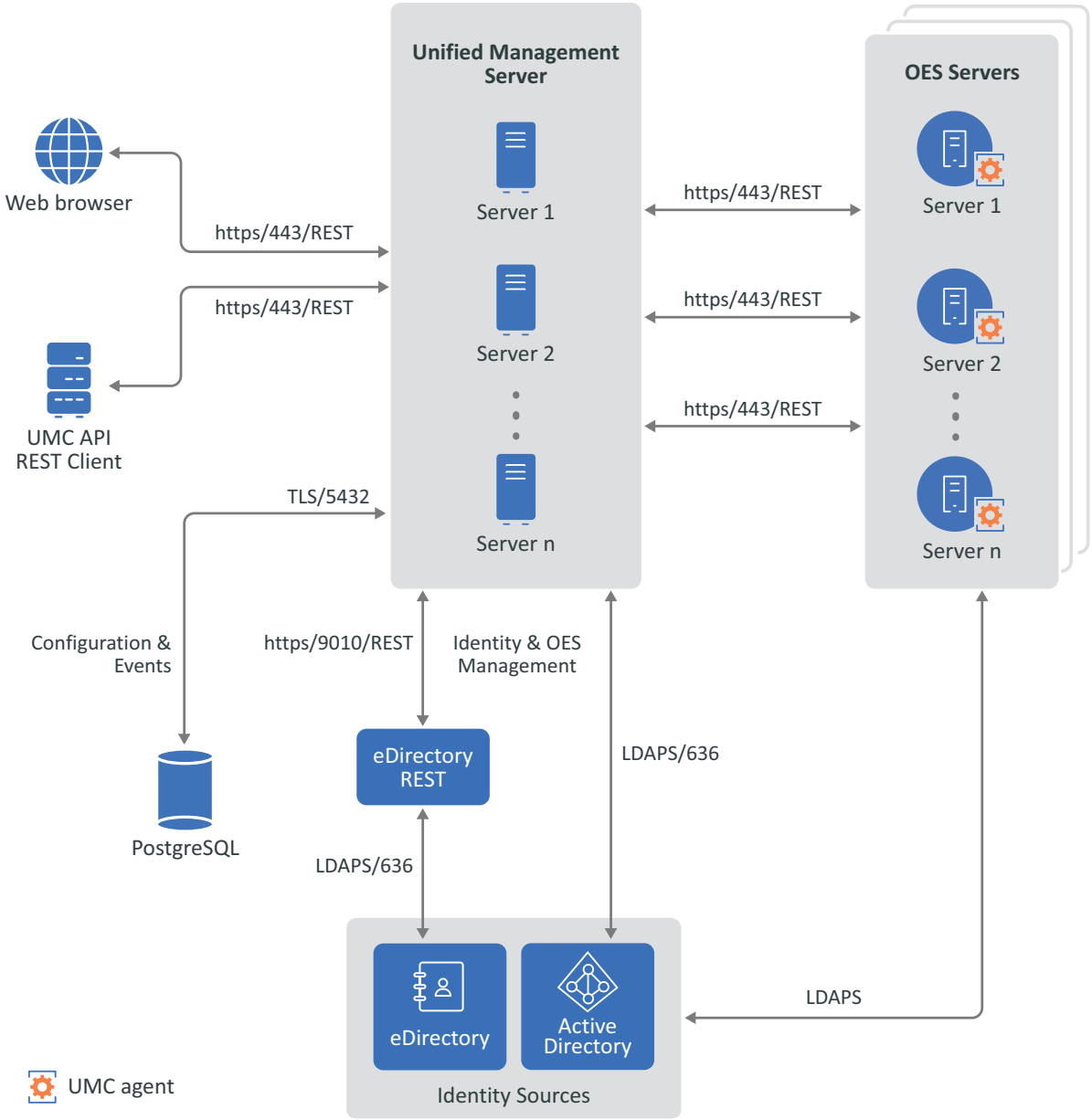
Stores user profiles to retrieve the browsing context and the set filters.

eDirectory Tree Details

The UMC console page is auto-populated with tree details as the information, including tree names and IP addresses, is stored in the database.

UMC Ports

Figure 2-2 *Port Diagram for UMC*



Tasks	Port	Description
Login	443	The UMC server can be accessed from any web browser-enabled device. Using the UMC REST APIs, you can create a customized interface to access the UMC server.
Manage OES services	443	The UMC server (OES or non-OES server) manages the OES services. **Load Balancer:** Multiple UMC servers can be deployed and configured to work in conjunction with a load balancer. This load-balancing configuration enhances the availability and reliability of OES services.
UMC Agents	443	The servers hosting OES services act as agents for the UMC server, managing the services.
Database	5432	PostgreSQL is the default database used for UMC, storing configuration details and events.
Identity Sources	9010 / 636	Identity and OES management are performed by the eDirectory REST server or the Active Directory server.

3 Configuring and Upgrading UMC

This chapter describes the procedure to configure and upgrade the Unified Management Console.

- “Support Matrix for Managing OES Services” on page 17
- “Prerequisites” on page 18
- “Configuring UMC During OES Installation” on page 18
- “Configuring UMC Post OES Installation” on page 19
- “Installing and Configuring Identity Console” on page 19
- “Upgrading UMC” on page 20

Support Matrix for Managing OES Services

Table 3-1 *UMC Supported Servers*

Services	OES 2023	OES 23.4	OES 24.1 OES 24.2	OES 24.3	OES 24.4	OES 24.4.1
BCC	NO	NO	NO	NO	NO	YES
LUM	NO	NO	NO	NO	NO	YES
SMDR	NO	NO	NO	NO	YES	YES
TSAFS	NO	NO	NO	NO	YES	YES
DFS (Move and Split jobs)	NO	NO	NO	NO	YES	YES
DFS (Replica and Junctions)	NO	NO	NO	YES	YES	YES
CIFS	NO	NO	NO	YES	YES	YES
NCP Connections	NO	NO	YES	YES	YES	YES
NCP Shares	NO	YES	YES	YES	YES	YES
Cluster	NO	YES	YES	YES	YES	YES
Files and Rights	YES (Update 4)	YES	YES	YES	YES	YES
Storage	YES	YES	YES	YES	YES	YES

Prerequisites

- Ensure to remove existing Identity Console before upgrade. For more information, see Uninstalling OpenText Identity Console (https://www.netiq.com/documentation/identity-console/identity_console-install/data/uninstall-identity-console.html) in Identity Console (https://www.netiq.com/documentation/identity-console/identity_console-install/data/bookinfo.html) documentation.

  NOTE: Manually installed standalone or docker Identity Console can cause port conflict issues.

- It is recommended to install UMC and Identity Console on the same OES server.
- Ensure that the OES server is a non-DSfW server.
- Open the following ports for UMC communication:
  - APACHE-443 (Secure HTTP)
  - OES-REST-3000
  - UMC-REST-3333
  - eDir API-9010 (default)
  - PostgreSQL DB-5432 (default)
- When installing the first instance of UMC, you must have `Supervisor` rights or admin-equivalent tree-level rights to the tree root.
- When installing successive instances of UMC, the administrator must have `Write` permissions on the `All Attributes Rights` property of the `umcConfig` object under the security context of the eDirectory.
- DNS name resolution of the IP address with hostname for the UMC server.
- UMC uses common proxy credentials for resolving contextless usernames. For example, anaya.opentext.com will be mentioned as “anaya” alone.

Configuring UMC During OES Installation

1. In the YaST install, on the **Installation Setting** page, click **Software** to go to the **Software Selections and System Tasks** page.

   For information about the entire install process, see Installing OES as a New Installation.
2. Select **OES Unified Management Console (UMC)** and click **OK**.

   NOTE: OES eDirectory and OES Database are automatically selected.
3. On the **Open Enterprise Server Configuration** page, click **OES Database**.
4. Specify database details and click **Next**.

   UMC ships with PostgreSQL as the default database. The default database port number is 5432 and can be modified if necessary.
5. On the **Open Enterprise Server Configuration** page, click **Unified Management Console**.
6. In the password box, enter the eDirectory admin’s password.

7 In the **OES Unified Management Console (UMC) Configuration**, specify the port for eDirectory API and click **Next**.

The default eDirectory API port is 9010 and can be modified if necessary.

8 On the **OES Configuration** page, click **Next** to start the configuration process.

After the successful configuration, click **Finish**.

NOTE: Use the command `yast2 umc` to configure UMC post UMC pattern installation.

To troubleshoot any issues, see UMC Health Script.

Configuring UMC Post OES Installation

1 In the console, run the command `yast2 oes-install` to display the Software Selection page.

2 Select the **OES Unified Management Console (UMC)** pattern, and click **Accept**.

NOTE: OES eDirectory and OES Database are automatically selected.

---

3 On the **Open Enterprise Server Configuration** page, click **OES Database**.

4 Specify database details and click **Next**.

UMC ships with PostgreSQL as the default database.

5 On the **Open Enterprise Server Configuration** page, click **Unified Management Console**.

6 In the password box, enter the eDirectory admin's password.

7 In the **OES Unified Management Console (UMC) Configuration**, specify the port for eDirectory API and click **Next**.

8 After the successful configuration, click **Finish**.

To troubleshoot any issues, see UMC Health Script.

Installing and Configuring Identity Console

Identity Console is used to administer eDirectory objects, users, schema, partitions, replicas, and rights on an OES server. Identity Console is deployed as a docker container.

To access Identity console, use `https://<umc_server_ip>:<eDir_api_port>/identityconsole/login.html`

Error Message: “Login Error. Invalid Credentials”

If you receive the error message “Login Error. Invalid Credentials,” and `/var/lib/docker/volumes/IDConsole-volume/_data/eDirAPI/var/log/edirapi` logs display “LDAP Result Code 49 Invalid Credentials: Hostname not valid.”, it indicates that the eDirectory IP address is not associated with Identity Console or included in the `edirapi.conf` file.

To resolve this issue, do the following:

1. Edit the `edirapi.conf` file located at `/var/lib/docker/volumes/IDConsole-volume/eDirAPI/etc/conf/`.
2. Modify the `edir-hosts` entry in the `edirapi.conf` file.
3. To restart the container, do the following:

   ```
   docker restart identityconsole-oes
   ```
4. Log in to the Identity Console using your credentials.

Upgrading UMC

After upgrading the OES server, UMC is automatically updated seamlessly without any additional tasks. UMC includes management of OES services and defect fixes.

4 Accessing UMC

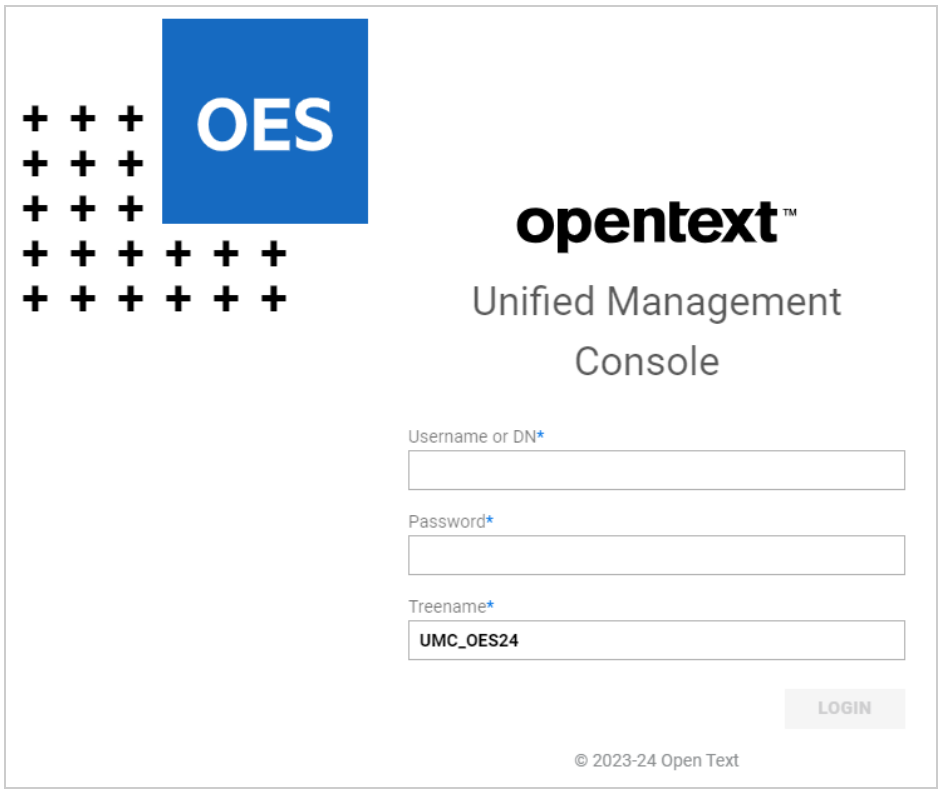
This chapter describes the UMC home page. For more information on administering OES services through the console, see Unified Management Console guide.

Login to UMC

1. Open any web browser and specify the UMC URL `https://<UMC_ServerIP/Hostname>/umc`.
2. Specify the username (CN or FQDN) and password.

   The tree name is auto-populated.

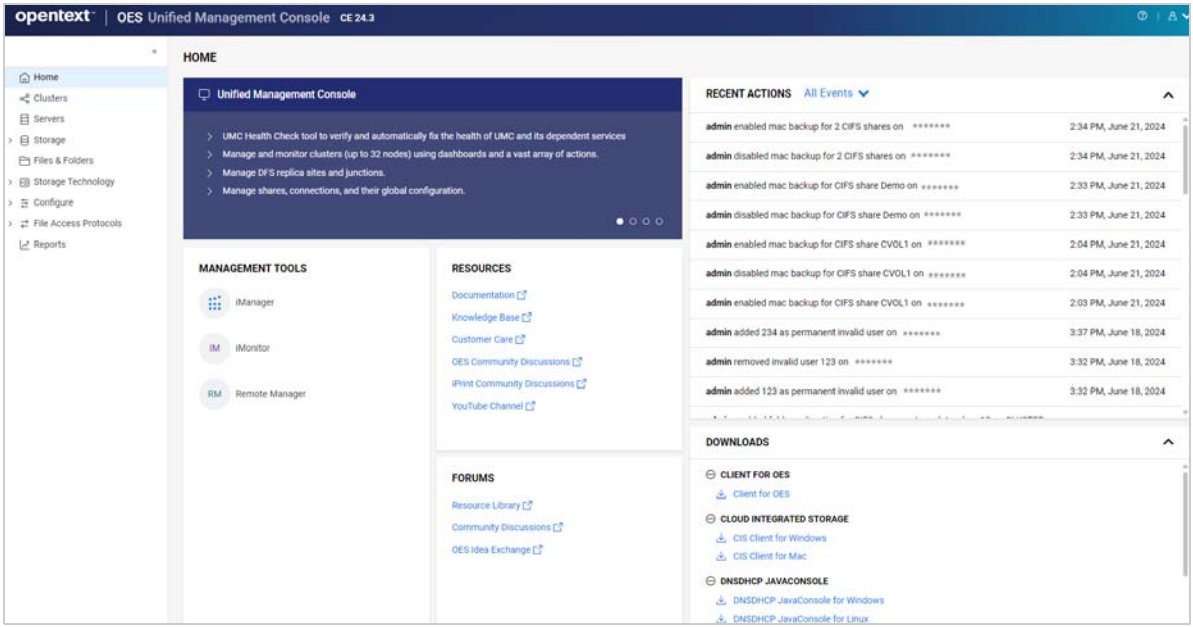
Figure 4-1 *Login Page*



After successful login, UMC Home page is displayed.

Home Page

Figure 4-2 *Home Page*



The UMC home page is the default landing page for all users.

- **Highlights** – Displays the high-level features of the release.
- Recent Actions – Displays a list of actions performed on the system by the logged-in user through UMC.
- Downloads – Contains the links to download the OES clients.
- Resources – Links to various resources such as documentation, knowledge base, YouTube channel, and so on.
- Forum – Links to Community discussions, resource library, and Idea forum.
- Management Tool – Links to various tools that are used to manage OES and its services. Click the tool to know more about it. These tools will be deprecated in the upcoming releases with UMC.

OES Services

- Cluster - Manage cluster and resources.
- BCC - Manage Business Continuity Clustering.
- Server - Modify OES server settings. Currently, only NCP server settings can be managed.
- Storage - Manage pools, volumes, pool snapshots, user quotas, partitions, software RAIDs, and devices.
- Files & Folders - Manage rights, quota on files and folders.
- Storage Technology - Manage DFS replica and junctions.
- File Access Protocols - Manage CIFS and NCP shares and connections on a server.
- Reports - Generate report for clusters.

- Users & Groups - Manage workstations, groups, users, and Linux configuration object.
- Identity Console - Launches Identity Console. Identity Console is used to administer eDirectory objects, users, schema, partitions, replicas, and rights on an OES server.