# MICRO FOCUS®

# Micro Focus Kanaka for Mac
# Version 3.2.1
## Installation and Administration Guide

**November 14, 2022**

## Third Party Systems

The software is designed to run in an environment containing third party elements meeting certain prerequisites. These may include operating systems, directory services, databases, and other components or technologies. See the accompanying prerequisites list for details.

The software may require a minimum version of these elements in order to function. Further, these elements may require appropriate configuration and resources such as computing, memory, storage, or bandwidth in order for the software to be able to perform in a way that meets the customer requirements. The download, installation, performance, upgrade, backup, troubleshooting, and management of these elements is the responsibility of the customer using the third party vendor's documentation and guidance.

Third party systems emulating any these elements must fully adhere to and support the appropriate APIs, standards, and protocols in order for the software to function. Support of the software in conjunction with such emulating third party elements is determined on a case-by-case basis and may change at any time.

# Contents

# About This Guide

This guide is written to provide network administrators the conceptual and procedural information for enabling Mac connectivity to Micro Focus Open Enterprise Server network storage resources through Micro Focus Kanaka for Mac.

## Audience

This guide is intended for network administrators who manage network client access to Micro Focus Open Enterprise Server storage resources in NetIQ eDirectory.

## Feedback

We want to hear your comments and suggestions about this guide. Please use the User Comments feature at the bottom of each page of the online documentation.

## Documentation Updates

For the most recent version of the *Micro Focus Kanaka for Mac Installation and Administration Guide*, visit the Micro Focus Kanaka for Mac Documentation Web site (http://www.novell.com/documentation/kanaka).

# 1 What's New

Version 3.2.1 of Micro Focus Kanaka for Mac is the latest version of a product that was first introduced in 2005. There have been enhancements with each new version of the product. An overview of some of the more recent changes in architecture, performance, features, and distribution follows:

- Section 1.1, "New in Version 3.2.1," on page 7
- Section 1.2, "New in Version 3.2," on page 7

## 1.1 New in Version 3.2.1

### macOS

Monterey (12) and Ventura (13) are supported via the Kanaka 3.2 Plug-in and Client. macOS versions earlier then BigSur (11) can use the older kanaka 3.1 Plug-in and Client.

### OES Support

Micro Focus Open Enterprise Server 2018 SP3 and 2023 are now supported.

**IMPORTANT:** OES 2023 does not support AFP directly, but if the configured storage server is running on an older OES version that does support AFP, Kanaka will still continue pass the configured AFP based path information to the Plug-in and Client.

## 1.2 New in Version 3.2

### macOS Version Support

BigSur (11) and Monterey (12) are supported via the Kanaka 3.2 Plug-in and Client. macOS versions earlier than Mojave (10.4) can use the Kanaka 3.0.1 Plug-in and Client.

### OES Support

Micro Focus Open Enterprise Server 2018 SP3 is supported.

Changes to macOS beginning in version 11 no longer allow network home directories for use with the Kanaka Plug-in. All logins with the Plug-in will create a local mobile account.

# 2 Overview

Micro Focus Kanaka for Mac provides macOS users automated single login access to NetIQ eDirectory storage resources through flexible login options. The Kanaka Plug-in component allows users to simultaneously log in to macOS and mount storage resources through a single username and password. The Kanaka Desktop Client allows users to access network storage resources after they have logged in as a local user to macOS.

*Figure 2-1* *Micro Focus Kanaka for Mac Architecture*
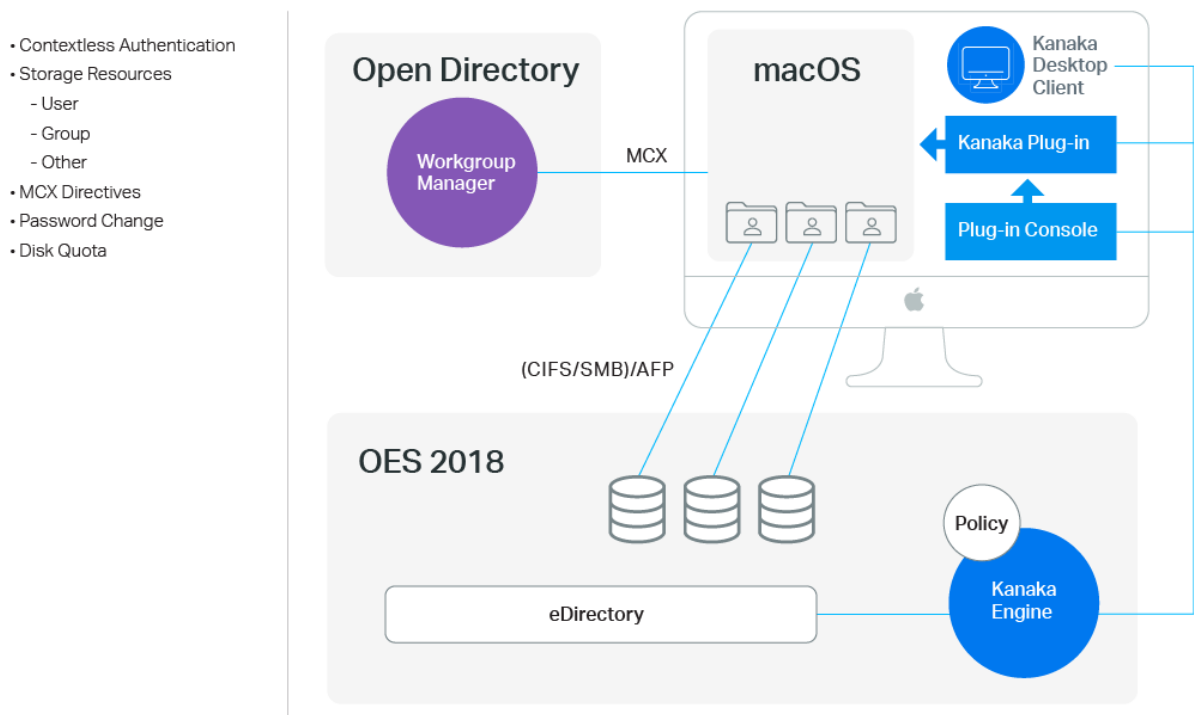


The components of Micro Focus Kanaka for Mac include the Engine, the management interface, and two methods of accessing Micro Focus Open Enterprise Server storage resources from macOS: the Kanaka Plug-in and the Kanaka Desktop Client. An expanded discussion of each of these components follows:

## 2.1 Installers and Executables

Micro Focus Kanaka for Mac is delivered via an ISO image. All components are in the ISO.

---

**NOTE:** Micro Focus Open Enterprise Server customers with a current Maintenance contract can download Micro Focus Kanaka for Mac for free through the Micro Focus Customer Care Center.

---

## 2.2 Engine

The Engine performs actions that enable communication between macOS and eDirectory. These actions include:

- Extending the eDirectory schema
- Creating a proxy user for performing certain tasks
- Storing volume client protocol information in eDirectory
- Assigning group home folders
- Authenticating users

## 2.3 Management Interface

All Micro Focus Kanaka for Mac management tasks are done through a browser-based management interface. The management interface is available after the Engine has been installed.

## 2.4 Kanaka Plug-In

The Kanaka Plug-in simplifies authentication to eDirectory along with access to a user's network home directory and collaborative storage through a single password login process. The Kanaka Plug-in requires users to enter valid eDirectory credentials via the macOS login window to log in and gain access to the desktop and any storage resources that are made available to them.

*Figure 2-2*   *The Kanaka Plug-In Authenticates via the Mac macOS loginwindow*
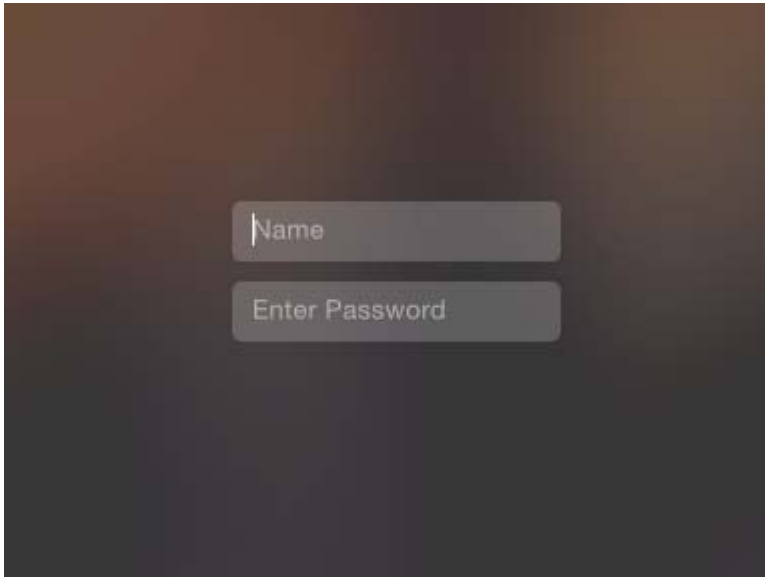


As an identity-based product, Micro Focus Kanaka for Mac utilizes eDirectory to view network user and collaborative storage attributes that pertain to a user and then mounts the storage resources accordingly.

*Figure 2-3*   *macOS Finder*
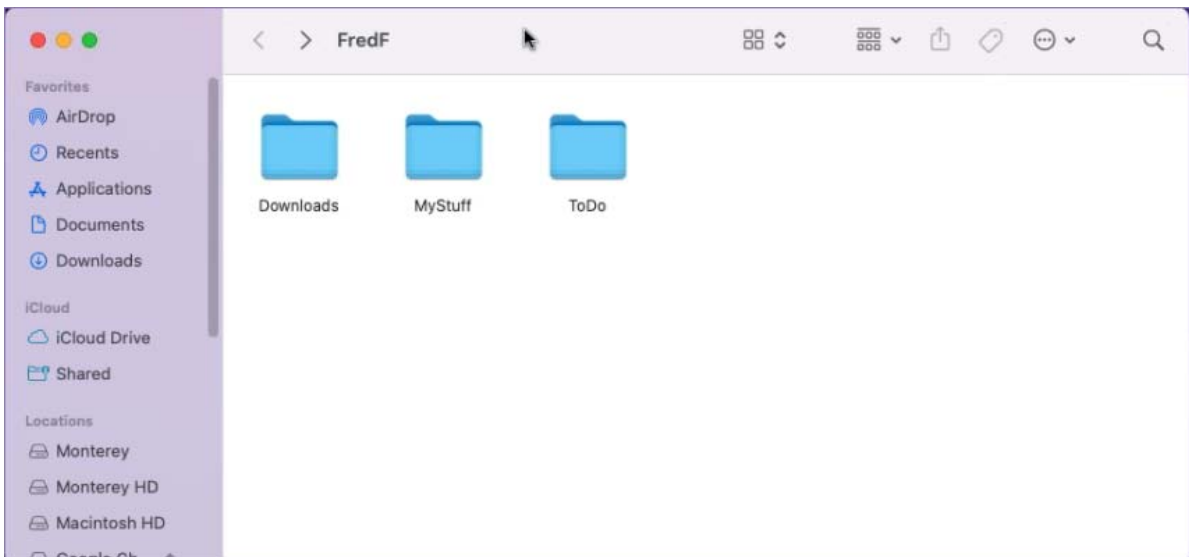


The screen shot above shows the Finder displaying a user's network storage resources. Micro Focus Kanaka for Mac can be configured so that these storage resources are mounted on the macOS desktop or accessed as shortcuts in the Dock.

Micro Focus Kanaka for Mac brings together native macOS technology, standard eDirectory authentication, and Open Enterprise Server's Native File Access connectivity. Micro Focus Kanaka for Mac communicates with eDirectory to perform contextless user authentication and retrieve identity

information in order to automatically mount both user home directories and collaborative storage resources located on servers and other storage resources via Open Enterprise Server's Native File Access protocols.

Native File Access allows macOS systems to connect to OES servers through AFP or CIFS/SMB (Common Internet File System/Server Message Block) protocols.

## 2.4.1    Authentication and Mounting via the Kanaka Plug-In

While logging in to macOS, the user is simultaneously authenticated to eDirectory through a Simple or Universal password. From eDirectory, Micro Focus Kanaka for Mac then retrieves identity information specific to the user including the home directory, login script, and collaborative storage attributes.

Upon retrieving these attributes, the Kanaka Plug-in converts them from their native format into a URL format that is needed by macOS to mount the storage resource. Depending on the configuration, the URL format can be AFP or CIFS/SMB.

The process for mounting collaborative storage resources, as well as eDirectory Storage Location Objects, is the same as the process for mounting user home directories.

---

**IMPORTANT:** When authenticating using the Kanaka Plug-In, the macOS workstation must not contain a local user account with the same name as the network account. If Mobility is enabled, a local "Mobile" account will be created.

---

## 2.4.2    Kanaka Plug-In, macOS, and Mobile Accounts

The Kanaka Plug-in leverages Apple's Mobile Account feature. Mobile accounts combine the ease of management in network accounts with the performance and portability of local home directories. The concept is that the user account information is stored in a network directory service. At login, it is cloned to the local directory on a client system.

Beginning with Kanaka for Mac version 3.2, all user logins are mobile accounts. When a user logs in, macOS creates a mobile account for the user if one doesn't already exist. If a mobile account does exist, macOS updates its locally cached information for the user and the login proceeds, and the user's network home directory and collaborative storage resources are mounted.

Mobile Accounts provide several benefits:

- Less network traffic than traditional network accounts. Reading and writing from the user's network home directory can be minimized.
- User's network home directory quotas can be smaller. ~/Library is not stored in the network home directory.
- If the network is down or the laptop is not on the corporate network, users can still log in to their local accounts with their eDirectory usernames and passwords.

## 2.4.3　Kanaka Plug-In Console

Users who authenticate to eDirectory via the Kanaka Plug-in can use the Kanaka Plug-in Console to view and minimally manage their identity within eDirectory. Kanaka Plug-in Console options let users view select user account information, monitor the quota for their network user and collaborative storage space, and change their eDirectory passwords.

*Figure 2-4*　*Identity Information Displayed in the Kanaka Plug-In Console*
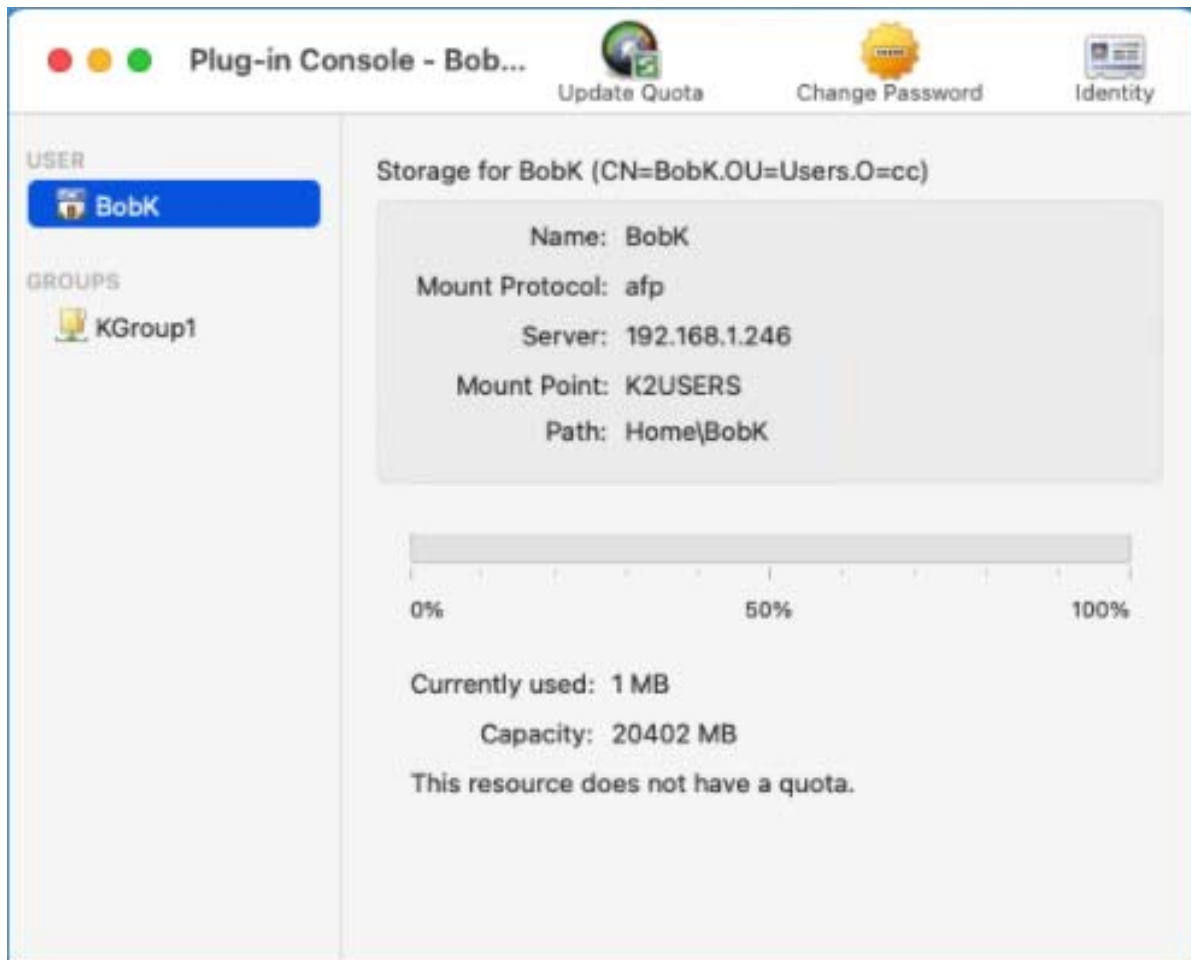


Clicking **Identity** displays eDirectory identity information, including the user's FDN (fully distinguished name).

The Kanaka Plug-in Console lists all mounted network storage resources for the user along with storage quota data.

*Figure 2-5* *eDirectory Password Management through the Kanaka Plug-in Console*
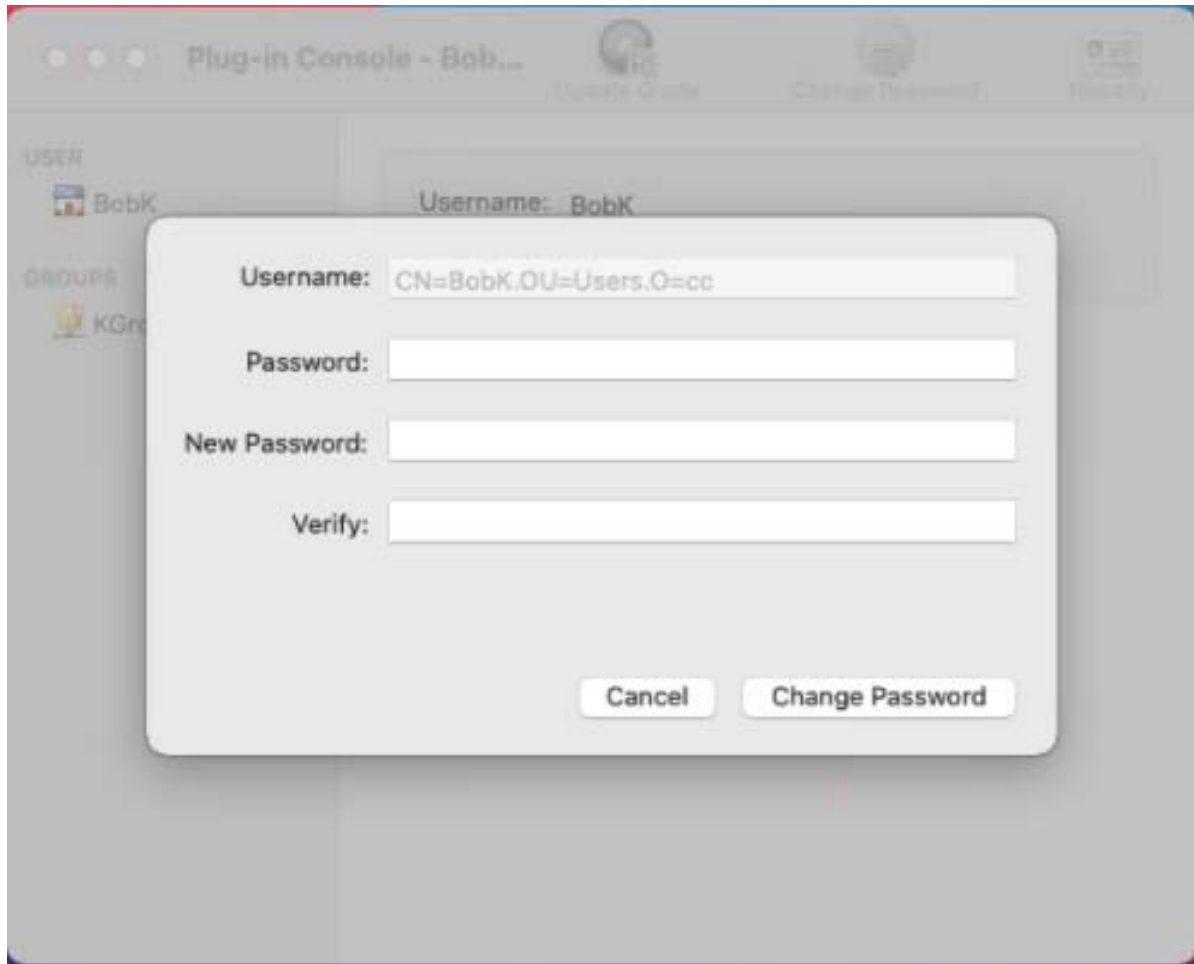


The Kanaka Plug-in Console also lets users change their eDirectory passwords natively through the macOS platform.

## 2.5 Kanaka Desktop Client

The Kanaka Desktop Client is the sensible connectivity option for users who require access to network storage resources, but are not required to authenticate to eDirectory each time they log in through macOS. Users who already have local accounts, for example, might prefer this option because it does not require a process to convert their local account to a network account, which is required with the Kanaka Plug-in.

Additionally, the Kanaka Desktop Client is ideal for macOS users who are on the go and often connect to the organization's network via VPN. Micro Focus Kanaka for Mac allows you to first log in to your organization's VPN and then use the Kanaka Desktop Client to access your network storage.

## 2.5.1 Authentication and Storage Mounting via the Kanaka Desktop Client

The process for authenticating to eDirectory begins with entering your eDirectory username and password in the Kanaka Desktop Client login window:

**Figure 2-6**   *The Kanaka Desktop Client*
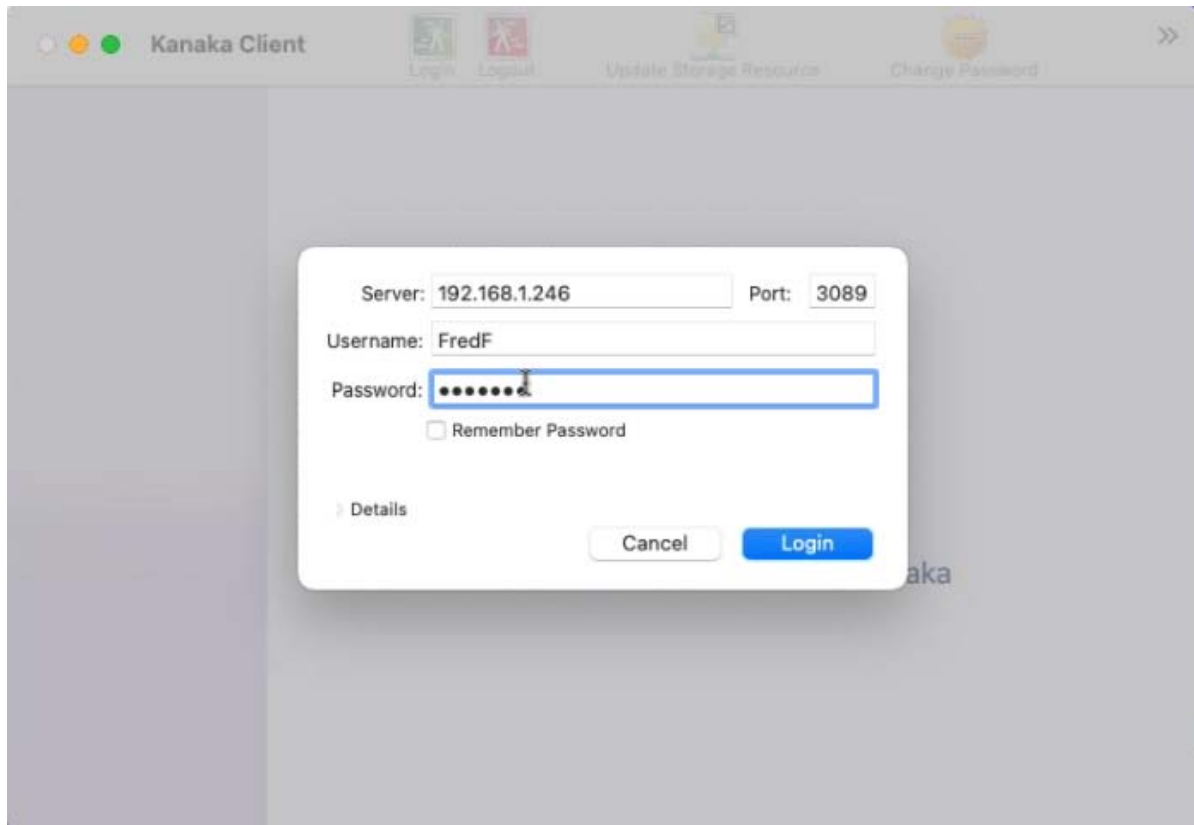


## 2.6 Deciding Which Access Method to Use

Depending on your environment, there might be scenarios where the Kanaka Plug-in is the preferred method of access over the Kanaka Desktop Client, and vice-versa. The table below provides some scenarios where one access method might be preferred over another.

**Table 2-1**   *Decision Matrix for Which Method of Access to Use*

| Scenario | Suggested Access Method |
| --- | --- |
| macOS users in a computer lab setting | Kanaka Plug-in |
| macOS users with assigned workstations and local accounts | Kanaka Desktop Client |
| macOS users who do not want to go through the login window to access network storage resources | Kanaka Desktop Client |

| Scenario | Suggested Access Method |
|---|---|
| macOS users who do not want to lose their workstation settings when accessing network storage resources | Kanaka Desktop Client |
| macOS mobile users who frequently work at home and connect to the organization's network via VPN | Kanaka Desktop Client |

# 3 Prerequisites

This section provides the procedures for completing necessary prerequisite tasks before you can install and configure Micro Focus Kanaka for Mac.

- Section 3.1, "Enabling File Protocols," on page 17
- Section 3.2, "Determining Which Protocols to Enable," on page 17
- Section 3.3, "Password Management," on page 18
- Section 3.4, "Testing AFP or CIFS," on page 19
- Section 3.5, "Generating Certificates," on page 20
- Section 3.6, "Add a Firewall Exception (Conditional)," on page 28

## 3.1 Enabling File Protocols

Micro Focus Kanaka for Mac enables communication between macOS and eDirectory through either AFP (Apple File Protocol) or CIFS/SMB (Common Internet File System/Server Message Block).

**IMPORTANT:** AFP (Apple File Protocol) has been identified as a deprecated technology. AFP is still available with OES2018 SP3. Furthermore, Big Sur and Monterey can mount AFP-shared volumes, but SMB is the preferred protocol.

When you enable either of these protocols, you subsequently enable Native File Access, allowing macOS users to do several things:

- Access files on the network
- Map network drives
- Create shortcuts to the servers

**IMPORTANT:** Micro Focus Kanaka for Mac adds considerable functionality to macOS connected systems through Native File Access. Native File Access must be configured on each server that a Mac with either the Kanaka Plug-in or the Kanaka Desktop Client might want to connect to. This includes servers with user home directories as well as servers with collaborative storage folders.

## 3.2 Determining Which Protocols to Enable

- Section 3.2.1, "CIFS," on page 18
- Section 3.2.2, "AFP," on page 18

Micro Focus Open Enterprise Server supports both the AFP and CIFS/SMB (listed simply as CIFS in the YaST Control Center interface) protocols.

**NOTE:** If you prefer, you can enable both AFP and CIFS on the same server.

### 3.2.1 CIFS

CIFS is a network file system plus a set of auxiliary services supported by underlying protocols. CIFS allows the sharing of directories, files, printers, and advertisement across a network. CIFS includes protocols for service announcement, naming, authentication, and authorization.

For more information, including procedures for enabling CIFS, see the *OES CIFS for Linux Administration Guide* (https://www.microfocus.com/documentation/open-enterprise-server/2023/file_cifs_lx/front.html).

### 3.2.2 AFP

AFP is Apple's network protocol solution to provide network file services for macOS and classic Mac OS. Large numbers of Mac clients can mount a remotely located volume (file system) through AFP and use the files simultaneously.

For more information, including procedures for enabling AFP, see the *OES AFP for Linux Administration Guide* (https://www.microfocus.com/documentation/open-enterprise-server/2018-SP3/file_afp_lx/h9izvdye.html).

**IMPORTANT:** OES 2023 does not support AFP directly, but if the configured storage server is running on an older OES version that does support AFP, Kanaka will still continue pass the configured AFP based path information to the Plug-in and Client.

## 3.3 Password Management

Password management is generally outside the scope of this guide and is covered appropriately in documentation such as the *Novell Modular Authentication Services (NMAS) Administration Guide* (http://www.novell.com/documentation/nmas33/admin/?page=/documentation/nmas33/admin/data/allq21t.html) and the *Novell Password Management Administration Guide* (http://www.novell.com/documentation/password_management33/pwm_administration/?page=/documentation/password_management33/pwm_administration/data/bwx6mik.html).

When authenticating to macOS, Micro Focus Kanaka for Mac determines the fully distinguished name of the user and then makes the appropriate API calls to verify the password with eDirectory. These APIs are currently limited to only the eDirectory password.

After authentication, user information and storage information are retrieved and returned to the Kanaka Plug-in and Desktop Client. The storage connection information is passed through to macOS so that it automatically connects to the appropriate network storage through the designated Native File Access protocol (AFP or CIFS).

The eDirectory password you use for authentication must match the password you use for Native File Access, whether it's Simple Password or Universal Password.

If you are using the Simple Password authentication method, you can use iManager to set the Simple Password.

If you are using the Universal Password authentication method, you can use iManager to set up Universal Password policies and apply them to users or containers. After the password policies are put into place, the Universal Password must be populated for each user. In most cases, this means that the user must go through a password change process.

Consult the *Novell Password Administration Guide* (http://www.novell.com/documentation/password_management33/).

Universal Password is easier than Simple Password to maintain throughout the lifecycle of a user. Beginning with eDirectory 8.8, APIs have been updated and Micro Focus Kanaka for Mac has been engineered to automatically use the Universal Password for all aspects of authentication and password change, so no synchronization is required.

## 3.4 Testing AFP or CIFS

Before you install Micro Focus Kanaka for Mac, you should test macOS connectivity to your Open Enterprise Server.

1. From a Mac, log in with a local account.
2. Press Command+k.
3. Do one of the following:
   - For Macs connecting via AFP, type `afp://`*IP_ADDRESS* or *DNS_hostname* and press Return, then click **Connect**.
   - For Macs connecting via CIFS, type `cifs://`*IP_ADDRESS* or *DNS_hostname* and press Return, then click **Connect**.



4. Log in as a user that has storage on the server.

   This should be a user that you intend to be a Micro Focus Kanaka for Mac user.

After authentication, you should see volumes that are accessible via AFP or CIFS.
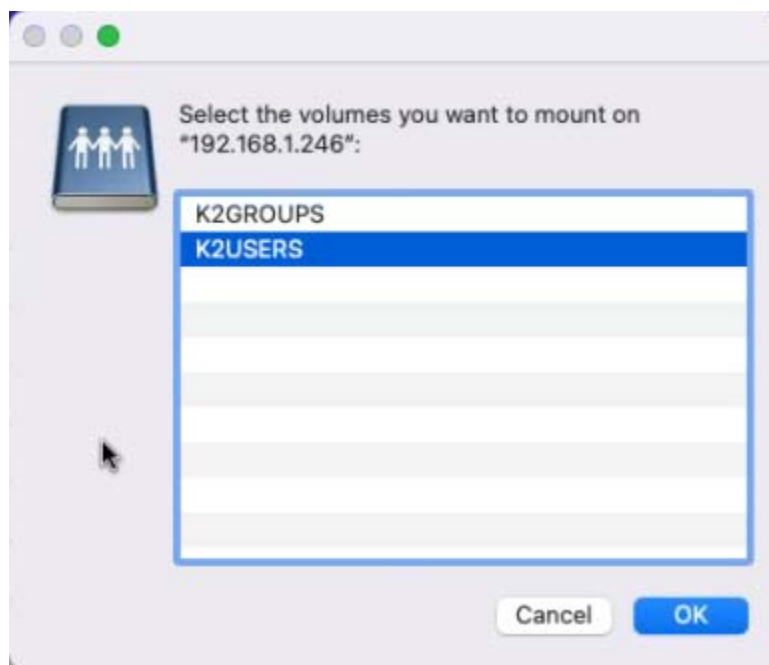


## 3.5 Generating Certificates

Micro Focus Kanaka for Mac 3.2 requires you to provide an x.509 certificate signed by a well-known certificate authority or another certificate authority that enables you export its trusted root certificate and deploy it to your Macs. The certificate must be in Privacy Enhanced Mail (PEM) format and must be installed in the appropriate secured location where the Kanaka Engine is running.

## 3.5.1 Certificate Types

There are two ways of obtaining a trusted certificate. Each method has its pros and cons.

- Create a certificate signing request, and have your internal eDirectory certificate authority (CA) sign the certificate. This is referred to as an internal CA.
- Create a certificate signing request, and have a trusted third-party certificate authority (CA) sign the certificate. This is referred to as an external CA.

*Table 3-1*  *Internal and External Certificate Authority Considerations*

| Certificate Authority | Pros | Cons |
| --- | --- | --- |
| Internal | <ul><li>Free</li><li>The expiration date can be extended much further than one issued by an external CA.</li></ul> | <ul><li>You need to install the certificate on each Mac computer running Micro Focus Kanaka for Mac 3.0.1.</li></ul> |
| External | <ul><li>The trusted root is already trusted by macOS.</li></ul> | <ul><li>You must depend on a third-party certificate provider.</li><li>The certificate can be expensive.</li><li>The certificate normally expires in one or two years.</li></ul> |

If you decide to use an external CA, you can obtain a list of CAs that are already trusted by opening the Keychain Access app and viewing the System Roots.

*Figure 3-1*   *List of Trusted Certificate Authorities*
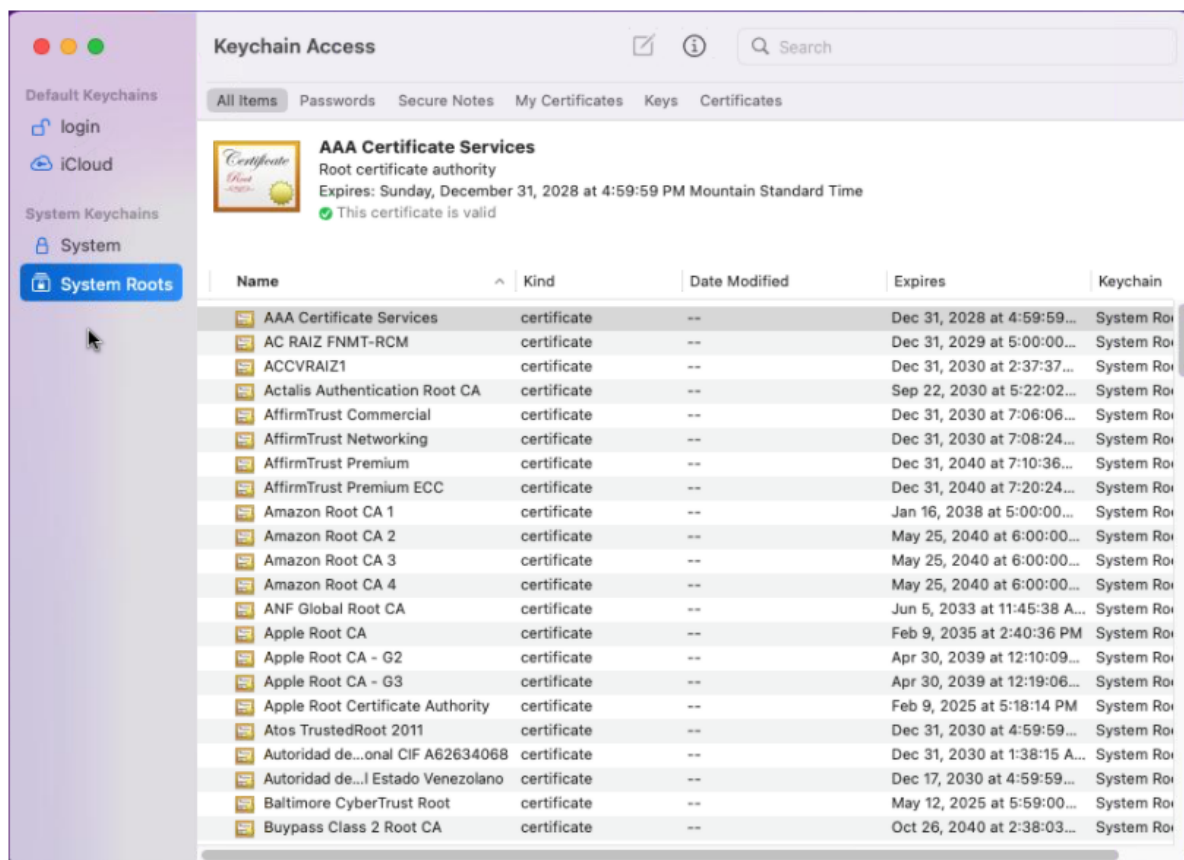
## 3.5.2    Exporting an eDirectory Server Certificate

Depending on usage, choose to export the DNS or IP certificate for the Open Enterprise Server that hosts the Kanaka Engine. If Kanaka clients are configured with the DNS hostname of the OES server, you should export the `DNS AG <server DNS hostname>` certificate. If Kanaka clients are configured with the IP address of the OES server, you should export the `IP AG <server IP address>` certificate.

1  Log in to iManager.

2  From **Roles and Tasks**, click **NetIQ Certificate Access**.

3  Click **Server Certificates**.

4  Select the certificate for the OES server hosting the Kanaka Engine.

5  Click **Export**.

6  From the **Certificates** drop-down menu, select the certificate that you checked in Step 4.

7  Leave **Export private key** selected.

8  Leave **Include all certificates in the certification path if available** selected.

9  Enter a password to protect the private key.

This is required when **Export private key** is selected.

10  Click **Next**.

**11** Click **Save the exported certificate**.

The file is saved to your `Downloads` folder with the name `cert.pfx`.

## 3.5.3 Convert a PKCS#12 Certificate to a PEM Certificate

iManager exports server certificates in the PKCS#12 or PFX format. This format needs to be converted to PEM format for the Kanaka Engine. You can use one of the following two methods to do so:

### microfocus-kanakaengine-convertcert

**1** Copy the `cert.pfx` file to the OES server hosting the Kanaka Engine.

**2** In a terminal session on the OES server hosting the Kanaka Engine type:

`microfocus-kanakaengine-convertcert`

**3** When prompted, enter the name of the certificate `cert.pfx`.

**4** When prompted, enter the pass phrase that was used when the certificate was exported.

In this case, the pass phrase from Step 9 from Section 3.5.2, "Exporting an eDirectory Server Certificate," on page 22.

You are then prompted twice to enter a new pass phrase for the temporary key.

**5** When prompted, re-enter the pass phrase you used for the temporary key in Step 4.

**6** Stop the Kanaka Engine:

`systemctl stop microfocus-kanakaengined`

**7** Copy the `server.pem` file:

`cp server.pem /etc/opt/microfocus/kanaka/engine/config`

**8** Start the Kanaka Engine:

`systemctl start microfocus-kanakaengined`

### Manual

**1** Copy the `cert.pfx` file to the OES server hosting the Kanaka Engine.

**2** In a terminal session on the OES server hosting the Kanaka Engine, enter the following commands and respond according to their responses:

`openssl pkcs12 -clcerts -nokeys -in cert.pfx -out out.crt`

    **2a** When prompted, enter the password that you provided when you exported the certificate in Step 9 of Section 3.5.2, "Exporting an eDirectory Server Certificate," on page 22.

        `openssl pkcs12 -nocerts -in cert.pfx -out private.key`

    **2b** When prompted, enter the password that you provided when you exported the certificate in Step 9 of Section 3.5.2, "Exporting an eDirectory Server Certificate," on page 22.

        `openssl rsa -in private.key -out newkey.key`

    **2c** When prompted, enter the pass phrase that you provided when you exported the certificate in Step 9 of Section 3.5.2, "Exporting an eDirectory Server Certificate," on page 22.

```
cat newkey.key > server.pem

cat out.crt >> server.pem
```

The `server.pem` file can now be copied for use by the Kanaka Engine.

**3** Stop the Kanaka Engine:

```
systemctl stop microfocus-kanakaengined
```

**4** Copy the `server.pem` file:

```
cp server.pem /etc/opt/microfocus/kanaka/engine/config
```

**5** Start the Kanaka Engine:

```
systemctl start microfocus-kanakaengined
```

## 3.5.4 Export an eDirectory CA Trusted Root

**1** Log in to iManager.

**2** From **Roles and Tasks**, click **NetIQ Certificate Access**.

**3** Click **Server Certificates**.

**4** Select the certificate for the OES server hosting the Kanaka Engine.

**5** Click **Export**.

**6** From the **Certificates** drop-down menu, select the organizational CA certificate (e.g. OU=Organizational CA.O=EINDOAK).

**7** Leave the export format as DER.

**8** Click **Next**.

**9** Click **Save the exported certificate**.

The file is saved to your `Downloads` folder with the name `cert.der`.

The certificate is now ready to be deployed to macOS.

## 3.5.5 Adding a Trusted Root Certificate to macOS

**1** Copy the `cert.der` file you created in Step 9 of Section 3.5.2, "Exporting an eDirectory Server Certificate," on page 22 to macOS.

**2** On macOS, open the Keychain Access.app.

**3** From the list of Keychains, select **System**.
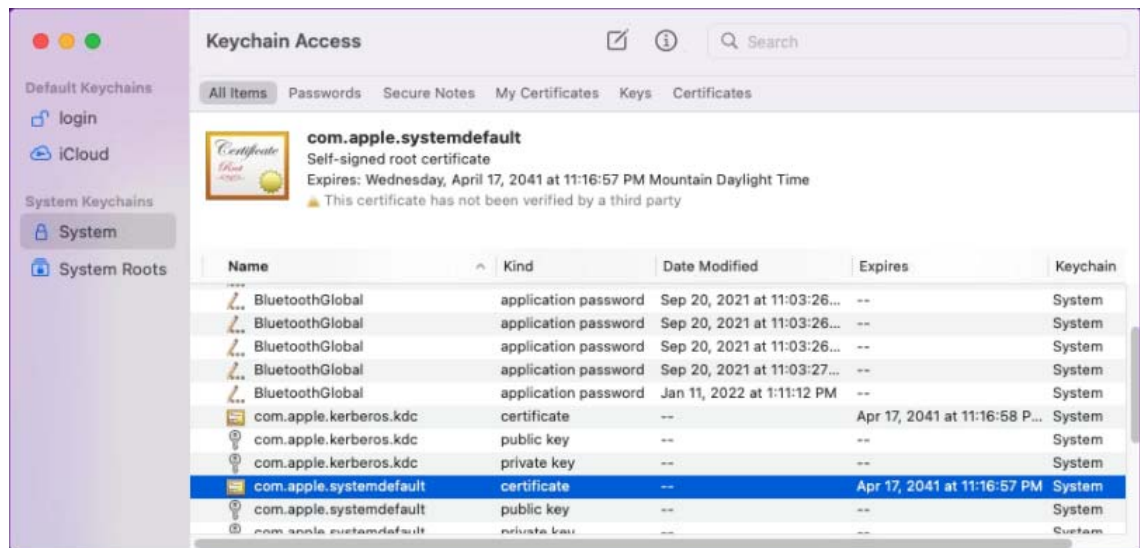
**4** Drag and drop `cert.der` to the System keychains.

**5** When prompted, enter the necessary local administrator credentials.

The certificate is added to the System Keychain, but it must still needs to be trusted.

If you select the certificate **Organizational CA,** note that the text indicates that the root certificate is not trusted.
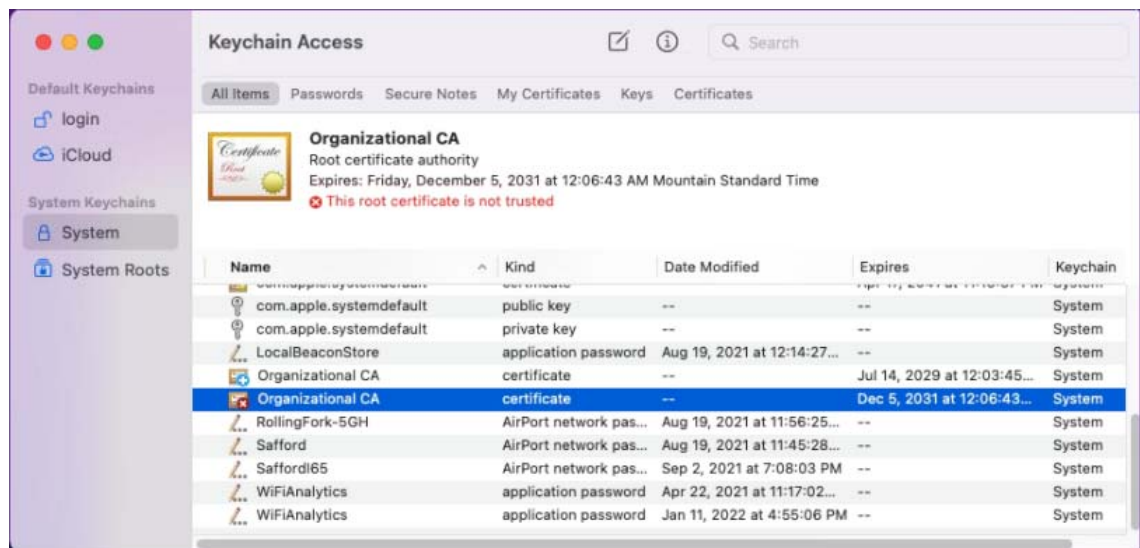


**6** Double-click **Organizational CA**.

**7** Expand **Trust**.

**8** For **When using this certificate**, select **Always Trust**.

Note that the trusted status has not changed yet.

**9** When prompted, enter the necessary local administrator credentials.

The status of **Organizational CA** should change to trusted.



Kanaka clients can now successfully connect to the Kanaka Engine.

## 3.5.6 Creating Your Own Certificate

**IMPORTANT:** Be sure to store all your certificates in a secure location.

**1** At the server that will host the Kanaka Engine, launch a terminal session.

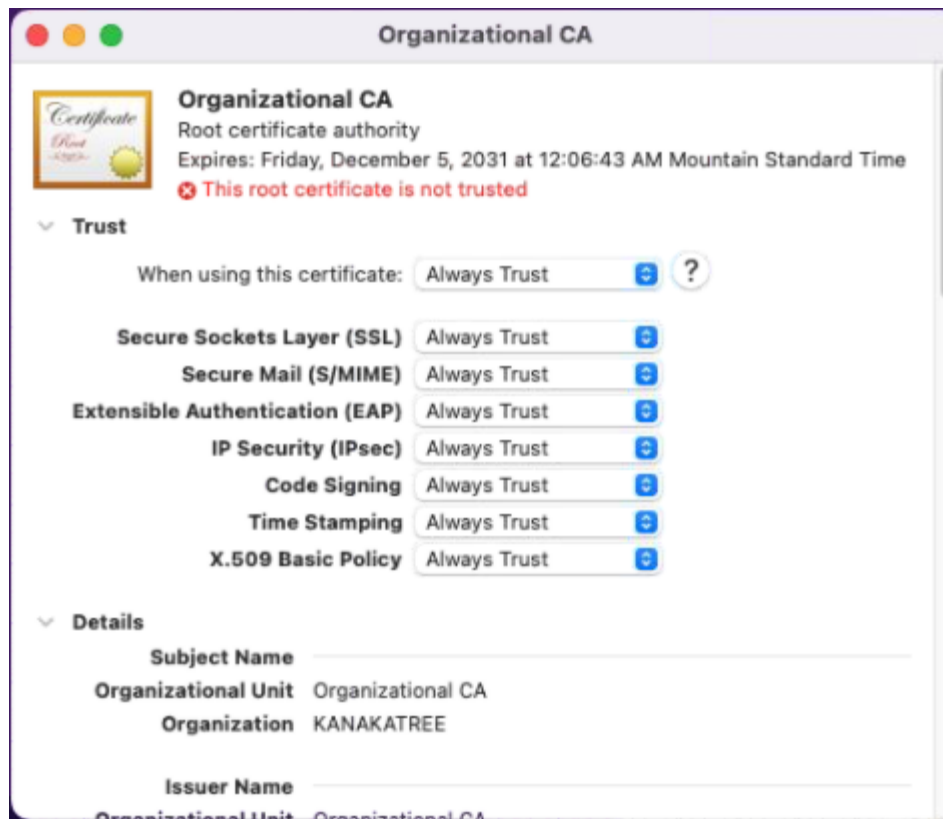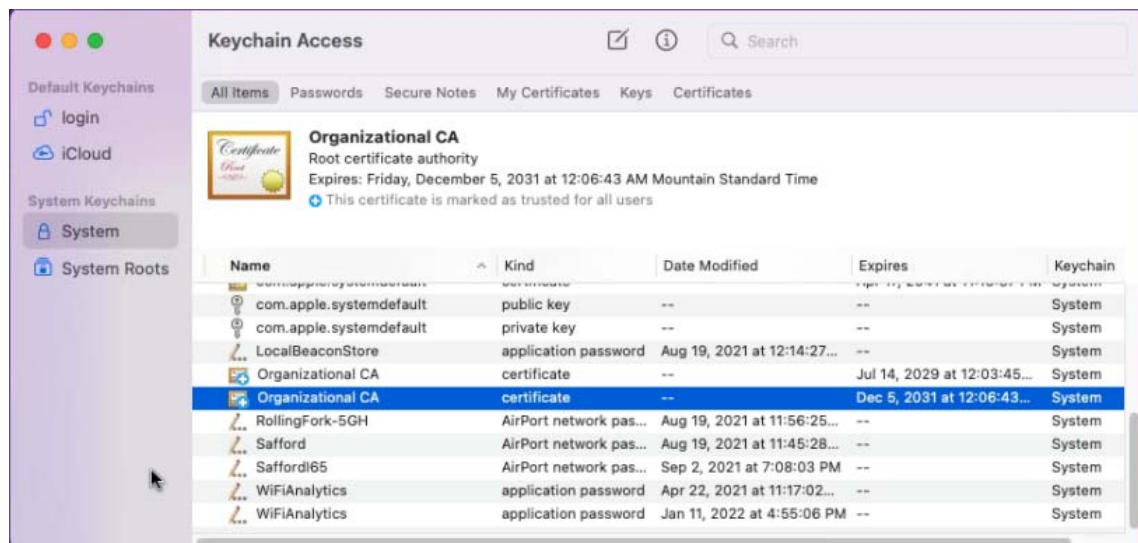**2** Create a private key and certificate signing request via OpenSSL.

The following command uses OpenSSL to create your private key and certificate signing request (CSR) with a single command.

```
openssl req –newkey rsa:2048 –keyout private.key  -out server.csr
```

**3** When prompted, answer each of the questions pertaining to the certificate.

| Question | Explanation |
| --- | --- |
| Country Name (two-letter code) | The ISO 3166 two-letter country code pertaining to the country where Kanaka Engine is located. |
| State or Province (full name) | The complete name of your state or province. |
| Locality Name (such as the city) | The complete name of your city. |
| Organization Name | The name of your company or organization. |
| Organizational Unit | The name of your department (optional). |
| Common Name | The name of your server. |
| Email Address | The email address of the certificate administrator. |
| Challenge Password | Generally optional, but required by some third-party certificate providers. |

**4** Submit the `server.csr` contents to the certificate authority of your choosing.

The certificate authority creates a certificate based the contents of the CSR file you created in Step 2. The certificate authority creates the certificate in one of many formats, such as DER, CER, CRT, or PEM. You can use any of these formats to produce the final PEM format that Micro Focus Kanaka for Mac will use.

**5** Convert the certificate to PEM format:

```
openssl x509 –inform DER –outform PEM –in certificate.crt -out
certificate.pem
```

**6** Remove the passphrase or password from the certificate:

```
openssl x509 –in certificate.pem -out insecure.certificate.pem
```

**7** Decrypt the private key:

```
openssl rsa –in private.key -out decrypted.private.key
```

The private key is encrypted by default and needs to be decrypted for the Kanaka Engine to use.

**8** Remove the passphrase or password from the certificate:

```
openssl rsa –in decrypted.private.key -out
insecure.decrypted.private.key
```

**9** Create the `server.pem` file with both the private key and certificate files:

```
cat insecure.decrypted.private.key insecure.certificate.pem >
server.pem
```

The output file must be named `server.pem`.

10 Proceed with Chapter 5, "Installing and Configuring the Engine," on page 31.

## 3.6 Add a Firewall Exception (Conditional)

If you have the firewall enabled, you will need to create an exception to allow Kanaka access through the firewall. To do so, follow the procedures below.

1 Launch YaST.

2 Select **Firewall** > **Allowed Services.**

3 Click the **Advanced...** button

4 In the **TCP Ports** field, add `3089`.

5 Click **OK**.

6 Click **Next**.

7 Click **Finish**.

# 4 Upgrading from Version 3.1

## 4.1 Upgrade Considerations

### 4.1.1 Kanaka Engine

The Kanaka Engine service can be upgraded only from Kanaka 3.1.

### 4.1.2 Kanaka Client and Plug-In

The Plug-in and Desktop Client for Micro Focus Kanaka for Mac 3.2 can only be installed on macOS Catalina (10.15) and higher. Previous versions of Kanaka cannot run on 10.15+. As such, there is no direct upgrade path for Mac components from Kanaka 3.0.1 and earlier. However, these earlier version's components can still be used on earlier versions of macOS, and are compatible with the Kanaka 3.2.1 Engine.

The Kanaka Engine service includes two DMG files, one containing the Kanaka 3.2 Mac components and one containing the Kanaka 3.0.1 components for use on earlier versions of macOS.

### 4.1.3 From Version 3.1 to 3.2

Version 3.1 clients will continue to function as-is because it is assumed that they have already been configured with a trusted root of the CA that signed the existing `server.pem` used by the version 3.1 Kanaka Engine.

## 4.2 Performing the Upgrade

1 From the ISO image, copy the RPM file that is applicable to the operating system and architecture of the server that will host the Kanaka Engine.

2 From the server that will host the Kanaka Engine, open a terminal session.

3 Navigate to the RPM file you copied in Step 1.

4 At the terminal console, run the following command to import the signature key via RPM:

   `rpm -import ./condrey-packages-gpgkey.pub`

5 Run the following command to install Kanaka:

   `zypper install ./microfocus-kanaka-engine-3.2.1.-x.x86_64.rpm`

6 Once the upgrade has completed, run `microfocus-kanakaengine-config` to verify the configuration was properly migrated.

# 5 Installing and Configuring the Engine

The Kanaka Plug-in and Kanaka Desktop Client have four basic needs for interacting with the Open Enterprise Server network infrastructure:

- Authenticating the user to eDirectory
- Retrieving information and interacting with eDirectory
- Retrieving information from the Open Enterprise Server file system
- Providing access to the Open Enterprise Server file system

All of these are accomplished via the Kanaka Engine, which you install and set up by following the procedures in this section.

- Section 5.1, "System Requirements," on page 31
- Section 5.2, "Installing the Kanaka Engine," on page 32
- Section 5.3, "Configuring the Engine," on page 33
- Section 5.4, "Replacing the PEM File," on page 39

**IMPORTANT:** You can have multiple Kanaka Engines in the same eDirectory tree. To do so, you must select or create a separate Kanaka proxy object for each server instance in Step 2 of the Setup Wizard.

This is important because each instance of a Kanaka Engine sets a different password for its Kanaka proxy object. If you use the same Kanaka proxy object for each Kanaka Engine, upon completion of the Setup Wizard, the new instance of the Kanaka Engine overwrites the current password for the object in eDirectory. This results in failures to perform operations for the Kanaka Engine instance that was initially configured for the proxy object.

**NOTE:** Micro Focus Kanaka for Mac does not support clusters, but you can install two engines with identical configurations and then add both servers to the macOS Directory Utility when you configure the Kanaka Plug-in.
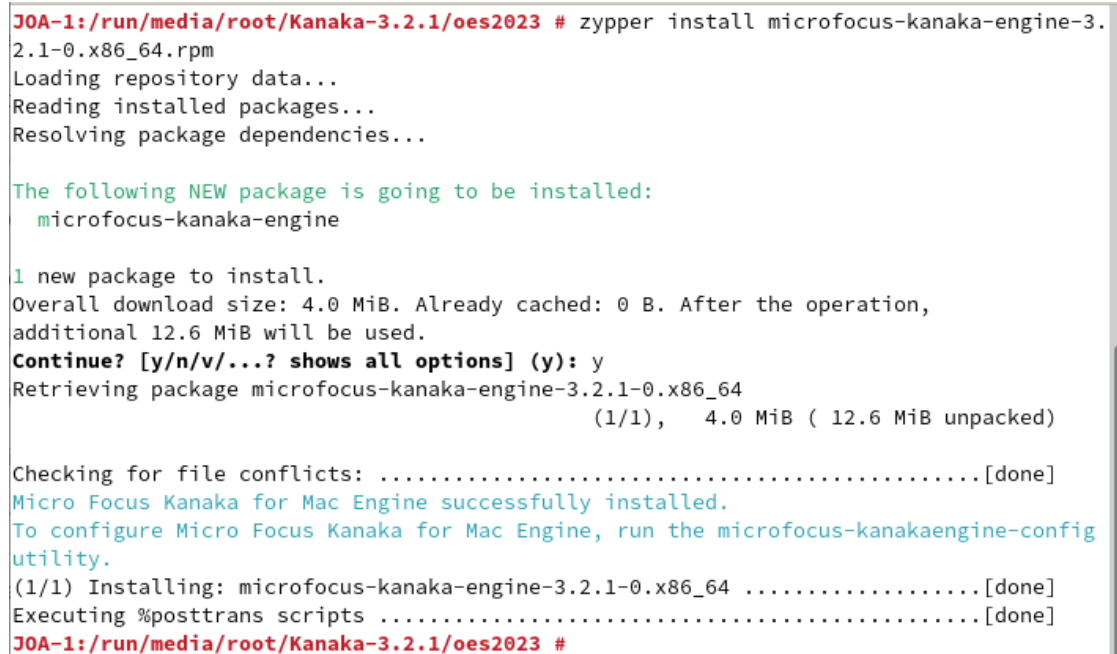
## 5.1 System Requirements

The Kanaka Engine can be hosted on Open Enterprise Server 2018 SP3 or later.

# 5.2 Installing the Kanaka Engine

**IMPORTANT:** These procedures do not work unless you have first generated a certificate and created a PEM file. If you have not done so already, do so now by following the procedures in Section 3.5, "Generating Certificates," on page 20.

1 From the ISO image, copy the RPM file to the server that will host the Kanaka Engine.

2 From the server that will host the Kanaka Engine, open a terminal session.

3 Navigate to the RPM file you copied in Step 1.

4 At the terminal console, run the following command:

```
zypper install ./microfocus-kanaka-engine-3.2.1-x.x86_64.rpm
```

```
JOA-1:/run/media/root/Kanaka-3.2.1/oes2023 # zypper install microfocus-kanaka-engine-3.
2.1-0.x86_64.rpm
Loading repository data...
Reading installed packages...
Resolving package dependencies...

The following NEW package is going to be installed:
  microfocus-kanaka-engine

1 new package to install.
Overall download size: 4.0 MiB. Already cached: 0 B. After the operation,
additional 12.6 MiB will be used.
Continue? [y/n/v/...? shows all options] (y): y
Retrieving package microfocus-kanaka-engine-3.2.1-0.x86_64
                                           (1/1),   4.0 MiB ( 12.6 MiB unpacked)

Checking for file conflicts: ...........................................[done]
Micro Focus Kanaka for Mac Engine successfully installed.
To configure Micro Focus Kanaka for Mac Engine, run the microfocus-kanakaengine-config
utility.
(1/1) Installing: microfocus-kanaka-engine-3.2.1-0.x86_64 ...................[done]
Executing %posttrans scripts ...........................................[done]
JOA-1:/run/media/root/Kanaka-3.2.1/oes2023 #
```

5 At the terminal console, run the following command:

```
microfocus-kanakaengine-config
```

This launches the Micro Focus Kanaka for Mac Engine Configuration utility.

6 Press Enter to select the default data path.

or

Specify a new data path.

7 Press 0 to select the displayed IP address.

or

Specify a new IP address.

If multiple addresses are listed, select the desired address for your network configuration.

8 When the HTTP Port [0] option appears, type `0`.

9 Unless there is a conflict, accept the default HTTPS port number of 3089.

If you need to use another port number, provide the new port number.

**10** Press Enter to continue.

```
--------------------------------------------------------------------------------
Micro Focus Kanaka for Mac Engine Service Config
--------------------------------------------------------------------------------
Data Path:                      /var/opt/microfocus/kanaka/engine/data
Engine Address:                 192.168.17.171
   HTTP Port:                   0
   HTTPS Port:                  3089
Default NCP Server Address:     JOA-1
Debug Level:                    5


--------------------------------------------------------------------------------
[D] Data Path                   [E] Engine Service
[N] Default NCP Server Address  [O] Debug Options
[S] Service Management          [Q] Quit


Selection->█
```

**11** Type `Q` to quit and save the configuration.

**12** When are asked if you want to restart the service, do not do so until completing Step 13.

**13** Copy the PEM file that you created in Step 9 under "Generating Certificates" to the following location:

`/etc/opt/microfocus/kanaka/engine/config`

**14** Restart the service by selecting `Y`.

## 5.3    Configuring the Engine

The Kanaka Engine services all requests made by the Kanaka client components. Besides performing the initial authentication, the Kanaka Engine allows the Kanaka Plug-in and the Kanaka Desktop Client to operate in a contextless manner to pull relevant individual user and storage access information from eDirectory and the file system and return the information in a format relevant to macOS.

The Engine also services password change requests, specifies client storage information through the Kanaka Plug-in Console, and informs Micro Focus Kanaka for Mac users of password expirations that will occur in the near future.

**1** From a Web browser, launch the management interface by entering `https://server_ip_or_DNS_name:3089`.

**2** Enter eDirectory credentials capable of modifying directory services and schema, such as an Admin or Admin equivalent.

You can log in with the following FDN formats:

```
CN=user.O=microfocus
.user.microfocus
user.microfocus
```

These formats work when the user object is contained within standard Organization and Organizational Unit objects. For example:

```
CN=user.O=microfocus
CN=user.OU=users.O=microfocus
```

However, if the user is located in something like a Locality, domain, or Country container the typeful FDN must be used. For example:

```
CN=user.O=it.L=east.O=microfocus
CN=user.O=IT.DC=microfocus.DC=com
CN=user.O=IT.c=us
```

Because you are performing administrative work, your must log in using a fully distinguished name in the **Username** field. You can use a format such as *cn=user.o=org* or *user.org*.



The management interface launches the Setup Wizard.

**Configure**

Restart Wizard

**Version**

Server Status

Version:
3.2.0.1 Sep 30 2021 09:25:00

**Setup Wizard Step 1 of 4 - Schema Extensions**

The Kanaka schema extensions for eDirectory are already installed. Click Next to continue.

NEXT

Copyright © 2004-2021 Condrey Corporation. All Rights Reserved.

**3** Click **Next** to extend the eDirectory schema.

As with all schema extensions, be aware that it might take some time for the schema extensions to be synchronized in a large tree.

The following page appears for you to create a proxy user and administration group:

**Configure**

Restart Wizard

**Version**

Server Status

Version:
3.2.0.1 Sep 30 2021 09:25:00

**Setup Wizard Step 2 of 4 - System Rights**

Kanaka requires appropriate rights in order to obtain information from eDirectory and perform operations. This action is performed under the authority of a Kanaka Proxy user object. A proxy user must be defined before Kanaka can continue.

**Select a context in which the Kanaka Proxy will be created. If there is an existing object by the specified name it will be reprovisioned.**

Kanaka Proxy Object: [                    ]   BROWSE

Kanaka also requires an administrators group to be defined. Only members of the Kanaka administrators group will be allowed to log in and perform administrative tasks in the Kanaka web interface.

**Either select an existing group to be defined as the administrators group or select a context in which a group will be created.**

Kanaka Administrators Group: [                    ]   BROWSE

☑ **Make CN=admin.O=cc a member of the Kanaka administrators group**

You can choose to have the wizard give the Kanaka Proxy the rights to perform all necessary tasks or you can manually configure them yourself. Manual configuration requires that you give the Kanaka Proxy rights to eDirectory and the appropriate file system rights to all volumes or paths that might be accessed by a user via Kanaka. See the documentation for more details.

☐ **Manually provision rights for Kanaka Proxy**

NEXT

Copyright © 2004-2021 Condrey Corporation. All Rights Reserved.

A proxy user is needed because Micro Focus Kanaka for Mac authenticates and operates under the rights of a proxy user.

**4** Use the **Browse** button that corresponds to the **Kanaka Proxy Object** field to browse to the container where you want the Micro Focus Kanaka for Mac proxy user to reside.

Ensure that this user has rights to retrieve user and group information from eDirectory as well as view quota information in the file system of all volumes holding user and collaborative storage.

The name `KanakaProxy` is prepended to the container object you specify.

The proxy user object is created in eDirectory when you click the **Next** button in the Setup Wizard.

**5** Use the **Browse** button that corresponds to the **Kanaka Administrators Group** field to do one of the following:

- Locate and select a group whose members you want to be Kanaka for Mac administrators.

- Browse to the location where you want the new KanakaAdmins group to reside in eDirectory.

The name `KanakaAdmins` is prepended to the object you specify.

The proxy user account and password are self-managed by the Kanaka Engine. The password is never stored in any location, so there is no concern for security of the password. No two Kanaka Proxy users ever have the same password.

**6** Leave the check box selected so the user you are logged in as can be a member of the administrators group.

This will ensure that you are able to log in and manage Micro Focus Kanaka for Mac via the management interface.

**7** Click **Next**.

The Kanaka Administrators Group object is created and the logged-in user is added to the group.

The Kanaka proxy object is also created. By default, this user object is automatically assigned Supervisor rights at the root of the eDirectory tree. You can remove this rights assignment and assign rights more granularly to the tree and the associated file systems. The object needs the following minimum rights:

- Browse Entry rights to the eDirectory tree
- Read and Compare Attribute rights to any of the following objects that might be used or accessed through Micro Focus Kanaka for Mac:
  - Users
  - Groups
  - Containers, including Os, OUs, Domains, Countries, and Locales
  - Login scripts
  - Profiles
  - Servers
  - Volumes
- Read and FileScan rights to any file system directories that might be used or accessed by a Micro Focus Kanaka for Mac user, including user home directories, group home directories, or any file system that might be mapped and later accessed through a login script.

The following page appears for you to create a user index:

Micro Focus Kanaka for Mac maintains an index of user objects for the purpose of supporting contextless logins from the Kanaka Plug-in and Kanaka Desktop Client. The index is made up of user objects in a set of search object containers in eDirectory.

**8** Use the **Browse** button to locate a context where your Micro Focus Kanaka for Mac users reside in eDirectory.



**9** Click **Add**, then repeat Step 8 to add another container.

Repeat this step until you have added all the contexts you want to the list.

Setup Wizard Step 3 of 4 - User Index

Kanaka maintains an index of user objects for the purpose of supporting contextless logins from Kanaka clients. The index is comprised of user objects in the following search object containers in eDirectory. The index is updated at the following times:

- Automatically based on the **Rebuild Times** schedule set below.
- On demand using the **Rebuild Now** button below.

Configure Kanaka by adding search object containers below as appropriate based on the location of user objects that will be using Kanaka clients.

Micro Focus Kanaka for Mac does not have the ability to differentiate users with the same name in different contexts. If you index containers with users having identical names, those users cannot log in.

**10** In the **Search Depth** region, specify whether you want Micro Focus Kanaka for Mac to search for users only at the top layer of the container, or within subcontainers as well.

**11** In the **Rebuild Times** region, specify the hours when you want Micro Focus Kanaka for Mac to rebuild the index.

You should choose an hour when there is minimal network activity.

**12** Click **Next**.

The index is updated under different circumstances:

- Automatically based on individual users logging in.

    If a given user is not found in the index, the user is automatically located in the given search containers and dynamically added to the index.

- Automatically based on the hourly rebuild times schedule set in the configuration.
- Automatically 90 seconds after the engine loads.
- On demand using the Micro Focus Kanaka for Mac management interface.

The following page appears:
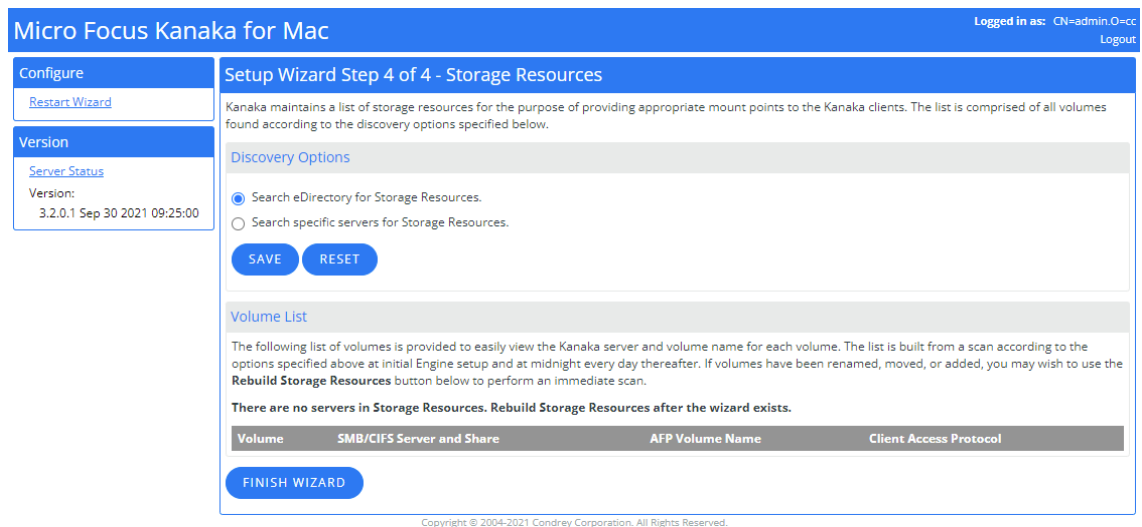
Micro Focus Kanaka for Mac must be configured for each AFP or CIFS volume name for each volume on the network containing home directories or collaborative storage.

For a description of the process that Micro Focus Kanaka for Mac uses to retrieve mount points for macOS, see Section 11.1, "Storage Resources," on page 61.

Storage Resources cannot be built during the setup wizard. However, it can be built once the setup wizard has finished and an internal restart of the Kanaka Engine server takes place.

**13** Click **Finish Wizard** to conclude the Setup Wizard.

When you click **Finish Wizard** the engine undergoes an internal restart operation and you are prompted to log in again. You might want to wait a few minutes while this process takes place.

**14** (Conditional) If you get an error trying to reload the page, check the Engine's status with the following command in a terminal session:

```
systemctl status microfocus-kanakaengined
```

If the status is unused, issue the following command to start the Engine:

```
systemctl start microfocus-kanakaengined
```

## 5.4 Replacing the PEM File

Follow the procedures below to replace the default PEM file with the new PEM file that you created in Section 3.5, "Generating Certificates," on page 20.

**1** From the server hosting the Kanaka Engine, launch a terminal session.

**2** Copy the PEM file that you created in Step 9 on page 27 to the following path:

```
/etc/opt/microfocus/kanaka/engine/config
```

**3** Stop the Kanaka Engine:

```
systemctl stop microfocus-kanakaengined
```

**4** Restart the Kanaka Engine:

```
systemctl start microfocus-kanakaengined
```

# 6 Installing the Plug-In and the Desktop Client

This section includes the procedures for installing the two client options for Micro Focus Kanaka for Mac, which are the Kanaka Plug-in and the Kanaka Desktop Client. For a discussion of each of these components, see Section 2.4, "Kanaka Plug-In," on page 10 and Section 2.5, "Kanaka Desktop Client," on page 14.

- Section 6.1, "Retrieving the Installation File," on page 41
- Section 6.2, "Installing the Kanaka Plug-In," on page 41
- Section 6.3, "Configuring the Kanaka Plug-In," on page 44
- Section 6.4, "Installing the Kanaka Desktop Client," on page 45

## 6.1 Retrieving the Installation File

The Kanaka Plug-In and Desktop client are both contained on a single DMG image file. This image file is available from either the Kanaka 3.2 ISO or via the Kanaka Engine's web server.

- Section 6.1.1, "Retrieving the Installation File from the ISO," on page 41
- Section 6.1.2, "Retrieving the Installation File from a Web Browser," on page 41

### 6.1.1 Retrieving the Installation File from the ISO

1. From the ISO, locate the `CLIENT` folder and select the `DMG` file containing the version of the Kanaka Client or Plug-In appropriate for the client macOS devices.
2. Copy the installation file to each Mac where the Plug-In or Desktop Client will be installed.

### 6.1.2 Retrieving the Installation File from a Web Browser

1. 1.From the Mac where the Plug-In or Client will be installed, open a browser and go to `https://Kanaka-Engine-server-address:3089/m/GetClient.html`.
2. Click the **MicroFocus_Kanaka_for_Mac-3.2.0.dmg** link to copy the installation file to the Mac.

## 6.2 Installing the Kanaka Plug-In

1. Double-click the `MicroFocus_Kanaka_for_Mac-3.2.0.dmg` file.

2  Double-click **Install Kanaka Plug-in 3.2.0**.

3  Click **Continue**.
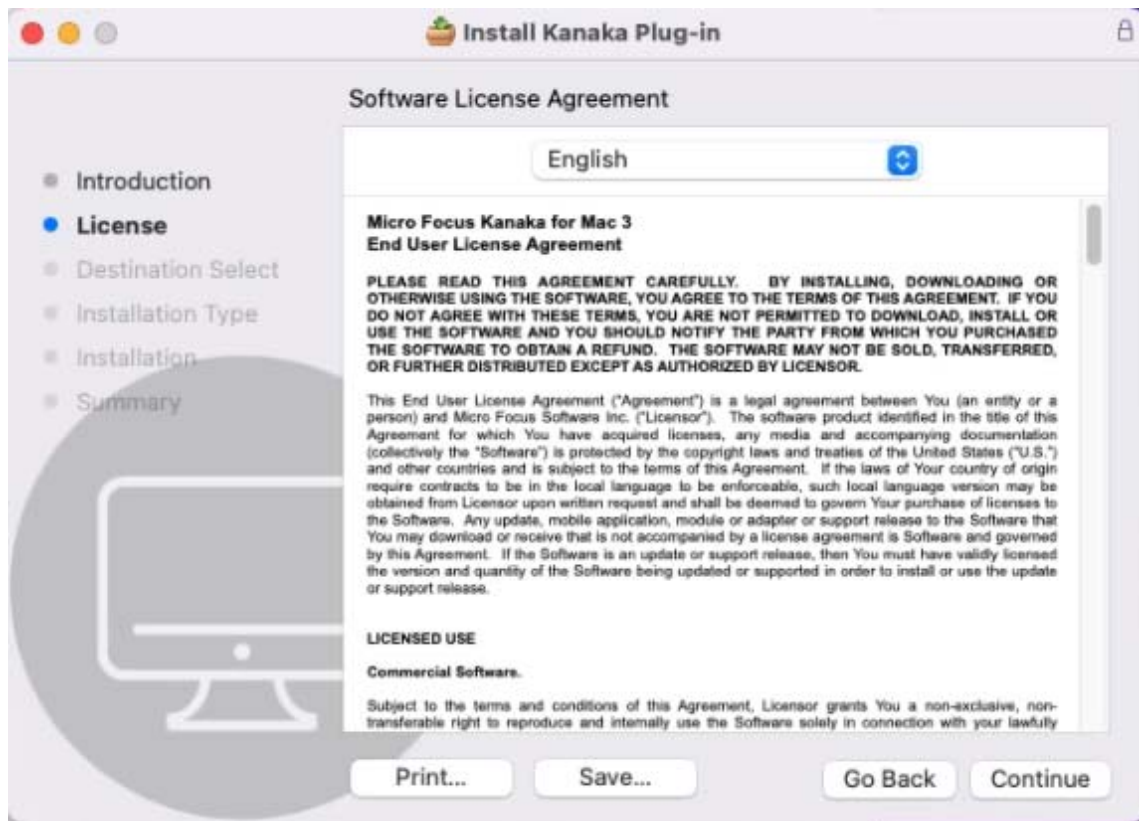
**4**  Review and accept the license agreement.
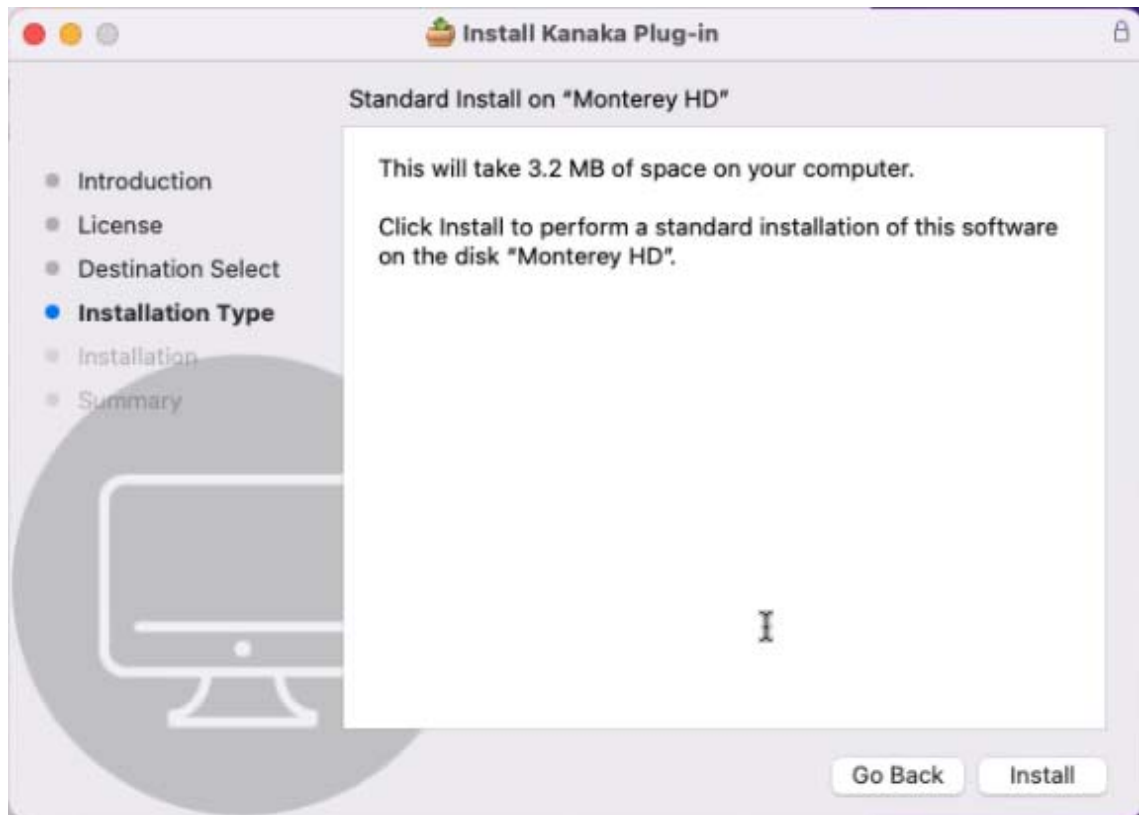
**5** Accept or change the default installation directory as needed, then click Install.

**6** Enter the local Administrator's credentials (to permit installation of the Kanaka Plug-in) and click **Install Software**.

**7** Once the installation process is complete, click **Close**.

# 6.3 Configuring the Kanaka Plug-In

You must configure the Kanaka Plug-in so it can communicate with the server hosting the Kanaka Engine.

**1** Run the Kanaka Utility by selecting **Applications** > **Kanaka**.

**2** Enter local Administrator's credentials for the Mac in order to continue, and click **Modify Configuration**.

**3** Click **+** to add a server.

In this case, the Kanaka Engine host server.

**4** Specify the address of the Kanaka Engine server by DNS name or IP address.

**5** Specify the port used to communicate with the Kanaka Engine service.

By default, this is 3089.
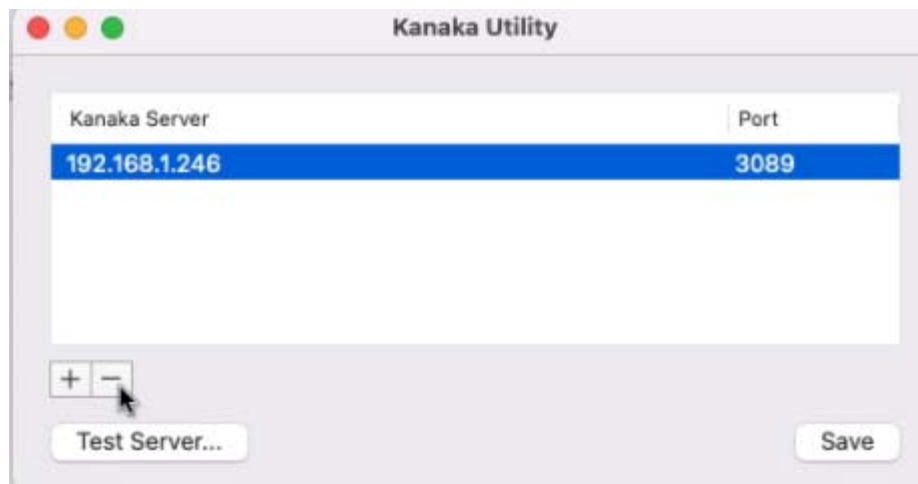


**6** Click **Save** and when prompted again, enter local Administrator's credentials.

**7** Open the Directory Utility application.

**8** Click **Search Policy** and confirm that **/Kanaka/Auth** is listed under **Directory Domains**.

If it is not, continue with the steps below to add the Kanaka search path.

**9** (Conditional) Click the Lock icon to enable you to make changes.

   **9a** In **Search Path** select **Custom Path**.

   **9b** Click **+**.

**9c** From the **Available Directory Domains**, select **/Kanaka/Auth**.
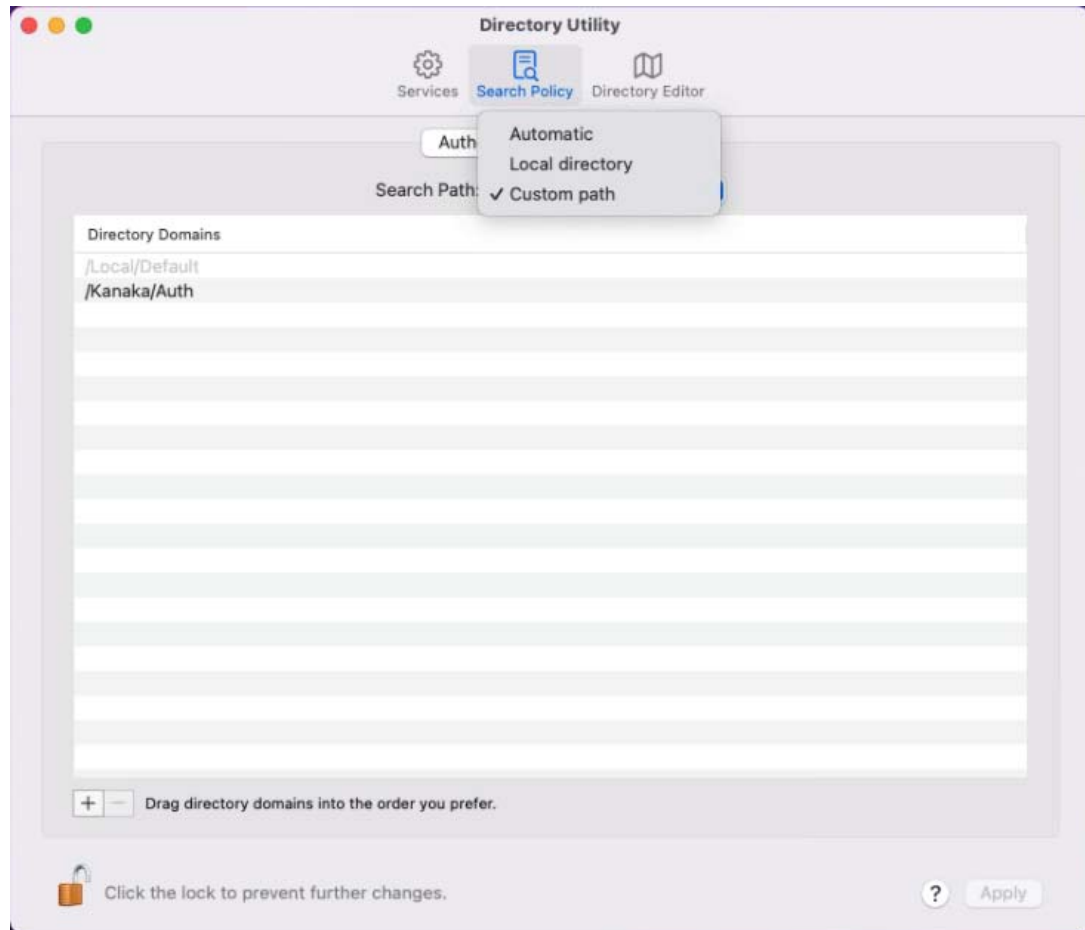


**10** Click **Apply** and close the Directory Utility.

The Kanaka Plug-in should now be available for use.

## 6.4 Installing the Kanaka Desktop Client

The Kanaka Desktop Client is designed to be a post-login window authentication client. Typical use is for users at home who log in to a local machine, use a VPN to their place of work, then use the client to authenticate to their eDirectory tree and access their home directories and group directories.

**1** Double-click the `MicroFocus_Kanaka_for_Mac-3.2.0.dmg` file.

**2** Drag the **Kanaka Client** icon over to the **Applications** icon.

# 7 Using the Kanaka Plug-In

To use the Kanaka Plug-in, simply log in as an eDirectory user. Kanaka provides contextless login, so just the common name of the user is needed. After login, the user's home directory is mounted and a link is placed in the Dock or the mount point is displayed on the desktop, depending on the Kanaka Policy configuration (see Section 11.5, "Policy," on page 66 for more details). Kanaka also discovers and mounts group shared storage and places it in the Dock or on the desktop depending on the Kanaka Policy configuration.

*Figure 7-1*  *macOS Dock with the Kanaka Plug-in and Mounted Network Home Directory Displayed*



In the graphic above, the network home directory is mounted and is displayed with a network icon, which varies in appearance based on the version of macOS. All of the shared directories to which the user has access are placed on the Dock next to the home folder icon. The Kanaka Plug-in Console provides users identity information, current quota details, and the ability to change the eDirectory password.

*Figure 7-2*  *The Kanaka Plug-in Console Displays Identity Information*
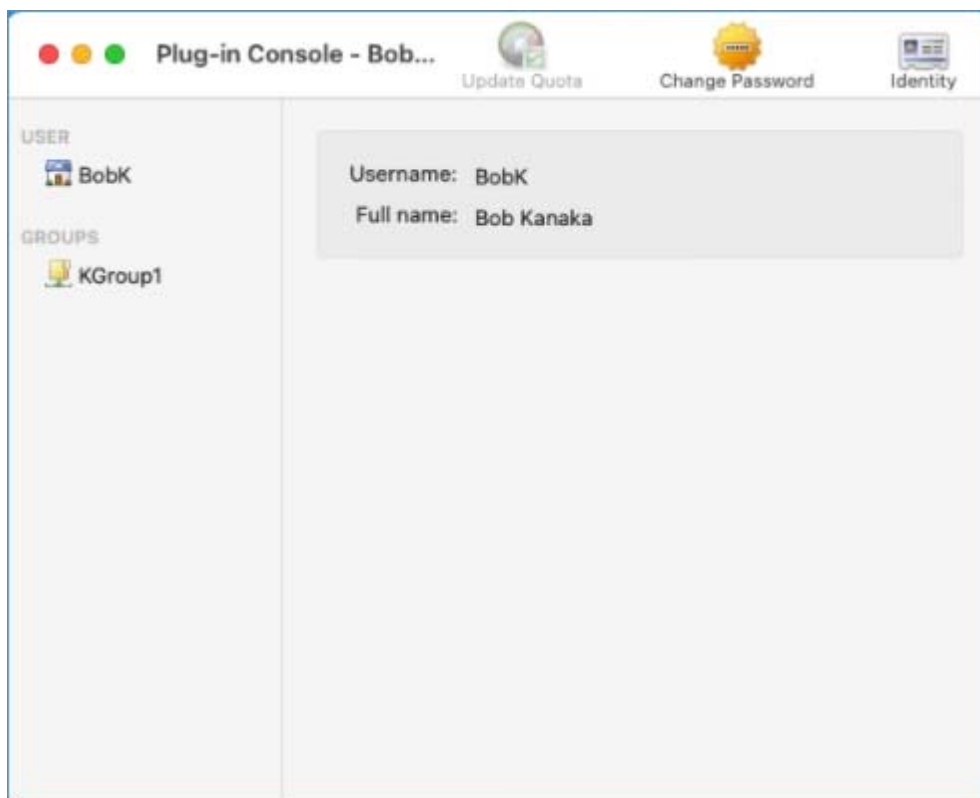
*Figure 7-3*  *The Kanaka Plug-in Console Allows Password Management*
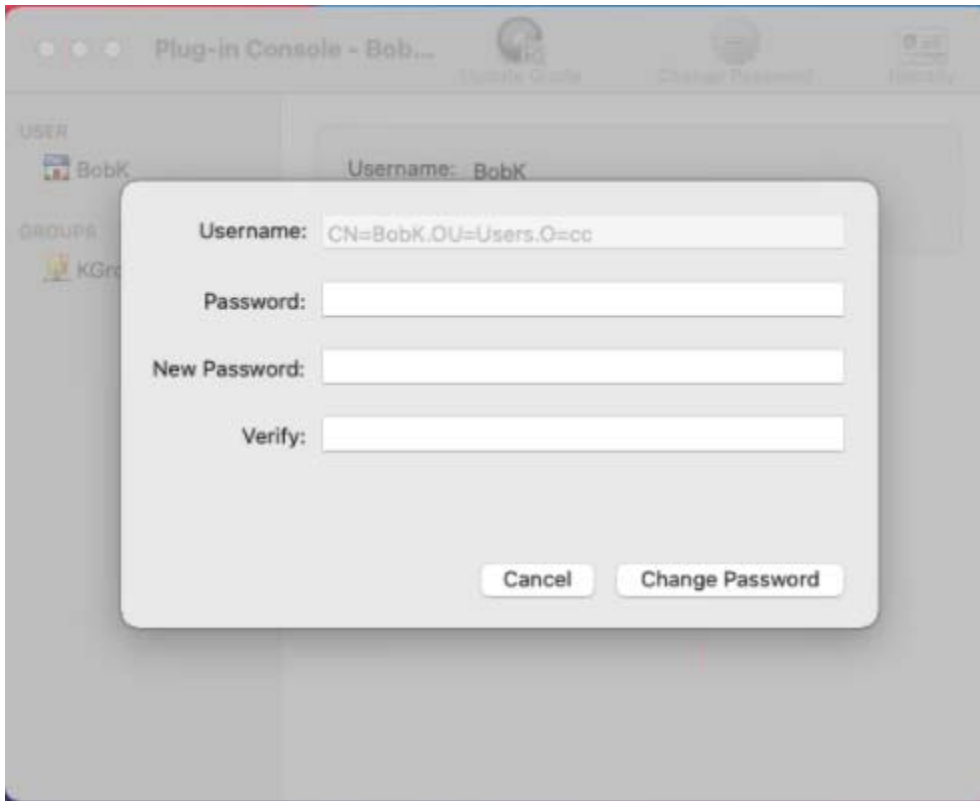


*Figure 7-4*  *The Kanaka Plug-in Console Displays Storage Capacity Information*
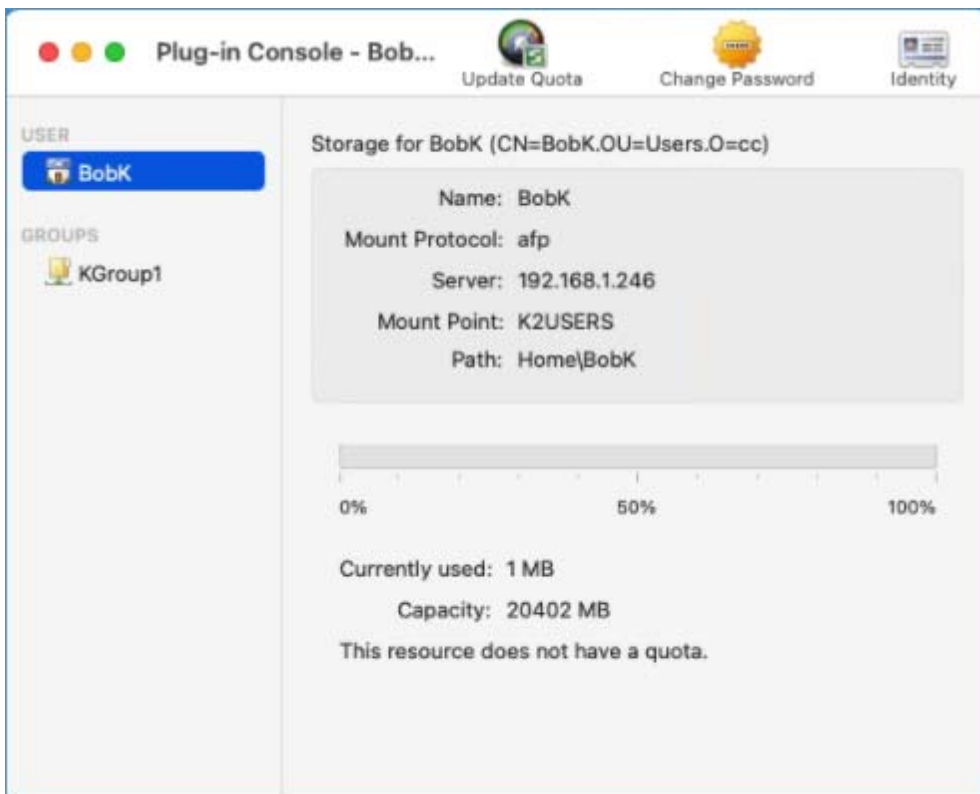
# 8 Using the Kanaka Desktop Client

## 8.1 Authentication

To use the Kanaka Desktop Client, simply open the Applications folder and double-click the Kanaka Desktop Client icon.

*Figure 8-1*   *The Kanaka Desktop Client Icon*



You are prompted to authenticate.

*Figure 8-2*   *Desktop Client Login*
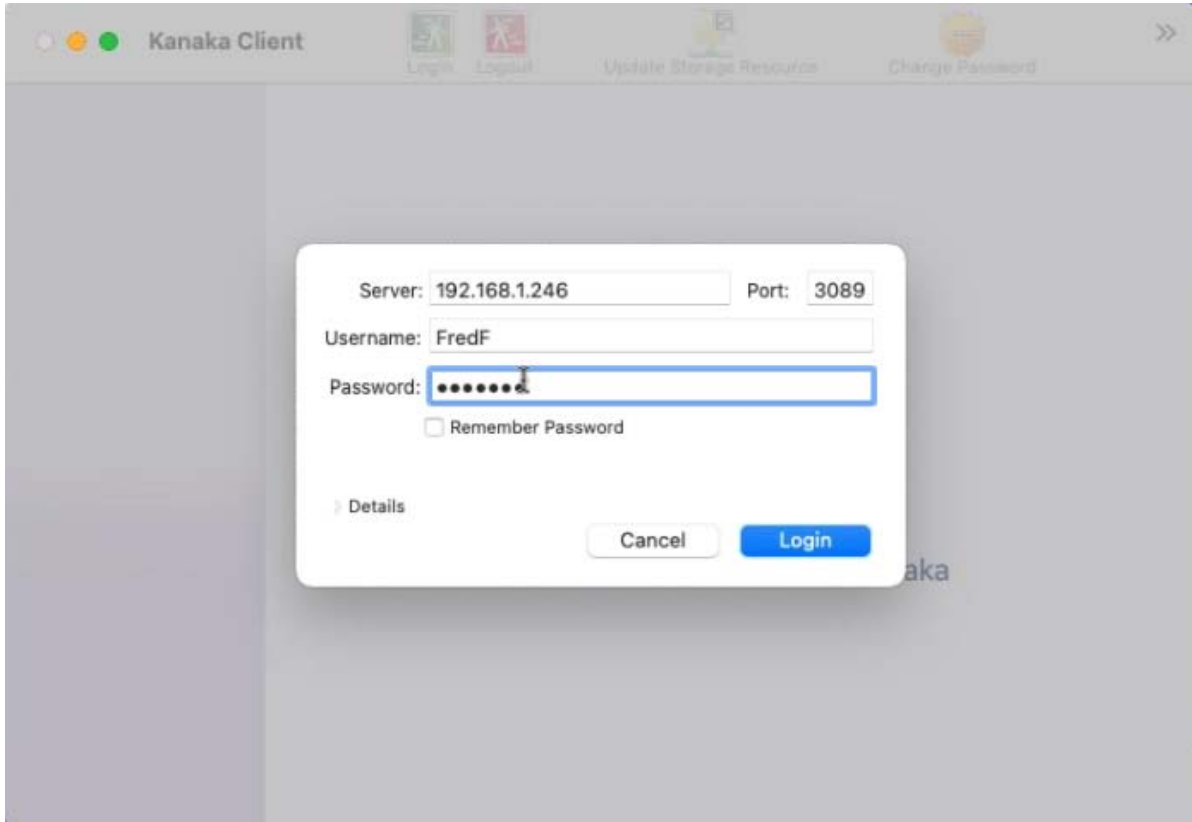


Use your contextless eDirectory credentials.

## 8.2    Storage Properties

Click the home folder to change to the Storage Properties page.

*Figure 8-3*  *Kanaka Desktop Client Property Page*
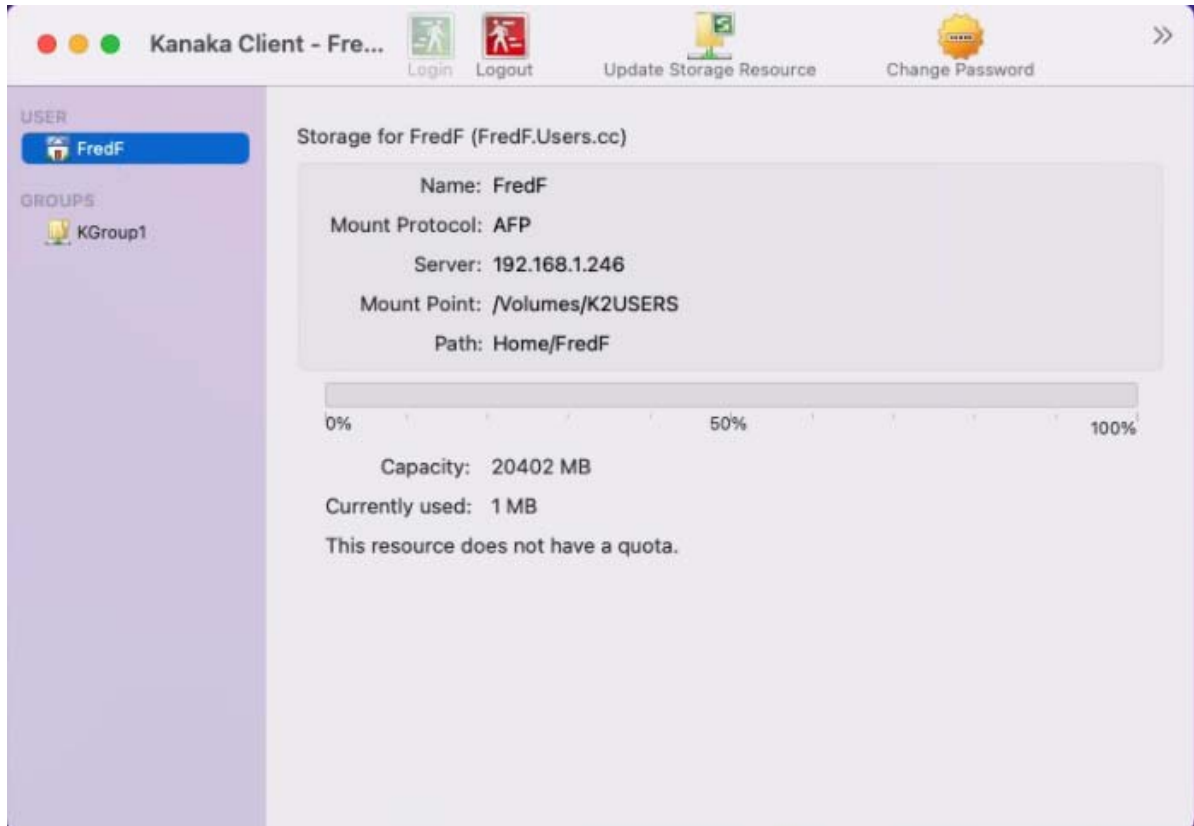


## 8.3    Home Directory

Double-click the home directory icon to view, browse, and access the contents of the directory.

*Figure 8-4*  *Kanaka Desktop Client Displaying Home Directory Contents*
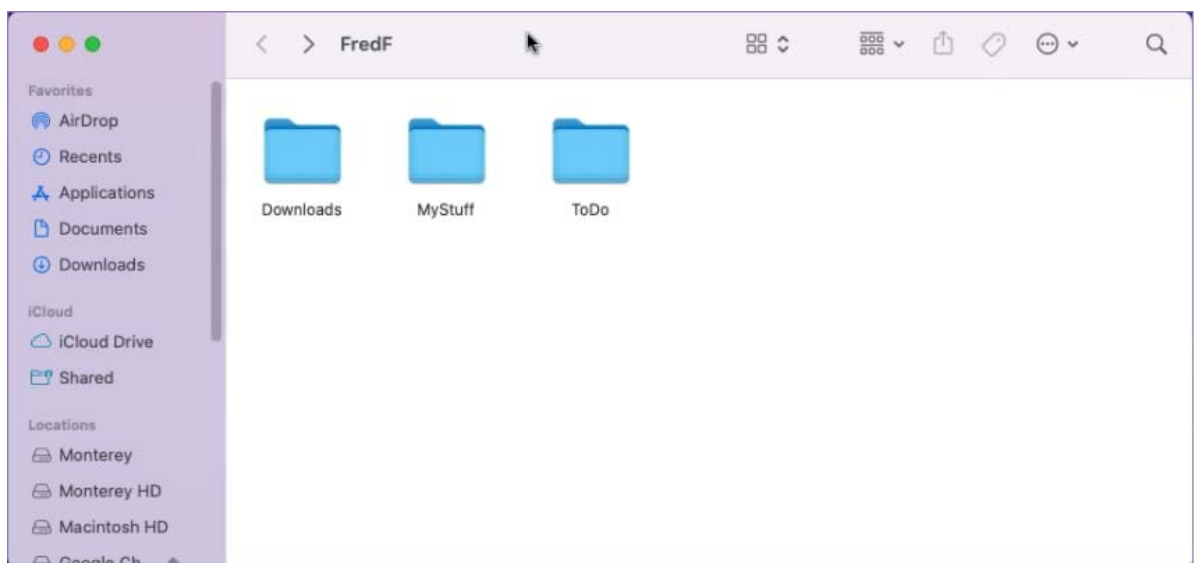
# 9 eDirectory Password Expiration

- Section 9.1, "Kanaka Plug-In," on page 53
- Section 9.2, "Kanaka Desktop Client," on page 55

## 9.1 Kanaka Plug-In

When your eDirectory password expires and you have the Kanaka Plug-in installed on your Mac, you are prompted at login time to change your password. Micro Focus Kanaka for Mac does not honor grace logins set by ConsoleOne or Universal Password policies, and requires you to enter a new password immediately.

*Figure 9-1*   *Kanaka Plug-in Password Change Dialog Box*

## 9.1.1 Kanaka Plug-In Console

While you are logged into the network, the Kanaka Plug-in Console periodically checks for your password to expire and provides a warning beginning at five days before it expires.

*Figure 9-2*  *Kanaka Plug-in Console with Password Expiration Information*
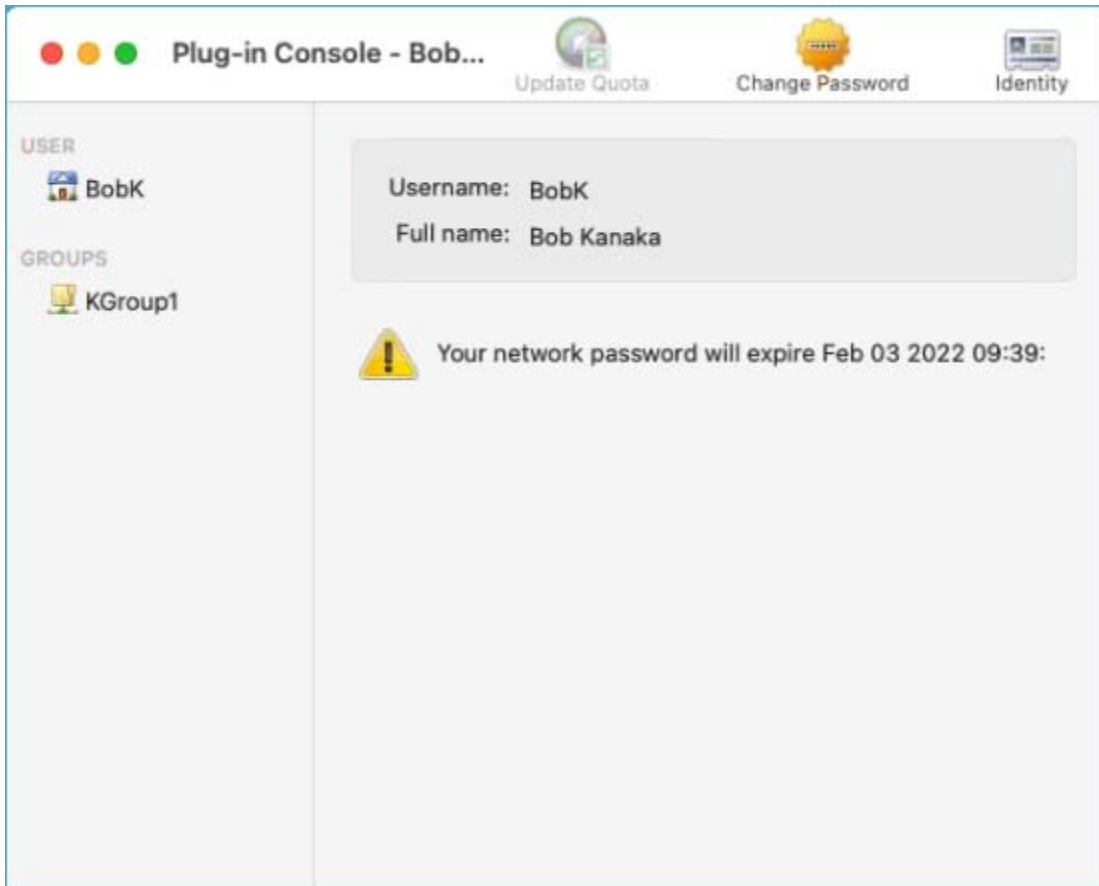


To change your password, click **Change Password** in the toolbar.

*Figure 9-3*  *Change Password Dialog Box*

## 9.2 Kanaka Desktop Client

During login, the Kanaka Desktop Client prompts you to change your password if it has expired. Micro Focus Kanaka for Mac does not recognize grace logins.

*Figure 9-4*  *Password Error*
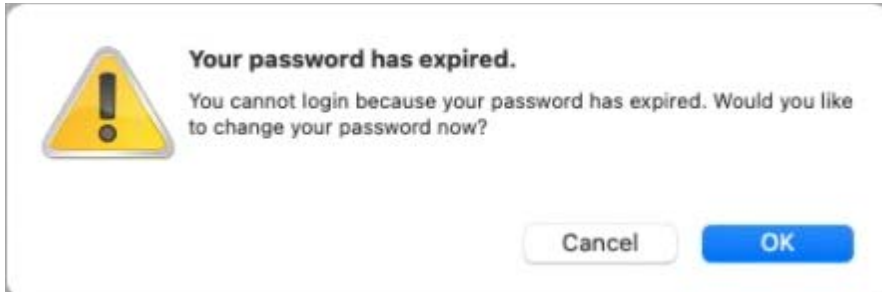


After you change your password, use the new password to log in.

# 10 Parsing eDirectory Login Scripts

Since the release of Version 2.7, Micro Focus Kanaka for Mac can parse eDirectory login scripts and mount the storage for access from the Kanaka clients.

For information on eDirectory login scripts, refer to the *Novell Login Scripts Guide* (http://www.novell.com/documentation/linux_client/login/?page=/documentation/linux_client/login/data/ak1lvlq.html). Additional documentation is available from  (http://www.novell.com/support/kb/doc.php?id=10068983).

## 10.1 Login Script Overview

A login script is a set of instructions that is executed when a user logs in using the OES Client for Windows, the OES Client for Linux, or some other method of login that accesses eDirectory object properties. A login script is simply a text file that the login executable interprets and runs line by line.

When a user successfully logs in to the network, one or more login scripts can be executed that automatically set up the workstation environment.

Login scripts are similar to batch files and are executed by the OES LOGIN utility.

You can use login scripts to map drives and search drives to directories, display messages, set environment variables, and execute programs or menus.

Login scripts are properties of specific eDirectory objects.

There are four types of login scripts:

- **Container:** Sets the general environments for all users in that container. Container login scripts are executed first and can be associated with organization or organizational unit objects. A user can use only one container login script.

- **Profile:** Sets environments for several users at the same time. Profile login scripts are executed after the container login script and are associated with Profile objects. A user can be assigned only one profile login script that is then associated with the user object in eDirectory. However, other profile login scripts can be assigned by using the PROFILE command in the login script or by selecting a different Profile login script from the OES Login window.

- **User:** Sets environments (such as printing options or an e-mail username) specific to a single user. User login scripts are executed after any container and profile login scripts and are associated with user objects. A user can have only one user login script. However, the User login script can be overwritten by selecting a different login script from the OES Login window.

- **Default:** Contains only essential commands, such as drive mappings to certain utilities, and cannot be edited. The default login script runs if a user (including user Admin) doesn't have a user login script, even if a container or profile login script exists.

**NOTE:** If you don't want to create any user login scripts and you don't want the default login script to execute for any users, you can disable the default login script by including the NO_DEFAULT command in the container or profile login script.

Maintaining many user login scripts can be time consuming. Therefore, you should try to include as much customization information as possible in the container and profile login scripts, which are fewer in number and easier to maintain.

For example, if all users need access to particular utilities in the same volume, put the search drive mapping to that volume in a single container login script rather than in every user login script.

Create profile login scripts if several users have identical login script needs. Profile login scripts are sometimes thought of as group login scripts.

Finally, in user login scripts, include only those individual items that can't be included in profile or container login scripts. For example, personal drive mappings could be included in the user login script.

**IMPORTANT:** Because three or more login scripts can execute whenever a user logs in, conflicts can occur and drive mappings can be overwritten by consecutive login scripts. The last login script to execute (usually the user login script) overrides any conflicting commands in a previous login script.

## 10.2 Login Script Sample

The login script consists of any statements available to NetStorage. In addition, you can use the following statement:

```
IF <KANAKA> = "1" THEN
MAP *
MAP *
END
```
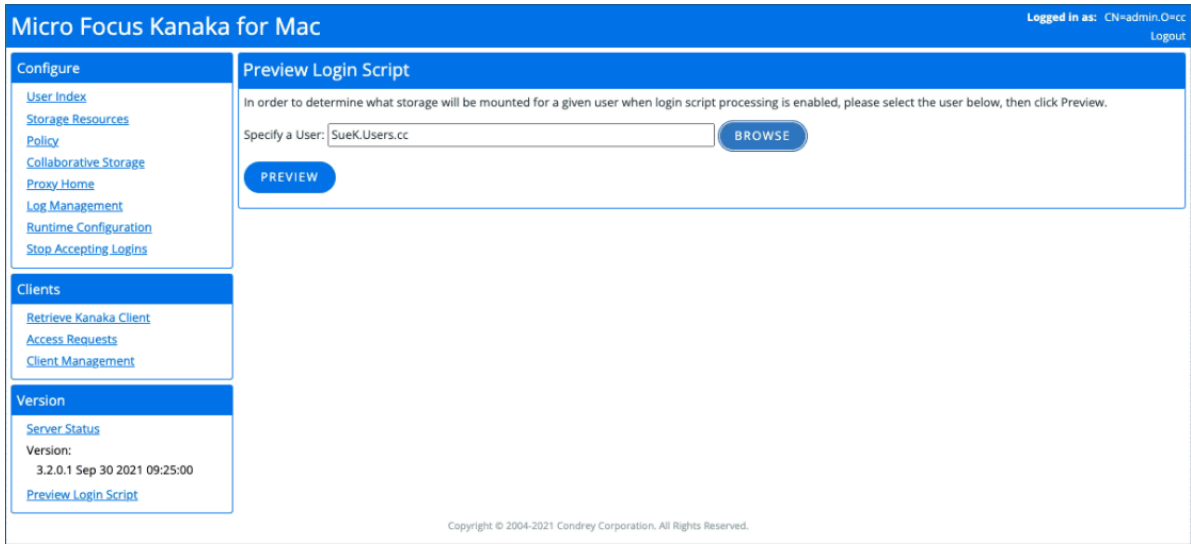
This section of the login script is always processed by Micro Focus Kanaka for Mac.

**Figure 10-1** *Sample Login Script with Mount Instructions for Kanaka for Mac*
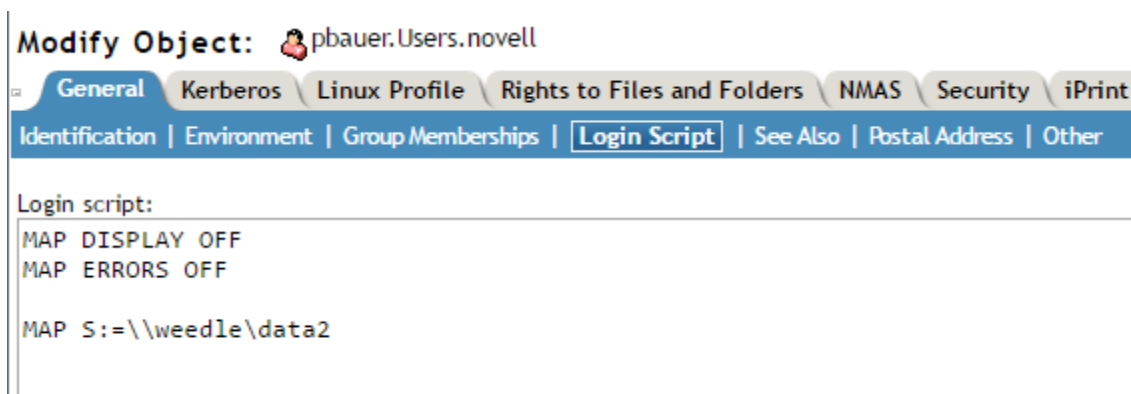


When you preview the login script parsing from the Kanaka User Interface, you see all the drive mappings that will occur for any particular user.

*Figure 10-2*   *Preview Login Script*

# 11 Reference

## 11.1 Storage Resources

CIFS requires that each volume be given a specific CIFS virtual server name. By default, this name follows the convention *SERVERNAME*. In addition, the volume must be shared with a particular name. By default, all volumes are shared as their volume name (such as SYS or VOL1). However, these are simply default names and you can name the volumes anything you want. Also, CIFS share and volume information is not stored in eDirectory, but in CIFS-related files.

If only one protocol is configured, it is listed as the access method in the **Client Access Protocol** column of the Storage Resources list. If both protocols are configured, one access protocol is indicated as the selected protocol, and the option to change to the other is indicated in the same field.

Kanaka clients connect to the Kanaka Engine to retrieve volume and path information that can then be used to mount both user home directories and collaborative (group) storage located on file servers.

In order for Micro Focus Kanaka for Mac to convert a standard path into its AFP equivalent path, it must know the AFP volume name. Therefore, eDirectory must hold a copy of the AFP volume name. One of the Micro Focus Kanaka for Mac schema extensions is an attribute added to the VOLUME object class that allows you to store the AFP volume name along with the volume itself. The Kanaka eDirectory configuration interface adds the schema extensions and provides the Web-based user interface that allows you to set the attribute accordingly.

In order for Micro Focus Kanaka for Mac to convert a standard OES path into its CIFS equivalent path, it must know the CIFS virtual server name and shared volume names. Therefore, eDirectory must hold a copy of the CIFS virtual server name and shared volume names. One of the Micro Focus Kanaka for Mac schema extensions is an attribute added to the VOLUME object class that allows you to store the CIFS virtual server name along with the shared volume name itself. The Kanaka eDirectory Configuration Interface adds the schema extensions and provides the Web-based user interface that allows you to set the attribute accordingly.

Before the Kanaka Plug-in or Kanaka Desktop Client can mount a volume, the AFP/CIFS volume name must be stored in eDirectory for each volume on each server that a Kanaka-based client might want to connect to. This includes servers holding user home directories as well as servers holding collaborative storage.

In setting up the Storage Resource list, access can be provided through either AFP or CIFS/SMB. If both are configured, either one can be selected as the access method for a given volume.

As part of the configuration of Native File Access protocols, Apple Filing Protocol (AFP) must be configured for each server and volume. AFP requires that each volume be given a specific name. By default, this name follows the convention *SERVER_NAME.VOLUME_NAME*. However, these are simply default names and you can name the volumes anything you want. Also, the AFP volume information is not stored in eDirectory, but in AFP-related files. You can rename how the AFP volume is displayed with the appropriate AFP volume configuration file (for example, `/etc/opt/novell/afptcpd/afpvols.conf`).

---

**IMPORTANT:** OES 2023 does not support AFP directly, but if the configured storage server is running on an older OES version that does support AFP, Kanaka will still continue pass the configured AFP based path information to the Plug-in and Client.

---

# 11.2   Cluster Volumes

To attach to a cluster volume, you need to set an alias in the `afpvols.conf` file in the `/etc/opt/novell/afptcpd` directory. The contents of the file follow.

```
This file describes information required to rename and export NSS volumes
through the AFP server. If the EXPORT_ALL_VOLUMES configuration option is
set to Yes, the information provided in this file is not used to export
volumes through AFP server. The information provided is used only to rename
AFP volumes.

Syntax:

CURRENT_NAME [new_vol]

where

CURRENT_NAME is the volume name as seen on the Finder in Mac. new_vol is
the new volume name.

Use a new line for each volume to be renamed.

Example 1: export data volume on server

serverA.data

Example 2: rename img volume on serverA to Graphics

serverA.img Graphics

Renaming volumes for clusters:

All shared volumes in a cluster needs to be renamed to the same volume name
in order for a cluster to be transparent to the user. For example, if your
cluster has 2 servers serverA and serverB and they share 2 volumes, vol1
and vol2, then each server needs to have an afpvols.conf file that renames
the volumes to a common volume name that the user will see in the Finder.
Then the AFP user will use the same volume name to mount the shared volume
and will not know or care whether it's using serverA or serverB.
```

```
Example 3: Renaming cluster volumes

afpvols.conf for serverA:

serverA.vol1 sharedVol1

serverA.vol2 sharedVol2

afpvols.conf for serverB

serverB.vol1 sharedVol1

serverB.vol2 sharedVol2
```

# 11.3 Collaborative Storage

Micro Focus Kanaka for Mac has the capability to automatically mount collaborative (group) storage on macOS. It does this based solely on the identity of the user. Micro Focus Kanaka for Mac uses the Home_Directory attribute, and now the login script attribute, to locate and mount the storage.

The concept of using the Home_Directory attribute to manage group storage originated with Micro Focus Storage Manager, which is a policy-based storage-management solution that revolutionizes use of the OES file system. Micro Focus Storage Manager unites the user-provisioning functionality of eDirectory solutions with the storage-provisioning capabilities of the OES file system. As a result, Micro Focus Storage Manager completely automates the creation, management, and deletion of personal and collaborative storage, delivering the industry's only identity-based storage management solution.

Micro Focus Storage Manager extends the Home_Directory concept to the group by adding a ccx-FSFManagedPath attribute to the group object. Therefore, much like a single user's home directory, it is easy to locate the storage for the group simply by looking at the ccx-FSFManagedPath attribute of the group.

Micro Focus Kanaka for Mac leverages the Home_Directory attribute of the user object to locate and mount the home directory for the given user. Micro Focus Kanaka for Mac also leverages the group home directory concept introduced by Micro Focus Storage Manager by running the group membership list for the user and pulling the ccx-FSFManagedPath attribute for each group the user is a member of and mounting each group directory on macOS.

However, Micro Focus Storage Manager is not required for Micro Focus Kanaka for Mac to deal with collaborative (group) storage. When the Micro Focus Kanaka for Mac schema extensions are applied to the tree, the Micro Focus Storage Manager ccx-FSFManagedPath attribute is also added, if it is not already present. This Web interface provides a methodology for assigning the group ccx-FSFManagedPath attribute for each group in the tree, analogous to setting the Home_Directory attribute on a user.

If all group storage is already managed with Micro Focus Storage Manager, there is nothing that you need to do for Micro Focus Kanaka for Mac to mount group storage for all users. Otherwise, you should use Micro Focus Kanaka for Mac to assign the ccx-FSFManagedPath attribute for each group that is not managed by Micro Focus Storage Manager. Simply click **Browse the Tree** in the menu to the left, locate the group, and click **Assign**. This allows the administrator to browse to a destination path and set the attribute for the given group.

**IMPORTANT:** The Engine does not assign the chosen object as a trustee of the directory. You should perform this step via traditional methods.

*Figure 11-1*   *Assigning the Home Directory Attribute to a Group*
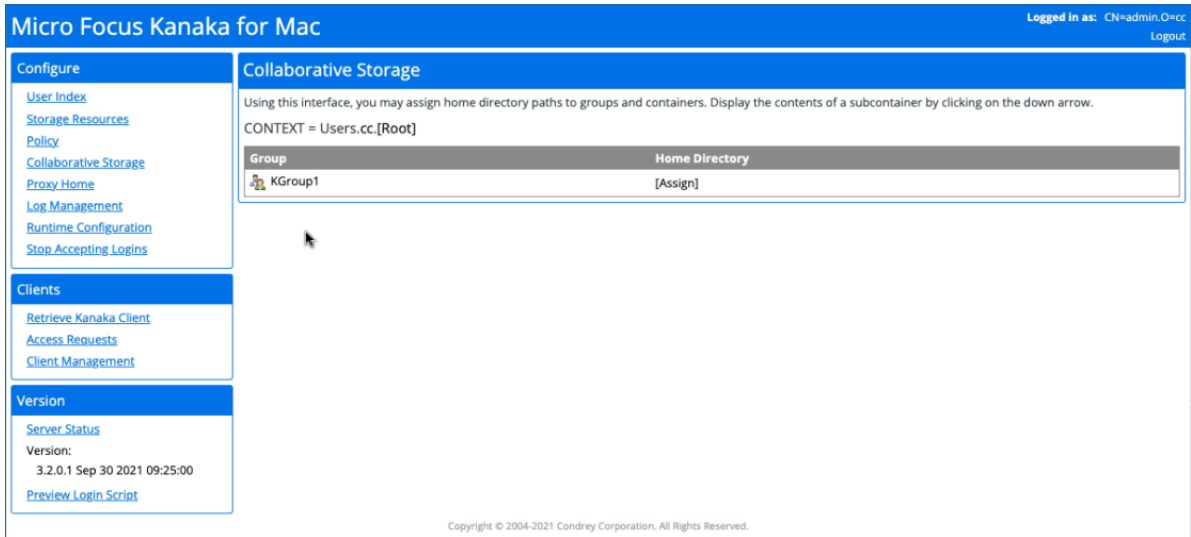


*Figure 11-2*   *Specifying a Group Directory Path*
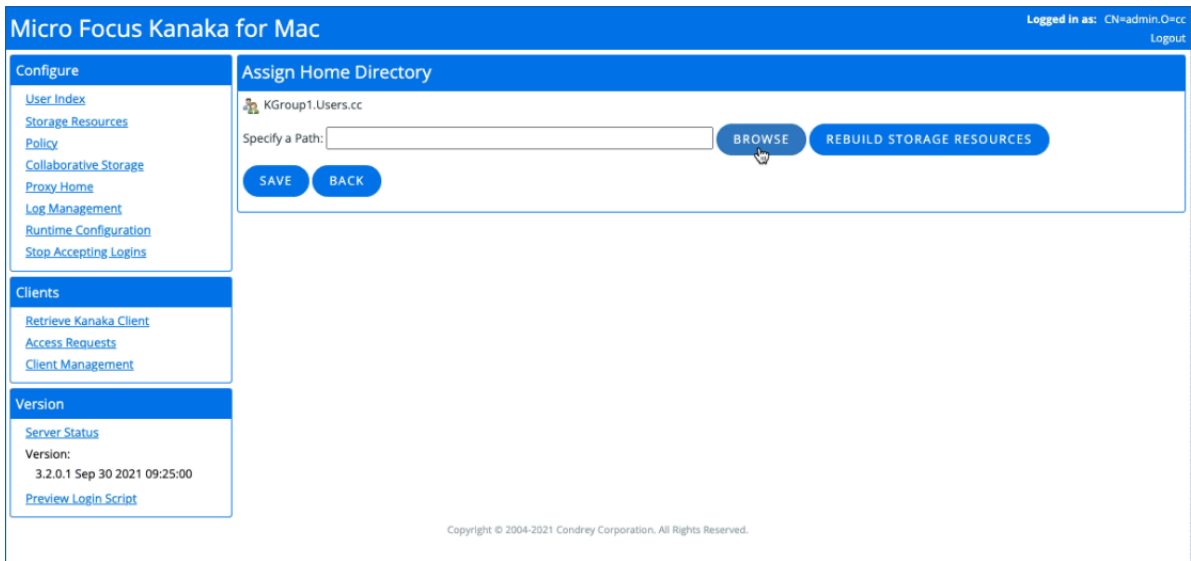
**Figure 11-3**   *Assigned Group Directories*
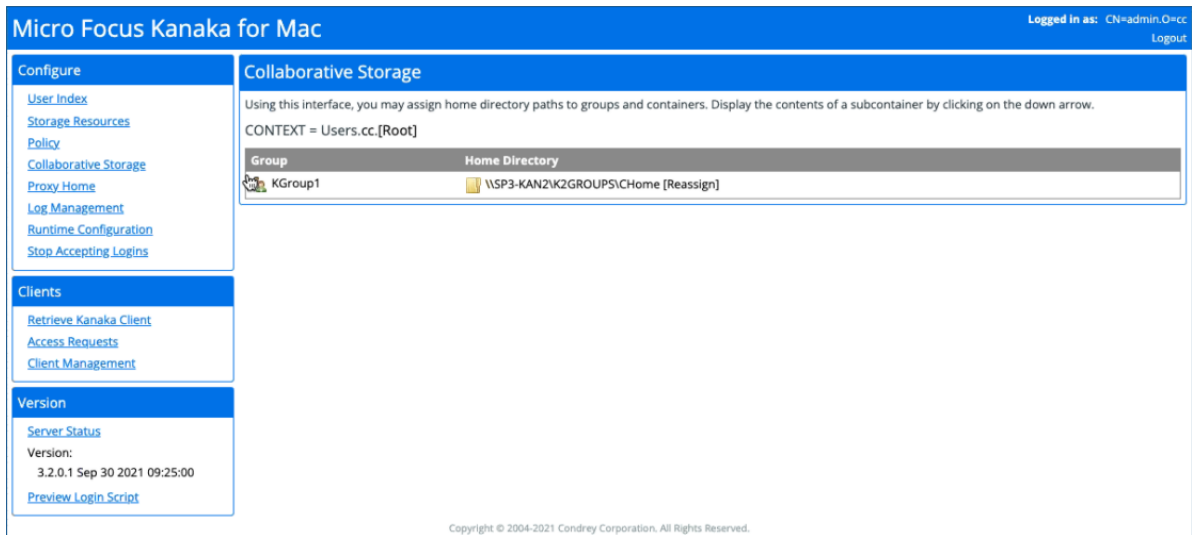


# 11.4 Proxy Home

Proxy home directories are useful in helping to avoid user problems logging in because of incorrectly assigned home directories and incorrectly managed volumes.

If a home directory is not provided as a part of the login process, macOS fails the login.

However, Micro Focus Kanaka for Mac can communicate to the user (and the administrator) and indicate the reason why the login is failing. A proxy home directory is passed back to the client for mounting when mounting the "real" home directory is not possible for some reason.

The proxy directories are managed in the Web management interface for Micro Focus Kanaka for Mac at `https://server_ip_or_DNS_name:3089`

**IMPORTANT:** It is very important for the volume of the server where the Kanaka Engine is running to have the Micro Focus Kanaka for Mac volume name configured so that all users can reference it.

*Figure 11-4* *Change Proxy Home Page*
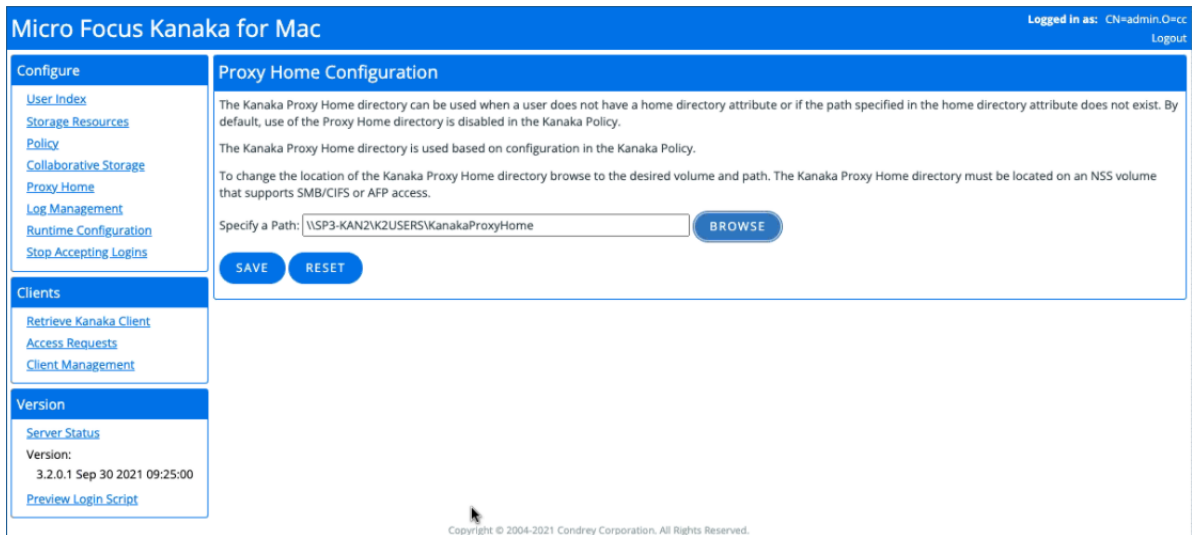


## 11.5 Policy

There are several options available in Micro Focus Kanaka for Mac to direct the behavior of the client. These options offer some flexibility in the setup to allow a more customized fit for individual installations. There are options for User Management, and for Managed Client Settings.

- ◆ Section 11.5.1, "User Management," on page 67
- ◆ Section 11.5.2, "Managed Client Settings," on page 71

# 11.5.1    User Management

*Figure 11-5*   *User Management Page*



Micro Focus Kanaka for Mac clients request various items of user-related information from eDirectory. The following options allow you to configure how these items are obtained as well as the operation of the clients themselves.

*Figure 11-6*   *Password Management Settings*



These two self-explanatory settings are selected by default.
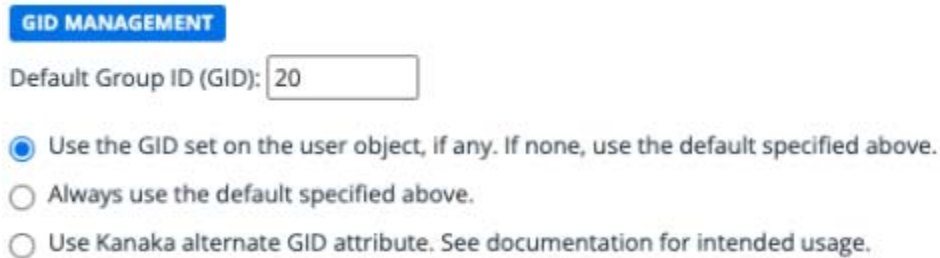
*Figure 11-7*   *UID Management Settings*

The UID is a User ID that is unique for each user logging in to macOS. This option allows you to use an existing number or use a randomly generated number from a range of numbers defined by Micro Focus Kanaka for Mac.

The auxiliary attribute class is posixAccount. The attribute is uidNumber.

*Figure 11-8*  *GID Management Settings*



The GID is a primary Group ID for a user. It defines security levels on macOS. By default, the GID is set to 20 (equivalent to "staff" on macOS) in Micro Focus Kanaka for Mac. If you want your users to have admin privileges on macOS, you can set the GID to 80 (equivalent to "admin" on macOS), but this is not recommended for lab environments. The auxiliary attribute class is posixAccount. The attribute is gidNumber.

The third option is based on an extended attribute that is added during the Kanaka installation. The class in eDirectory is named cccKanakaGidNumberClass and the attribute name is cccKanakaGidNumber. You can use this attribute to define the GID for users individually.
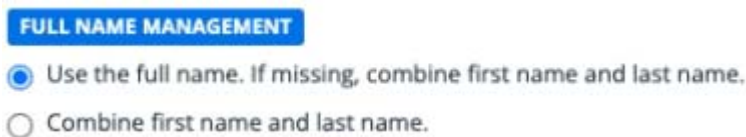
For example, if you want students to have a GID of 20 (staff) and teachers or administrators to have a GID of 80 (admin), you can set the cccKanakaGidNumber attribute for the teachers or administrators to a value of 80 and choose the **Use Kanaka alternate GID attribute** option.

*Figure 11-9*  *Full Name Management Options*



This region lets you specify how the user's name is displayed in the Kanaka Plug-in Console, Desktop Client, and the logout option.

*Figure 11-10*  *Home Directory Management Settings*

This setting gives you the option to allow the user to log in or not if the Home Directory attribute is not populated. If you choose the proxy directory option, you need to add and configure a proxy home directory for your environment. This is a directory with limited rights, and you can display a message to explain (such as a document or HTML page) that the user does not have a home directory defined, and perhaps direct them to a contact at the Help Desk.
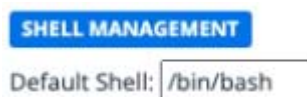
*Figure 11-11*

If the path specified in the home directory does not exist:

- ● Do not test for existence. (best performance)
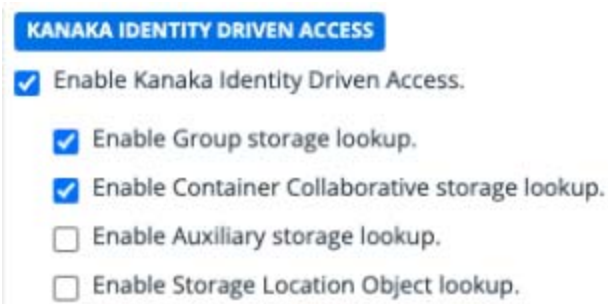- ○ Use a proxy directory.
- ○ Deny login.

This setting indicates whether Micro Focus Kanaka for Mac should actually test for the existence of the path specified in the home directory attribute. By default, this option should be turned off. If you do test for existence and the path doesn't exist, you have the option to use the proxy directory or deny login.

*Figure 11-12*  *Shell Management Setting*

**SHELL MANAGEMENT**

Default Shell: /bin/bash

This is the default shell for the user's environment on macOS.

*Figure 11-13*  *Identity Driven Access Settings*

**KANAKA IDENTITY DRIVEN ACCESS**

☑ Enable Kanaka Identity Driven Access.

☑ Enable Group storage lookup.
☑ Enable Container Collaborative storage lookup.
☐ Enable Auxiliary storage lookup.
☐ Enable Storage Location Object lookup.

These settings enable the mounting of additional storage other than the user's home directory.

**Enable Kanaka Identity Driven Access:** Selecting this option enables you to select the options below.

**Enable Group storage lookup:** During the installation of Micro Focus Kanaka for Mac, group objects are extended with an attribute called ccx-FSFManagedPath. In its simplest explanation, it is analogous to having a home directory attribute on a group object.

**Enable Container Collaborative storage lookup:** Container objects can also be extended with an attribute named ccx-FSFManagedPath. In its simplest explanation, it is analogous to having a home directory attribute on a container object. It treats users in a container as if they were members of a group, without having to manage a group object for those users.

**Enable Auxiliary storage lookup:** This option works only when you have Micro Focus Storage Manager implemented with Auxiliary storage defined and enabled. Auxiliary Storage is like having multiple home directory attributes.

**Enable Storage Location Object lookup:** These are traditional Storage Location Objects in eDirectory. Micro Focus Kanaka for Mac supports only NCP Storage Location Objects.

*Figure 11-14* *Login Script Settings*
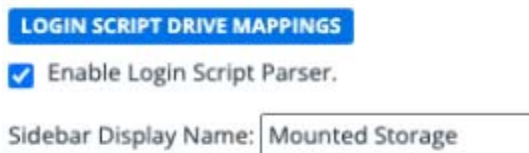


By enabling the Login Script Parser, the Kanaka Engine will parse any login scripts associated with the user. Login scripts are parsed with the same criteria as NetStorage logins.

*Figure 11-15* *Mounted Storage*
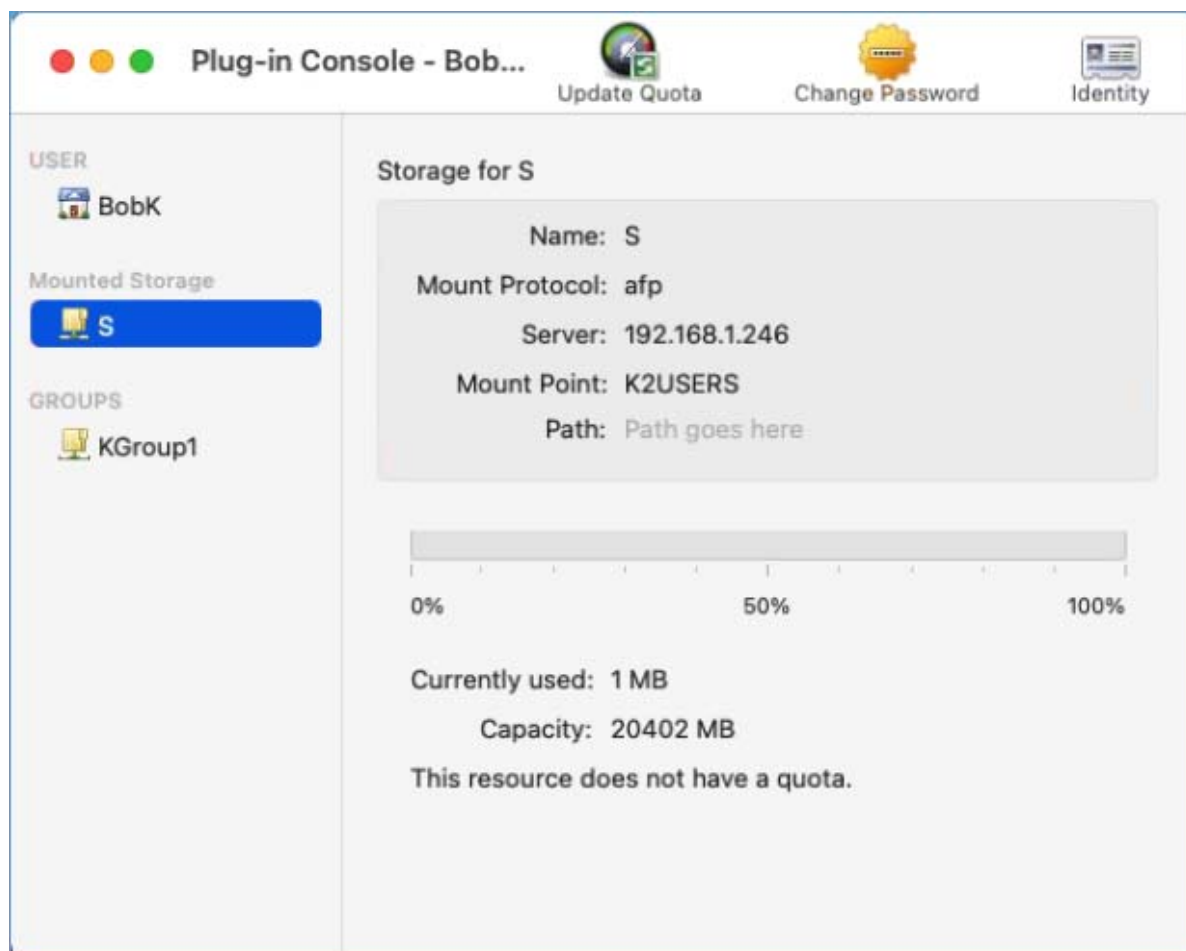
## 11.5.2 Managed Client Settings

For several years, Apple has had a technology for managing workstations and the user experience, often referred to as MCX, or Managed Client for OS X via a Workgroup Manager server. Micro Focus Kanaka for Mac gives the administrator the ability to choose between Micro Focus Kanaka for Mac or a Workgroup Manager server to deliver these settings to the workstation.

*Figure 11-16*   *Managed Client Settings Page*



Micro Focus Kanaka for Mac clients can receive Managed Client Settings (MCX) configured in the Kanaka policy or from a properly configured OS X server. The following options instruct the client to use MCX settings generated by Micro Focus Kanaka for Mac or to use settings obtained from an OS X server.

*Figure 11-17*   *MCX Settings*



If you choose the setting for Workgroup Manager, you will need to verify that your LDAP v3 settings in the macOS Directory Utility point to that server.
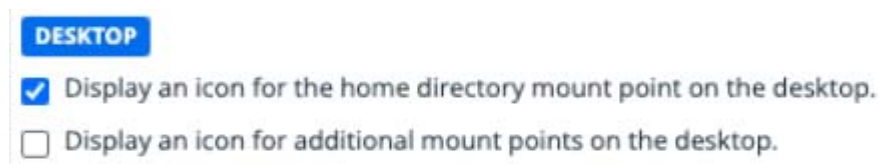
*Figure 11-18*   *Dock Settings*

This option displays an icon on the Dock for the user's home directory and for any additional storage that is configured.

*Figure 11-19*  *Desktop Settings*



These options place a mount point on the user's desktop. This mount point is at the root of the volume, so users will need to drill down to get to the folders and files they have rights to.

---

**NOTE:** Users can only see folders and files to which they have rights.

---

*Figure 11-20*  *Kanaka Plug-in Console Setting*



This setting enables the Kanaka Plug-in Console to automatically start after a login.

*Figure 11-21*  *Mobility Settings*



**Create mobile account at login:** This setting will allow a local "mobile" account to be created on the workstation and will keep the user's profile and other information local. Prior to macOS11, network home directories were maintained only on the network volumes if this option was not checked. The Kanaka 3.2 client and macOS11 require this option to be checked. If this server is being used with older Kanaka and macOS clients, whether to create a local "mobile" account is optional. This option has the most performance benefits because it can read the profile locally much more quickly than from the network. If you do not create a mobile account, the user profile information is created in the user's home directory on the network.

**Require confirmation before creating mobile account:** Warns the user of a mobile account that is created during login.

# A  Documentation Updates

This section contains information about documentation content changes that were made in what is now titled the *Micro Focus Kanaka for Mac Installation and Administration Guide*. The changes are listed according to the date they were published.

The documentation for this product is provided on the Web in two formats: HTML and PDF. The HTML and PDF documentation are both kept up-to-date with the changes listed in this section.

If you need to know whether a copy of the PDF documentation that you are using is the most recent, the PDF document includes a publication date on the title page.

The documentation was updated on the following dates:

## A.1  November 14, 2022

| Location | Update |
|---|---|
| Various chapters. | Referenced lack of OES 2023 direct support for AFP. |
| Section 3.1, "Enabling File Protocols," on page 17. | Retitled section. |
| Section 3.5.3, "Convert a PKCS#12 Certificate to a PEM Certificate," on page 23. | Updated terminal commands. |
| Section 4.2, "Performing the Upgrade," on page 29. | Updated terminal commands. |
| Section 11.5.2, "Managed Client Settings," on page 71. | Removed reference to Create home using network home with default sync settings, which was removed in version 3.2.0. |

## A.2  September 4, 2020

Updates were made to the following sections:

| Location | Update |
|---|---|
| Section 3.6, "Add a Firewall Exception (Conditional)," on page 28. | New section. |
| "microfocus-kanakaengine-convertcert" on page 23. | Replaced incorrect commands with corrected ones. |
| "Manual" on page 23. | Replaced incorrect commands with corrected ones. |
| Section 5.2, "Installing the Kanaka Engine," on page 32. | Updated procedures. |