Progress®
Kemp® LoadMaster®

# Feature Description User Management

Generated on: 16 September 2024

# Copyright

**Visit the following page online to see Progress Software Corporation's current Product Documentation Copyright Notice/Trademark Legend:** Product Documentation Copyright Notice & Trademarks | Progress

# Table of Contents


## Chapter 1: Introduction . . . . . 5

Document Purpose . . . . . 5

Intended Audience . . . . . 6

## Chapter 2: User Management . . . . . 7

The Default Administrator User (bal) . . . . . 7

Set the Minimum Password Length . . . . . 8

Create a New User . . . . . 8

Modify an Existing User . . . . . 9

User Permissions . . . . . 10

Change a User's Password and WUI Authentication Method . . . . . 14

Session Management . . . . . 14

Other WUI Session Management Fields . . . . . 17

## Chapter 3: Client Certificate WUI/API Authentication . . . . . 19

Generate and Download Client Certificates . . . . . 20

Create the Personal Exchange Format (PFX) File . . . . . 21

Import the PFX File into the Microsoft Management Console (if using Windows) . . . . . 22

Enable Session Management . . . . . 30

Enable Client Certificate Authentication . . . . . 31

Enable the 'No Local Password' Option for Users . . . . . 32

Accessing the API with the Local Certificate . . . . . 33

## Chapter 4: WUI Authentication using LDAP Groups . . . . . 34

Add an LDAP Endpoint . . . . . 35

Create the Remote User Groups. . . . . 36
Select the Remote User Groups . . . . . 37

**Chapter 5: References . . . . . 40**

# 1

# Introduction

## Introduction

The LoadMaster supports multiple user logins with varying levels of access. Users can be managed by navigating to **System Configuration > System Administration > User Management** in the LoadMaster Web User Interface (WUI). Users created here can only access the LoadMaster using the WUI and Application Program Interface (API). Remote access via SSH is not supported for other LoadMaster users. The default administrator user (**bal**) can access the LoadMaster using SSH.

By default, WUI access is granted when users enter their username and password. The LoadMaster can also be configured to utilize RADIUS authentication and client certificate authentication for WUI access.

**Related Links**

- Document Purpose
- Intended Audience

# Document Purpose

## Document Purpose

This document provides an overview of user management, permissions, session management and client certificate WUI authentication.

# Intended Audience

## Intended Audience

This document is intended to be used by anyone interested in finding out more about managing users and WUI authentication in the LoadMaster WUI.

# 2

# User Management

## User Management

Refer to the sections below for details on some key aspects of user management and WUI authentication.

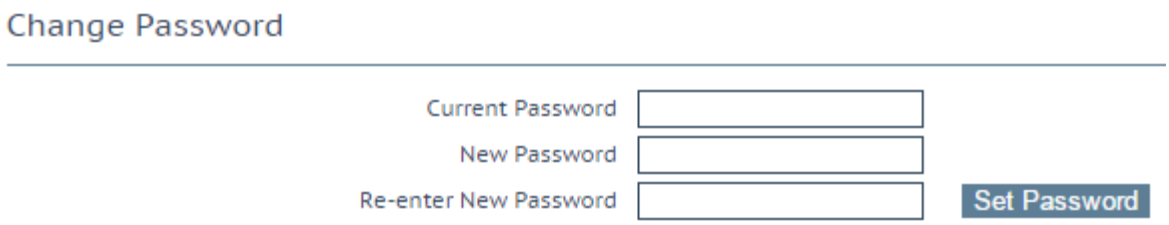
**Related Links**

- The Default Administrator User (bal)
- Set the Minimum Password Length
- Create a New User
- Modify an Existing User
- Session Management

# The Default Administrator User (bal)

## The Default Administrator User (bal)

The default administrator user on all LoadMasters is the **bal** user. The password for the **bal** user is set after initially configuring the LoadMaster using the WUI. Before initially setting the password, the default password for the **bal** user is **1fourall**. The **bal** user has the highest level of access in the LoadMaster. All other users created have only a subset of the access which the default account has. The **bal** user is the only user who can access the LoadMaster using SSH.




The password for the **bal** user can be changed in **System Configuration > System Administration > User Management**. The **bal** password can only be changed by the **bal** user.

# Set the Minimum Password Length

## Set the Minimum Password Length

You can set the minimum password length for local users by following the steps below:

1. In the WUI, go to **System Configuration > System Administration > User Management**.




2. Select the desired value from the **Minimum password length** field (this ranges from **8** to **16**).
3. Refresh the page.

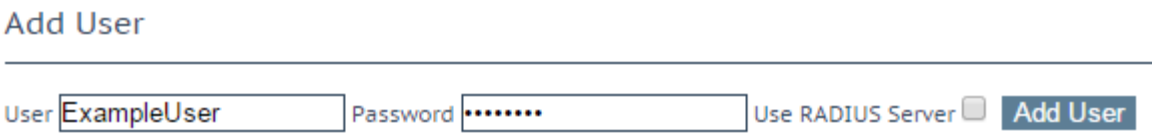
**Note:** After selecting a different value for this field, you must refresh the page for the new value to be enforced.

# Create a New User

## Create a New User

Other LoadMaster users can be created and provided with the necessary permissions. Follow the steps below to create a new LoadMaster user:

1. In the LoadMaster WUI, navigate to **System Configuration > System Administration > User Management**.




2. In the **Add User** section, enter the username for the new user.

   **Note:** Usernames can be a maximum of 64 characters long. Usernames can start with a digit and can contain alphanumeric characters, in addition to the following special characters: **=~^._+#@/-**

3. Enter a **Password** for this user.

   **Note:** The minimum password length is defined by what is set in the **Minimum password length** field..

4. Depending on or not Session Management is enabled, another option will appear for this new user:

- **Session Management disabled:** If Session Management is not enabled, the **Use RADIUS Server** check box will appear. For further information on RADIUS WUI authentication, please refer to the RADIUS Authentication and Authorization, Technical Note.
- **Session Management enabled:** If Session Management is enabled, the **No Local Password** check box will appear. This can be optionally enabled if using client certificate authentication for WUI access. For further information on client certificate WUI authentication, refer to the Session Management section of this document.

  **Note:** Certificate-based authentication will be deprecated at some point in the future.

1. Click **Add User**.

After a user has been added, modifications can be made to their user account, such as the configuration of their permissions. Refer to the Modify an Existing User section for instructions and further information relating to modifying an existing user.

# Modify an Existing User

## Modify an Existing User

To modify an existing user, navigate to **System Configuration > System Administration > User Management** and click **Modify** next to the relevant user. On the modify screen, there are three areas:

- **Permissions:** For further details on each of the permission types, refer to the User Permissions section.
- **Change Password:** For further information on this section, refer to the Change a User's Password and WUI Authentication Method section.
- **API Keys:** When running API commands, you can authenticate using an API key. An API key is a unique identifier used to authenticate a user. The **API Keys** section on the **Modify** user screen displays any API keys currently generated for that specific user. You can have up to 16 API keys per user - if you try to create more, the oldest is silently deleted. The oldest API key is listed at the top. To generate an API key for a specific user, click **Generate New APIKey**.

- **Local Certificate:** For further information on this section, refer to the Client Certificate WUI/API Authentication section.

**Related Links**

- User Permissions
- Change a User's Password and WUI Authentication Method

# User Permissions

## User Permissions

A number of "roles" are available to select from in the modify user screen. A change to a user's roles takes effect in real-time. The different roles can be combined and they are mutually exclusive.

The default access provided to users is read only access. This provides access to:

- Read access to most screens in the WUI
- Read access to log files
- Generate Client Certificate Requests (CSRs)
- Perform basic debugging

The various permission roles are described in the sections below.

## Real Servers

This role permits the following operations on Real Servers:

- Add
- Modify
- Delete
- Enable
- Disable

---

**Note:** This role does not provide any permissions on SubVSs.

---

While adding or modifying a Real Server, the following settings can be set or modified:

- **Real Server Address**
- **Port**
- **Forwarding Method**
- **Weight**
- **Connection Limit**

## Virtual Services

This role relates to managing Virtual Services. This includes SubVSs. Virtual Service actions permitted vary depending on whether or not the **Allow Extended Permissions** option is enabled. For further information, refer to the Virtual Service Permissions section.

## Rules

This role permits managing content rules. Rule actions permitted include adding, deleting and modifying.

## System Backup

This role permits performing system backups.

## Certificate Creation

This role permits managing SSL certificates. Certificate management includes adding, deleting and modifying SSL certificates.

## Intermediate Certificates

This role permits managing intermediate certificates. This includes adding and deleting intermediate certificates.

## Certificate Backup

This role permits the ability to export and import certificates.

## User Administration

This role is allowed access to all functionality within the **System Configuration > System Administration > User Management** screen, for all user management.

## GEO Control

This role provides the ability to manage GEO settings, if relevant. For further information on GEO, refer to the **GEO, Feature Description** on the Documentation Page.

## Add Virtual Services

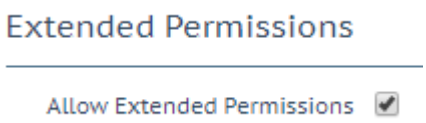
This role is only visible if the **Allow Extended Permissions** check box is enabled. This role relates to managing Virtual Services. This includes SubVSs. Refer to the Virtual Service Permissions section for further details on the permissions provided by this option.

# All Permissions

This role provides all permissions, except the ability to change the **bal** password.

# Virtual Service Permissions

There are two permissions relating to Virtual Services - **Virtual Services** and **Add Virtual Services**.




The **Add Virtual Services** permission is only visible when the **Allow Extended Permissions** check box is selected on the **User Management** screen. The Virtual Service operations allowed differ based on what combination of options you have selected. For a summary of these connotations, refer to the table below:

| Allow Extended Permissions | Virtual Services | Add Virtual Service | Operations Allowed | Operations not Allowed |
|---|---|---|---|---|
| Enabled | Enabled | Disabled | • View existing Virtual Services<br>• Modify existing Virtual Services<br>• Change Virtual Service port | • Add Virtual Service<br>• Duplicate Virtual Service<br>• Change Address<br>• Export template |
| Enabled | Disabled | Enabled | • View existing Virtual Services | • Add Virtual Service<br>• Duplicate Virtual Service<br>• Change Address<br>• Export template<br>• Modify existing Virtual Services<br>• Change Virtual Service port |
| Enabled | Enabled | Enabled | • Add Virtual Service<br>• Duplicate Virtual Service | Not applicable |

| Allow Extended Permissions | Virtual Services | Add Virtual Service | Operations Allowed | Operations not Allowed |
|---|---|---|---|---|
| | | | • Change address<br>• Export template<br>• View existing Virtual Services<br>• Modify existing Virtual Services<br>• Change Virtual Service port | |
| Enabled | Disabled | Disabled | View existing Virtual Services | Not applicable |
| Disabled | Enabled | Disabled | • Add Virtual Service<br>• Duplicate Virtual Service<br>• Change address<br>• Export template<br>• View existing Virtual Services<br>• Modify existing Virtual Services<br>• Change Virtual Service port | Not applicable |
| Disabled | Disabled | Disabled | View existing Virtual Services | • Add Virtual Service<br>• Duplicate Virtual Service<br>• Change address<br>• Export template<br>• Modify existing Virtual Service<br>• Change Virtual Service port |

# Change a User's Password and WUI Authentication Method

## Change a User's Password and WUI Authentication Method

To change an existing user's password, follow the steps below:

1. In the main menu of the LoadMaster WUI, navigate to **System Configuration > System Administration > User Management**.
2. Click **Modify** on the relevant user.




3. Enter the **New Password** for the user.
4. Re-enter the password.
5. Click **Change Password**.

Depending on whether or not Session Management is enabled, another option will appear in this section:

- **Session Management disabled:** If Session Management is not enabled, the **Use RADIUS Server** check box will appear. For further information on RADIUS WUI authentication, please refer to the RADIUS Authentication and Authorization, Technical Note.
- **Session Management enabled:** If Session Management is enabled, the **No Local Password** check box will appear. This can be optionally enabled if using client certificate authentication for WUI access. For further information on client certificate WUI authentication, refer to the Client Certificate WUI/API Authentication section of this document.

**Note:** Certificate-based authentication will be deprecated at some point in the future.

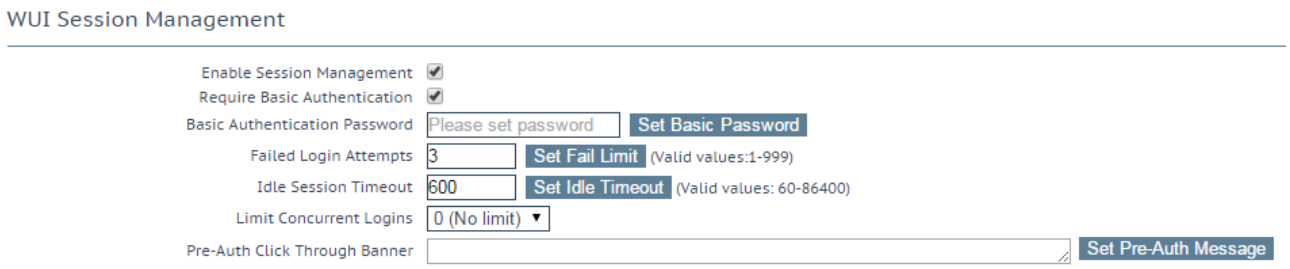
# Session Management

## Session Management

Session Management provides increased security when users are logging in to the LoadMaster WUI. WUI Session Management can be enabled/disabled and configured in the following screen: **Certificates & Security > Admin WUI Access > WUI Session Management**.

Session management is enabled by default on all LoadMasters initially deployed with firmware version 7.1.35 or above.

**Note:** If you perform a factory reset of the LoadMaster, you must enable the **Enable Session Management** check box and disable the **Require Basic Authentication** check box to successfully run APIv2 (JSON-format) requests.




The level of user permissions determine what WUI Session Management fields can be seen and modified. Refer to the table below for a breakdown of permissions.

| Control | Bal user | User with 'All Permissions' | User with 'User Administration' permissions | All other users |
|---|---|---|---|---|
| Session Management | Modify | View | View | None |
| Require Basic Authentication | Modify | View | View | None |
| Basic Authentication Password | Modify | View | View | None |
| Failed Login Attempts | Modify | Modify | View | None |
| Idle Session Timeout | Modify | Modify | View | None |
| Limit Concurrent Logins | Modify | Modify | View | |
| Pre-Auth Click Through Banner | Modify | Modify | View | None |

| Control | Bal user | User with 'All Permissions' | User with 'User Administration' permissions | All other users |
|---|---|---|---|---|
| Currently Active Users | Modify | Modify | View | None |
| Currently Blocked Users | Modify | Modify | View | None |

When using WUI Session Management, it is possible to use one or two steps of authentication.

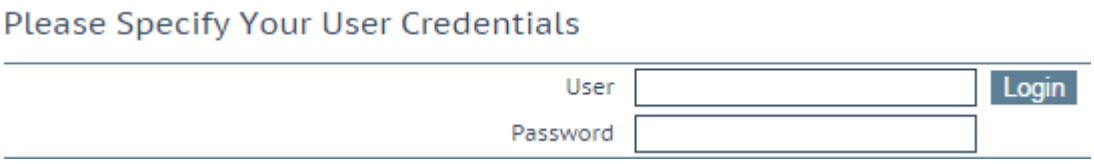
In addition to the **bal** user, another user exists by default in the LoadMaster called **user**. The purpose of the **user** user is so that administrators can provide credentials of the **user** user to people, instead of providing the **bal** credentials. The password for the **user** user, can be set by configuring the **Basic Authentication Password** text box. The password needs to be at least 8 characters long and should be a mix of alpha and numeric characters. If the password is considered to be too weak, a message appears asking you to enter a new password. Only the **bal** user is permitted to set the **Basic Authentication Password**.

If the **Enable Session Management** check box is ticked and **Require Basic Authentication** is disabled, the user only needs to log in using their local username and password (or using a client certificate, if client certificate WUI authentication is enabled – refer to the Client Certificate WUI/API Authentication section for further information). Users are not prompted to log in using the **bal** or **user** logins.

If the **Enable Session Management** and **Require Basic Authentication** check boxes are both selected, there are two levels of authentication enforced in order to access the LoadMaster WUI. The initial level is Basic Authentication where users log in using the **bal** or **user** logins, which are default usernames defined by the system.

Once logged in using Basic Authentication, the user then must log in using their local username and password (or using a client certificate – if client certificate authentication is enabled) to begin the session.

**Note:** LDAP users need to login using the full domain name. For example; an LDAP username should be **test@progress.com** and not just **test**.




After a user has logged in, they may log out by clicking the **Logout** button, , in the top right-hand corner of the screen.

**Related Links**

- Other WUI Session Management Fields

# Other WUI Session Management Fields

The other fields relating to WUI Session Management, are described in the sections below.

**Failed Login Attempts**

The number of times that a user can fail to login correctly before they are blocked can be specified within this text box. The valid values that may be entered are numbers between **1** and **999**.

If a user is blocked, only the **bal** user or other users with **All Permissions** set can unblock a blocked user.

If the **bal** user is blocked, there is a 'cool-down' period of 10 minutes before the **bal** user can login again.

**Idle Session Timeout**

The length of time (in seconds) a user can be idle (no activity recorded) before they are logged out of the session. The valid values that may be entered are numbers between **60** and **86400** (between one minute and 24 hours).

---

**Note:** Any page that refreshes automatically will not time out from the WUI **Idle Session Timeout** setting. For example, the **Real Time Statistics** page, **GSLB Statistics** page, **WAF False Positive Analysis** page, and so on.

---

**Limit Concurrent Logins**

This option enables LoadMaster administrators to limit the maximum number of concurrent login sessions logins a single user can have to the LoadMaster WUI at any one time.

The values that can be selected range from 0 to 9.

A value of 0 allows an unlimited number of logins.

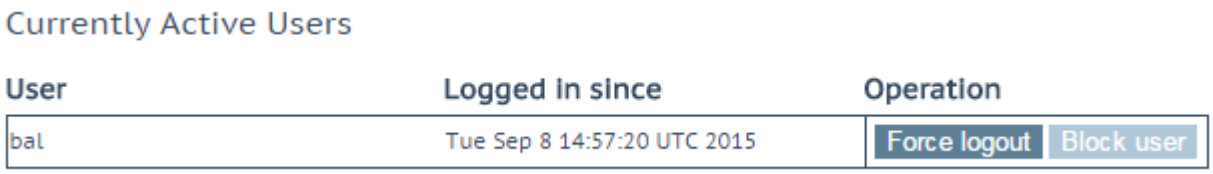
The value entered represents the total number and is inclusive of any **bal** user logins.

**Pre-Auth Click Through Banner**

Set the pre-authentication click through banner that is displayed before the LoadMaster WUI login page. This field can contain plain text or HTML code but not JavaScript. For security purposes, you cannot use the **'** (single quote) and **"** (double-quote) characters. This field accepts up to 5,000 characters.

**Active and Blocked Users**

Only the **bal** user or users with 'All Permissions' set can use this functionality. Users with 'User Administration' permissions set can view the screen but all buttons and input fields are greyed out. All other users cannot view this portion of the screen.



### Currently Active Users

The user name and login time of all users logged into the LoadMaster are listed within this section.

To immediately log out a user and force them to log back into the system, click the **Force logout** button.

To block a user from being able to log in to the system, click the **Block user** button**.** The user will not be able to log back in to the system until they are unblocked or until the LoadMaster reboots. Clicking the **Block user** button does not force the user to log off, to do this, click the **Force logout** button.

If a user exits the browser without logging off, that session will remain open in the currently active users list until the timeout has reached. If the same user logs in again, before the timeout is reached, it would be within a separate session.

### Currently Blocked Users

The user name and login time of when the user was blocked are listed within this section.

To unblock a user to allow them to login to the system, click the **Unblock** button.

# 3

# Client Certificate WUI/API Authentication

If needed, the LoadMaster can be configured to grant WUI/API access using client certificate authentication. There are two methods of client certificate WUI authentication:

- Using Common Access Card (CAC) authentication. This works for both WUI and API access.
- Using a local certificate which was generated in the LoadMaster WUI for a particular user. This only works for API access.

**Note:** You can allow local users to log in even if the client certificate has been deleted from the LoadMaster by enabling the **Allow Client Certificate Login Without Locally Installed User Certificate** option (under **Certificates & Security > Remote Access > Administrator Access**). By default, this option is disabled. Legacy local certificate login is not secure. Only enable this option if necessary. When enabling this option, a confirmation warning appears. Click **OK** to confirm.

For instructions on how to configure CAC WUI authentication, refer to the DoD Common Access Card Authentication, Feature Description.

For instructions on how to generate local certificates and use them for API authentication, refer to the sections below.

**Note:** Certificate-based authentication will be deprecated at some point in the future.

**Related Links**

- Generate and Download Client Certificates
- Create the Personal Exchange Format (PFX) File

- Import the PFX File into the Microsoft Management Console (if using Windows)
- Enable Session Management
- Enable Client Certificate Authentication
- Enable the 'No Local Password' Option for Users
- Accessing the API with the Local Certificate


# Generate and Download Client Certificates

## Generate and Download Client Certificates

Client certificates can be generated and downloaded using the LoadMaster WUI.

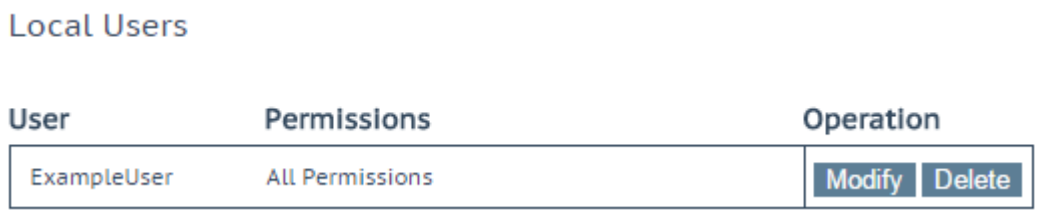
To generate a local certificate, follow the steps below:

---

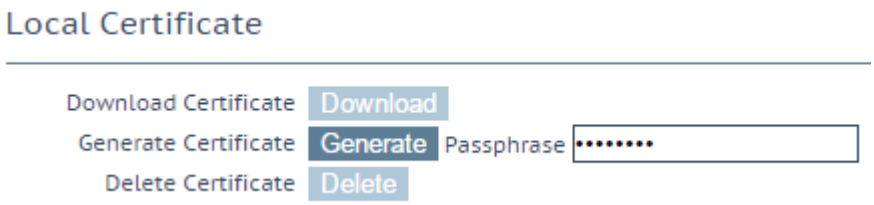
**Note:** Users with 'User Administration' permissions are able to manage local certificates for themselves and other users.

---

1. In the main menu of the LoadMaster WUI, navigate to **System Configuration > System Administration > User Management**.




2. Click **Modify** on the relevant user.

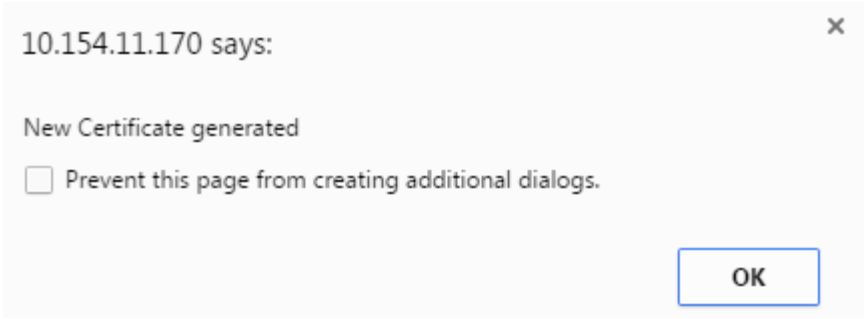



3. Enter a **Passphrase** and click **Generate**.

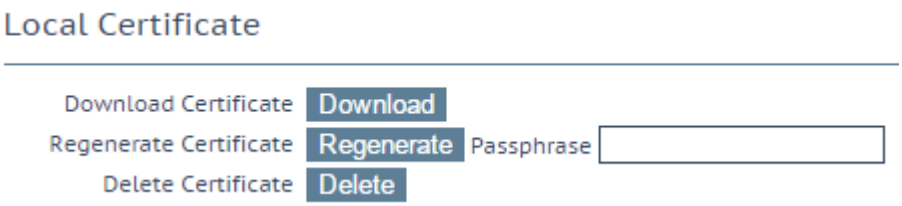
---

**Note:** This is an optional step. If a passphrase is entered it gets used to encrypt the private key.

---




4. Click **OK** to the pop-up message that appears.




5. Click **Download**.

Client certificates can also be regenerated from this screen.

# Create the Personal Exchange Format (PFX) File

## Create the Personal Exchange Format (PFX) File

When you generate a certificate, as described in the Generate and Download Client Certificates section, the LoadMaster creates a .pem file. For certificate-based authentication to work with PowerShell, a .pfx file is required.

There are several ways to convert the .pem file to .pfx. For the purposes of this document, we use OpenSSL. If you are using Windows, you may need to install OpenSSL to run these steps.

To create a .pfx file, follow the steps below:

1. Open the .pem certificate.
2. Copy from the start of the **-----BEGIN CERTIFICATE-----** section to the end of the **-----END CERTIFICATE-----** section.
3. Paste this text into a new file.
4. Save the file as **<CerFileName>.cer**.
5. Go to the .pem certificate file again.
6. Copy from the start of the **-----BEGIN RSA PRIVATE KEY-----** section to the end of the **-----END RSA PRIVATE KEY-----** section.
7. Paste this text into a new file.
8. Save the file as **<KeyFileName>.key**.
9. Use the **openssl** command to create the .pfx file:

**openssl pkcs12 -export -out <NewFileName>.pfx -inkey <KeyFilename>.key -in <CerFileName>.cer**

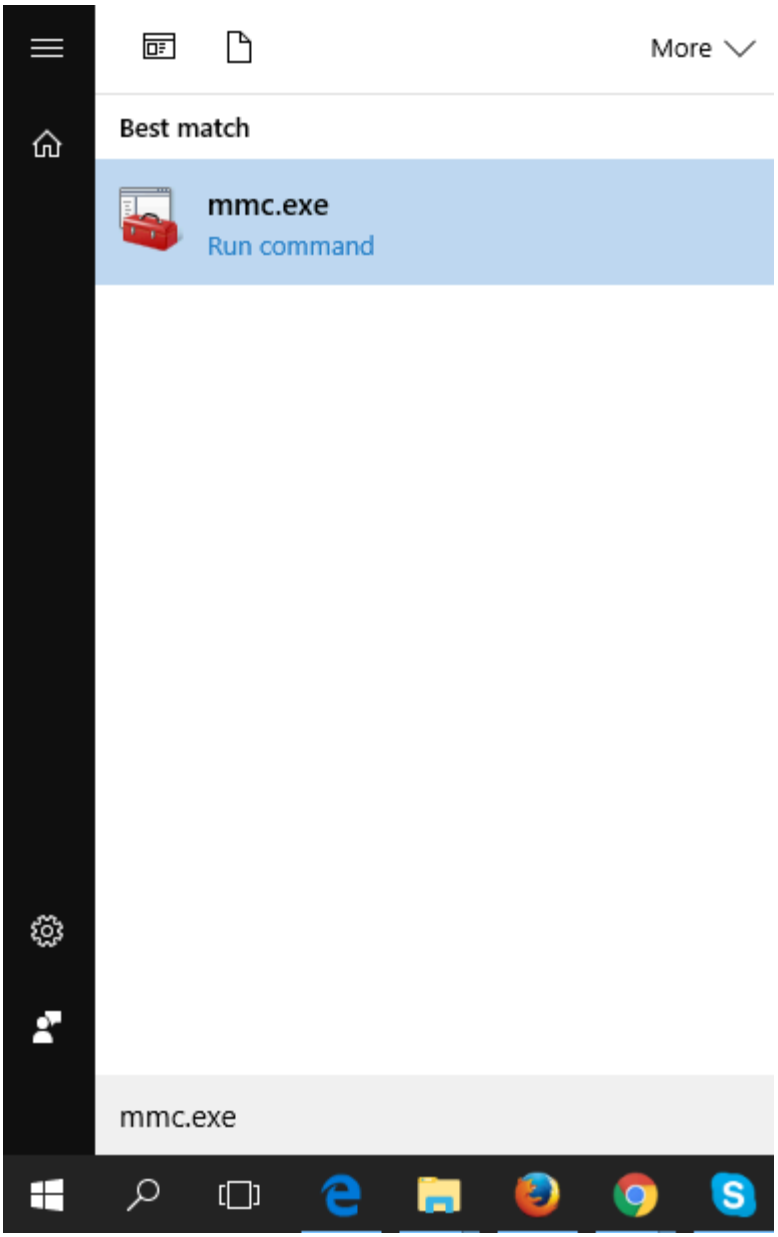
10. Import the certificate to the web browser.

# Import the PFX File into the Microsoft Management Console (if using Windows)

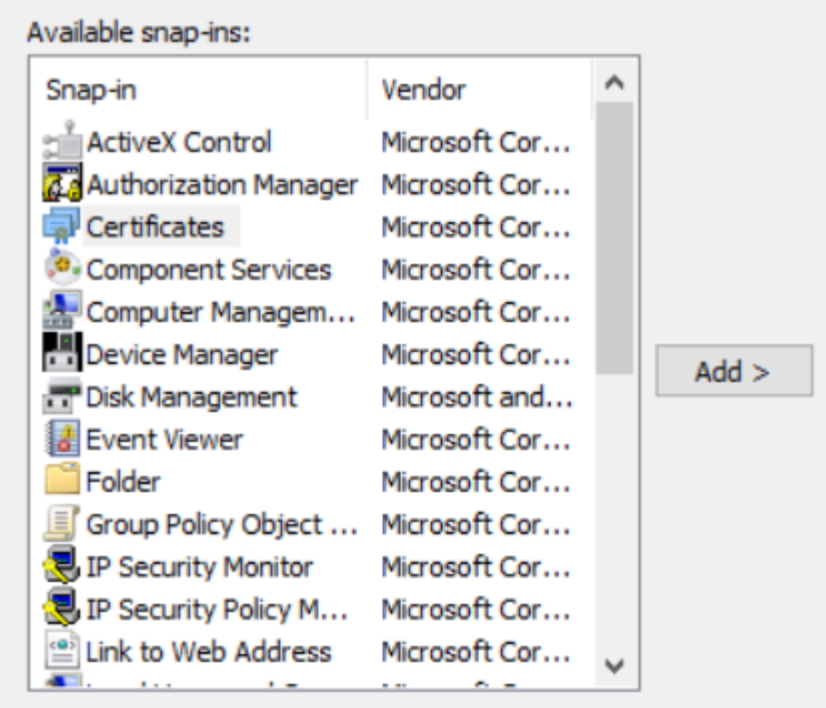
## Import the PFX File into the Microsoft Management Console (if using Windows)

You can either import the PFX file into a web browser, or into the Microsoft Management Console.

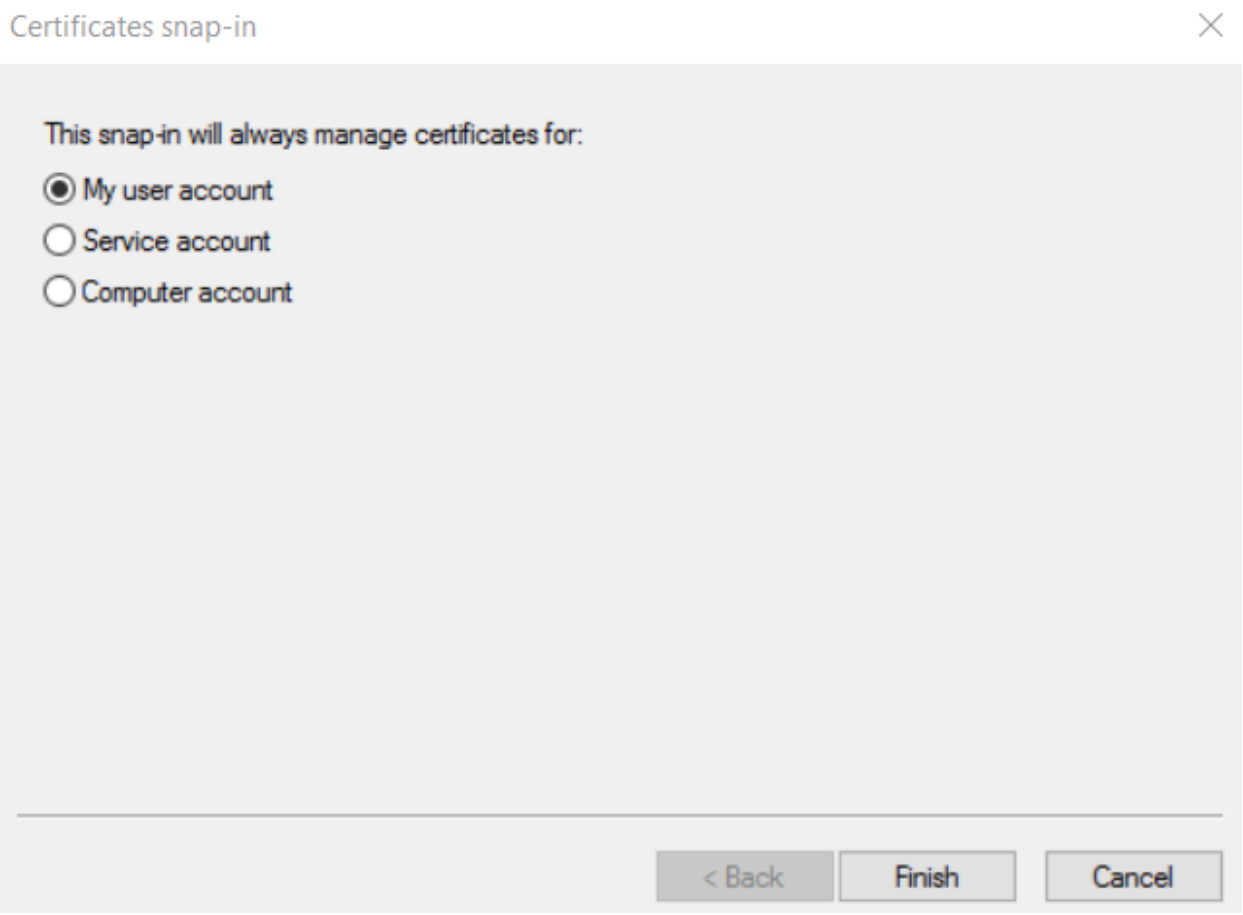
If you are using Windows, follow the steps below to import the .pfx file into the Microsoft Management Console:



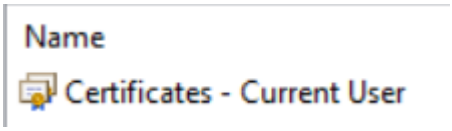

1. Click **Start** and type **mmc.exe**.
2. Click **mmc.exe** to open the Microsoft Management Console.
3. Click **File** and select **Add/Remove Snap-in**.



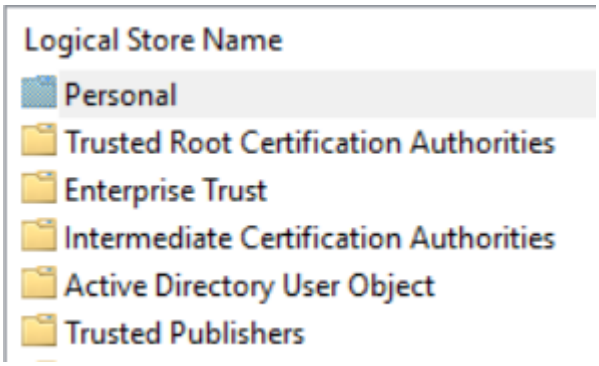

4. Select **Certificates** on the left and click **Add**.



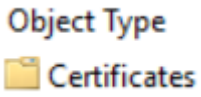
5. Ensure that **My user account** is selected and click **Finish**.
6. Click **OK**.



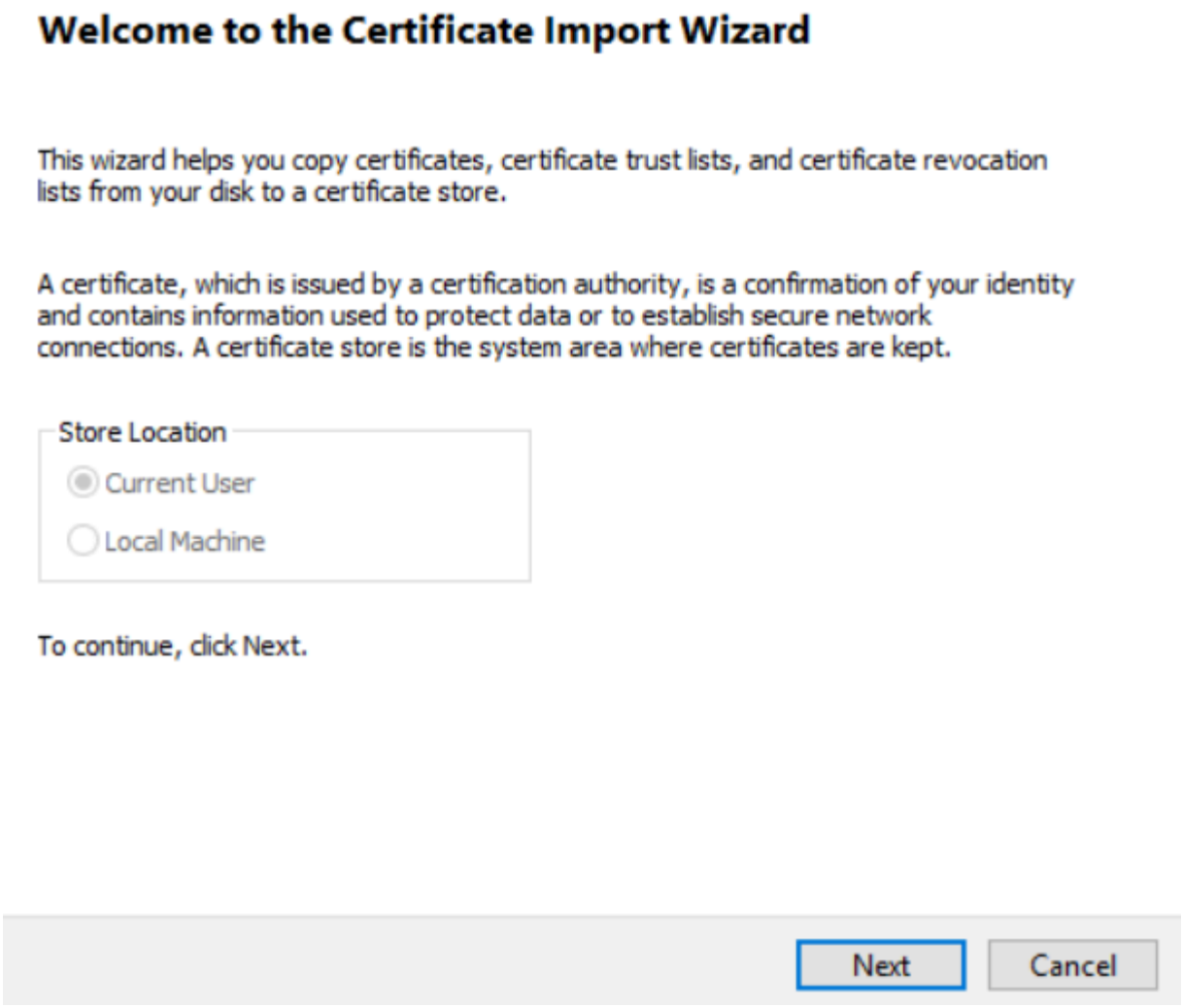

7. Double-click **Certificates – Current User**.



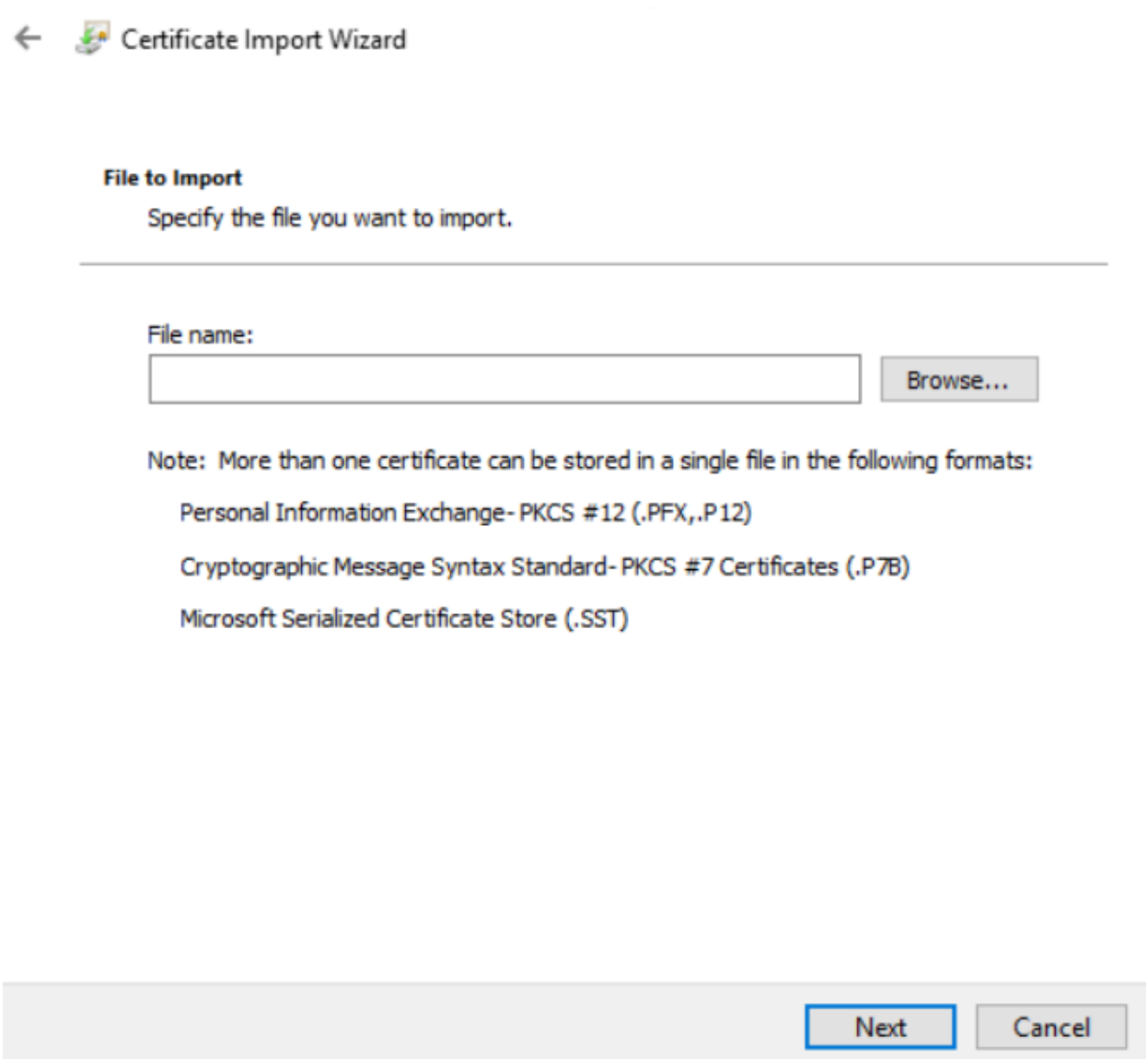

8. Double-click **Personal**.



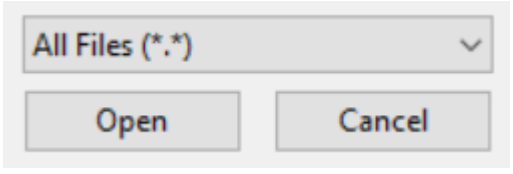

9. Double-click **Certificates**.
10. Right-click on any white space in the middle panel, select **All Tasks** and click **Import**.



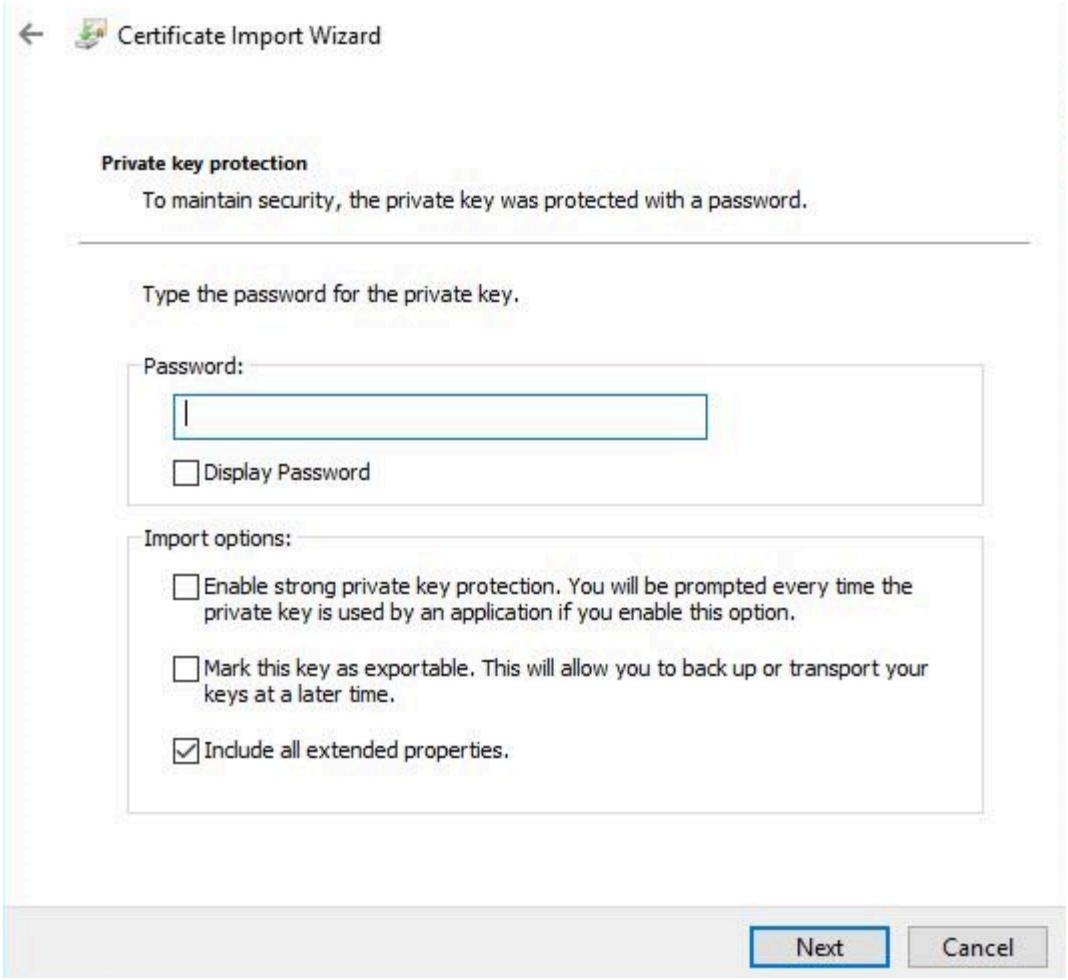

11. Click **Next**.



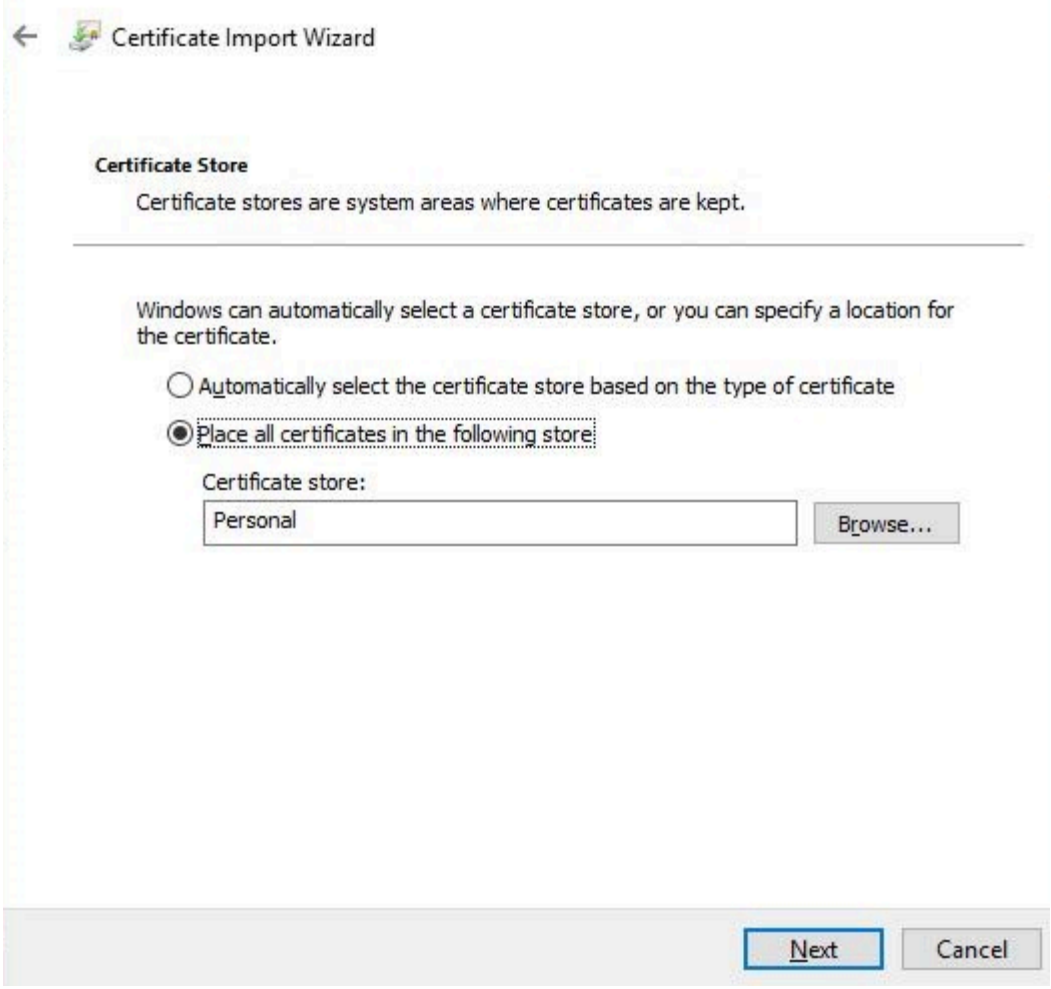

12. Click **Browse**.
13. Browse to the location of the .pfx file to be imported.



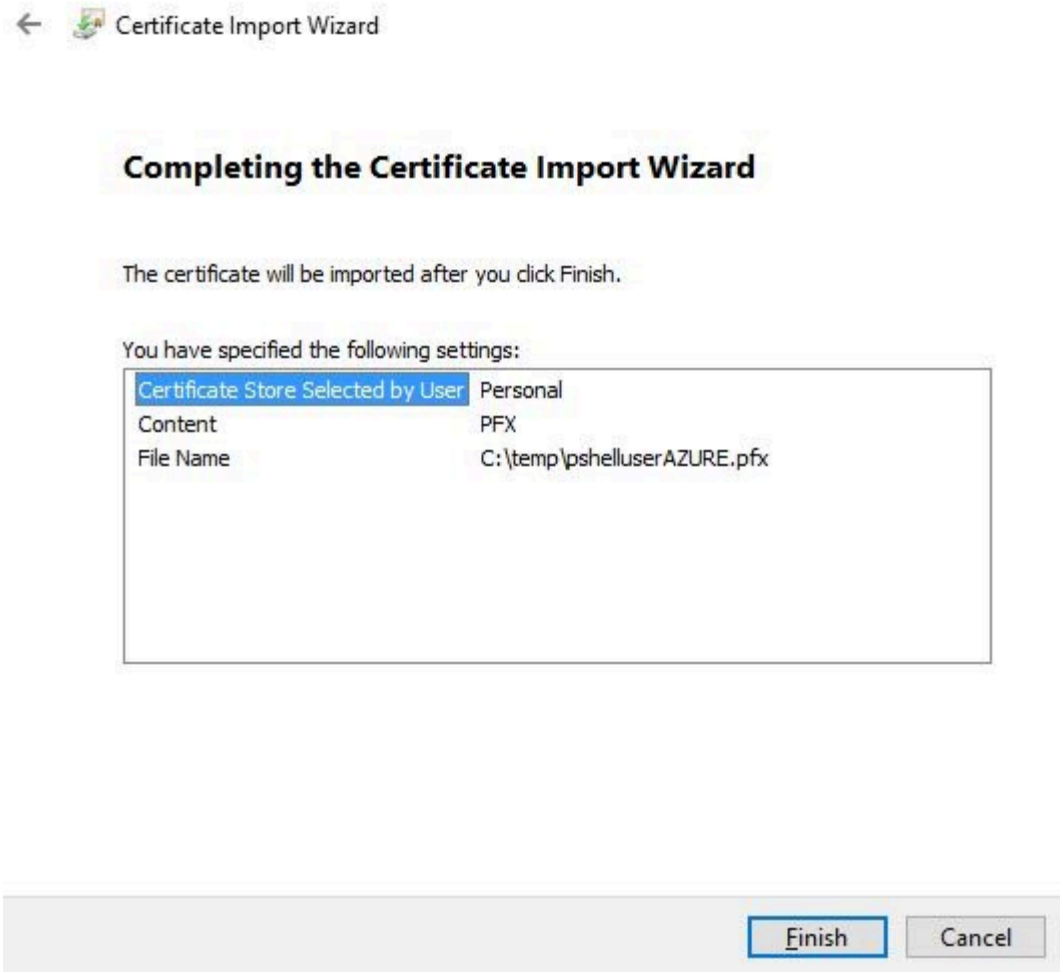

14. Select **All Files** in the drop-down menu in the bottom-right.
15. Double-click the .pfx file.




16. Enter the **Password** (if necessary).
17. Click **Next**.




18. Click **Browse** and select the **Personal** certificate store.
19. Click **Next**.



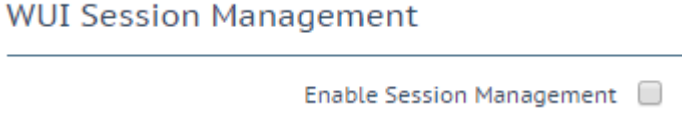

20. Review the settings and click **Finish**.

# Enable Session Management

## Enable Session Management

Session Management must be enabled before client certificate authentication can be enabled. To enable Session Management, follow the steps below:

1. In the main menu of the LoadMaster WUI, navigate to **System Configuration > Miscellaneous Options > WUI Settings**.




2. Tick the **Enable Session Management** check box.

**Note:** After this check box is enabled, the user is required to log in in order to continue using the LoadMaster.

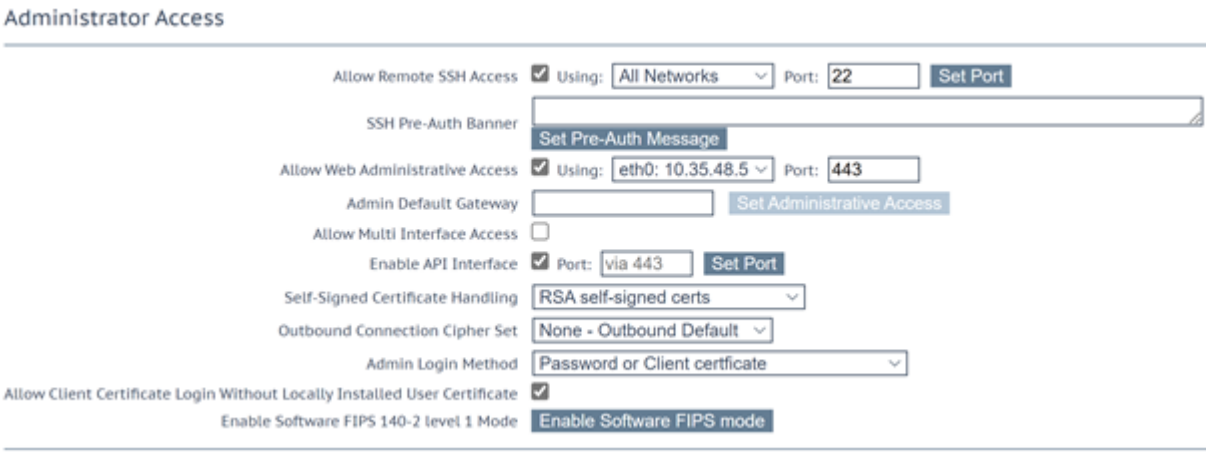
3. Configure any other settings as needed. For further information on Session Management, refer to the Session Management section.

# Enable Client Certificate Authentication

## Enable Client Certificate Authentication

A number of different login methods are available to enable. For steps on how to set the **Admin Login Method**, along with a description of each of the available methods, refer to the steps below:

1. In the main menu of the LoadMaster WUI, navigate to **Certificates & Security > Remote Access**.




2. Select the relevant **Admin Login Method**.

**Note:** Using local certificates will only work with API authentication. As a result of this, it might be best to select the **Password or Client certificate** option. This will allow API access using the client certificate and WUI access using the username/password.

The following login methods are available:

**Note:** The **Pre-Auth Click Through Banner** in the **Admin WUI Access** screen must be set for all **Admin Login Method** options to be made available.

- **Password Only Access (default):** This option provides access using the username and password only – there is no access using client certificates.
- **Password or Client certificate:** The user can log in using either the username/password or using a valid client certificate. If a valid client certificate is in place, the username and password is not required.The client is asked for a certificate. If a client certificate is supplied, the LoadMaster will check for a match. The LoadMaster checks if the certificate is a match with one of the local certificates, or checks if the Subject Alternative Name (SAN) or Common Name (CN) of the certificate is a match. The SAN is used in

preference to the CN when performing a match. If there is a match, the user is allowed access to the LoadMaster. This works both using the API and user interface.An invalid certificate will not allow access.If no client certificate is supplied, the LoadMaster will expect that a username and password is supplied (for the API) or will ask the user to enter a password using the standard WUI login page.

- **Client certificate required:** Access is only allowed using the use of a client certificate. It is not possible to log in using the username and password. SSH access is not affected by this (only the **bal** user can log in using SSH).
- **Client certificate required (Verify via OCSP):** This is the same as the **Client certificate required** option, but the client certificate is verified using an OCSP service. The OCSP Server Settings must be configured in order for this to work. For further information on the OCSP Server Settings, refer to the DoD Common Access Card Authentication, Feature Description.

Some points to note regarding the client certificate methods are below:

- The **bal** user does not have a client certificate. Therefore, it is not possible to log into the LoadMaster as **bal** using the **Client certificate required** methods. However, a non-**bal** user can be created and granted **All Permissions**. This will allow the same functionality as the **bal** user.
- There is no log out option for users that are logged in to the WUI using client certificates, as it is not possible to log out (if the user did log out the next access would automatically log them back in again). The session is terminated when the page is closed, or when the browser is restarted.

# Enable the 'No Local Password' Option for Users

## Enable the 'No Local Password' Option for Users

When using client certificate authentication, there are a number of different login methods which can be selected. One of these options (**Password or Client certificate**) will allow access using the username/password if a client certificate is not supplied. For further information on each of the login methods, refer to the Enable Client Certificate Authentication section.

When Session Management is enabled, it is possible to enable a **No Local Password** option for the LoadMaster users. If local certificates are in use and this option is enabled, the user will only be able to access the API using a local certificate and the user will not be able to access the LoadMaster WUI.

To enable the **No Local Password** option for a user, follow the steps below:

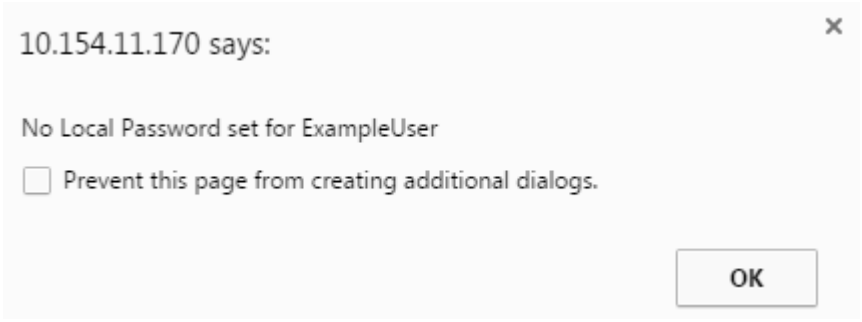
1. In the main menu of the LoadMaster WUI, navigate to **System Configuration > System Administration > User Management**.




2. Click **Modify** on the relevant user.




3. Enable the **No Local Password** check box.




4. Click **OK** to the pop-up message.

# Accessing the API with the Local Certificate

## Accessing the API with the Local Certificate

Using local certificate authentication allows access to the LoadMaster RESTful API. This does not currently work with the PowerShell or Java APIs. In order for an API command to be run successfully using local certificate authentication, a cURL command should be run which includes the certificate in the command, instead of the username.

# 4

# WUI Authentication using LDAP Groups

## WUI Authentication using LDAP Groups

The LoadMaster enables you to authenticate to the WUI using LDAP groups. This means you do not need to set up local users on your LoadMasters.

If you do not use group authentication, you would need to create a local user on each LoadMaster (or one LoadMaster in a High Availability (HA) pair). You would need to define a password for LoadMaster access and for Active Directory. Initially, both passwords could be the same. However, if a user changes their Active Directory password, the passwords become different and this can cause confusion, in addition to the user having to remember another password.

Using group authentication allows you to configure LDAP endpoint (for example, Active Directory) group names on the LoadMaster. The LoadMaster queries the endpoint to check if a user is a member of the LoadMaster group. The response from the endpoint is either authentication failure or success.

If the user changes their Active Directory password, their access to the LoadMaster is still granted (if they are a member of a defined group) because the Active Directory is queried by the LoadMaster for authentication.

The LoadMaster user is able to use their Active Directory password to access any LoadMaster and acquire the permissions of the Active Directory group they are a member of for use on the LoadMaster.

When a user logs in, a check of the user groups on the Active Directory is performed if the following conditions are met:

- If LDAP WUI Authentication is enabled, and
- A list of groups is defined, and

- The user logging in is not locally defined or the Local Users option is disabled

To configure WUI authentication using LDAP groups, first create an LDAP endpoint configuration, then create the remote user groups and select them in the **WUI Authentication and Authorization** screen. Refer to the sections below for further details.

**Related Links**

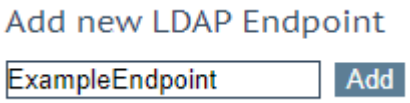
- Add an LDAP Endpoint
- Create the Remote User Groups
- Select the Remote User Groups

# Add an LDAP Endpoint

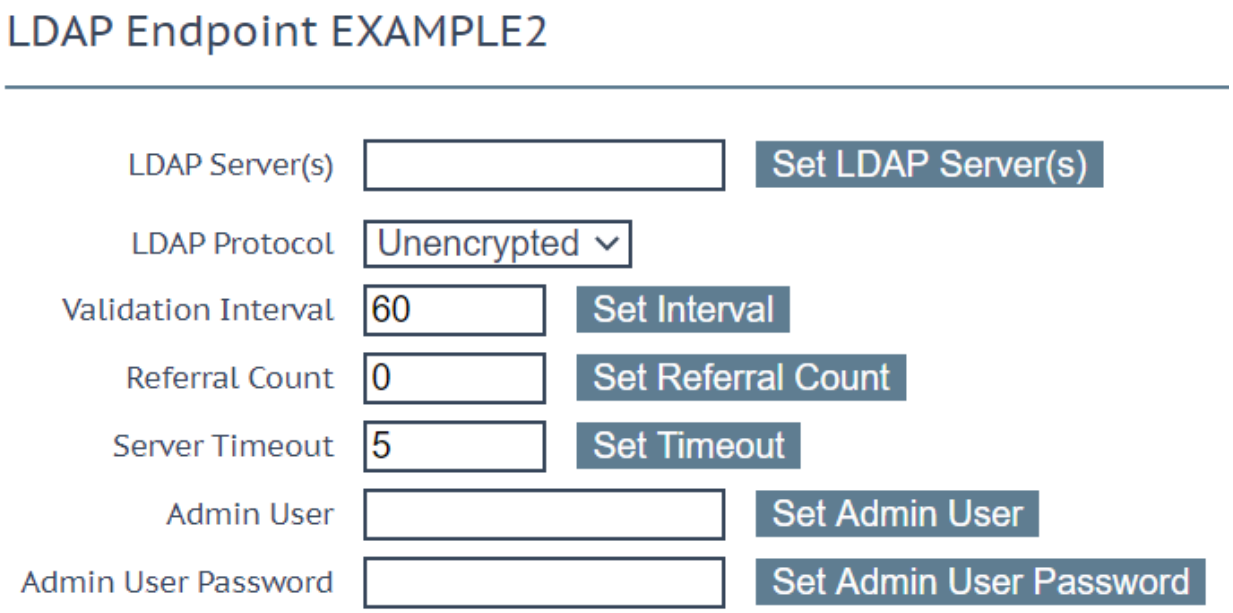
## Add an LDAP Endpoint

First, you must add an LDAP endpoint to the LoadMaster. To do this, follow the steps below:

1. In the main menu, go to **Certificates & Security > LDAP Configuration**.




2. Enter a name for the LDAP endpoint configuration and click **Add**.




3. Configure the details as needed.

Now that your LDAP endpoint exists, you must create the remote user groups. For further details, refer to the

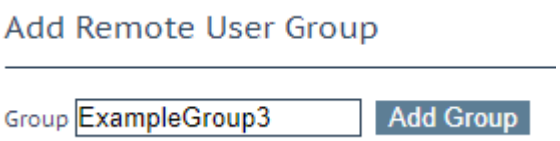
section below.

# Create the Remote User Groups

## Create the Remote User Groups

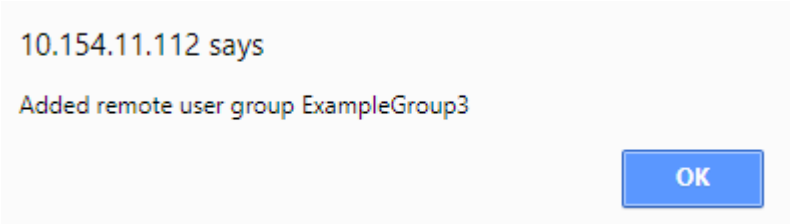
To create the remote user groups, follow the steps below:

1. In the main menu, go to **System Configuration > System Administration > User Management**.

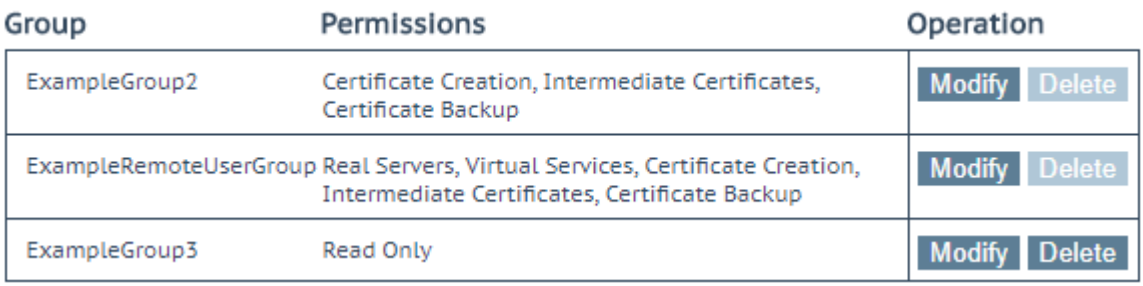



2. Enter a name for the remote user group and click **Add Group**.

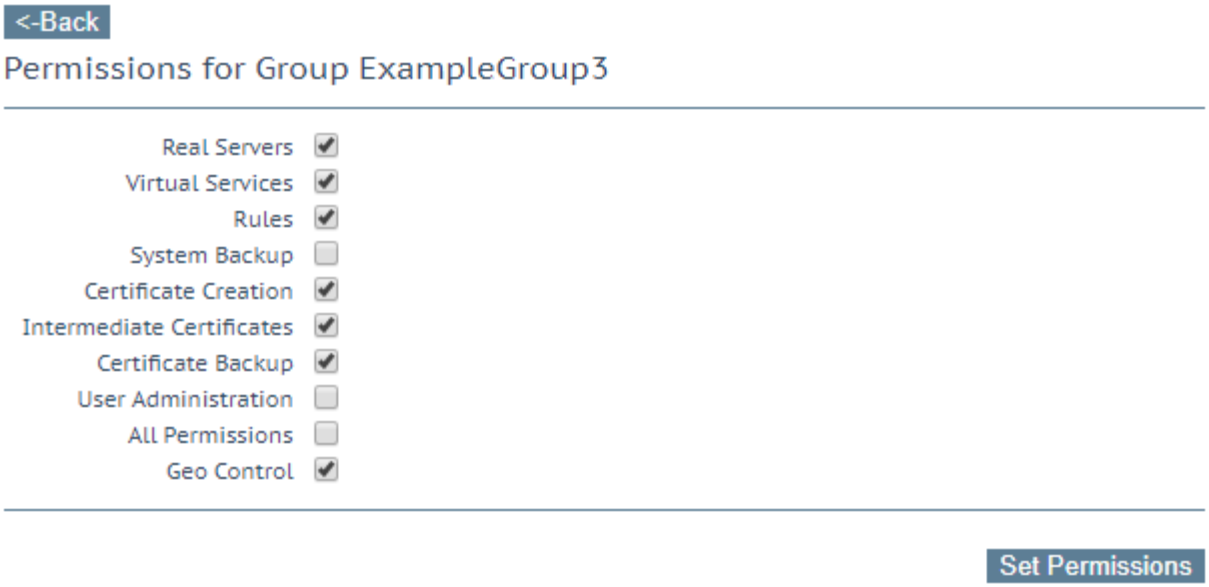
**Note:** The following characters are permitted in the group name: alphanumeric characters, spaces, or the following special symbols: **=~^._+#,@/-**.



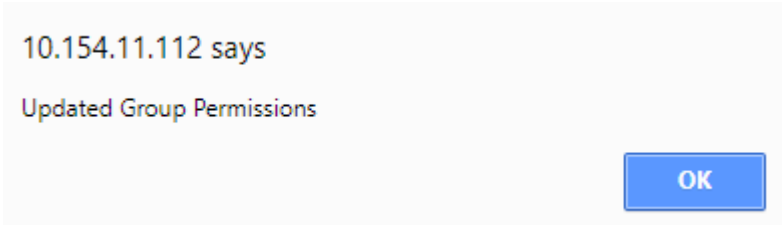

3. Click **OK** to the message.




4. By default, the group has **Read Only** permissions. Click **Modify** to edit the group permissions.




5. Select the relevant permissions that you want this group to have. For details on the different permissions, refer to the User Permissions section.
6. Click **Set Permissions**.




7. Click **OK**.
8. Click **Back**.
9. Create any other remote user groups, as needed.

Now that your remote user groups are configured, you need to select them in the **WUI Authentication and Authorization** screen. Refer to the section below for steps on how to do this.

---

**Note:** It is important to select and apply the group, or groups. If there are no groups selected, no group checking is performed and remote users can log in without a group check.

---

# Select the Remote User Groups

When your remote user groups are configured, you must select them in the **WUI Authentication and Authorization** screen.

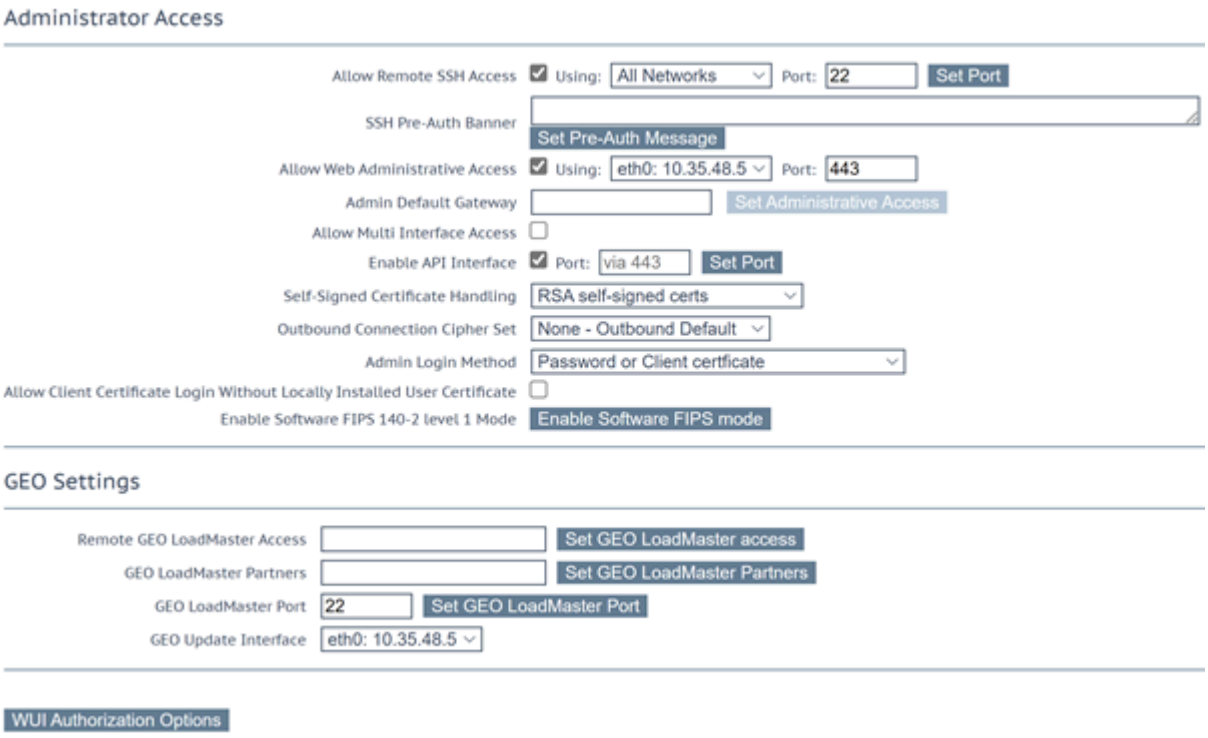
---

**Note:** It is important to select and apply the group, or groups. If there are no groups selected, no group checking is performed and remote users can log in without a group check.

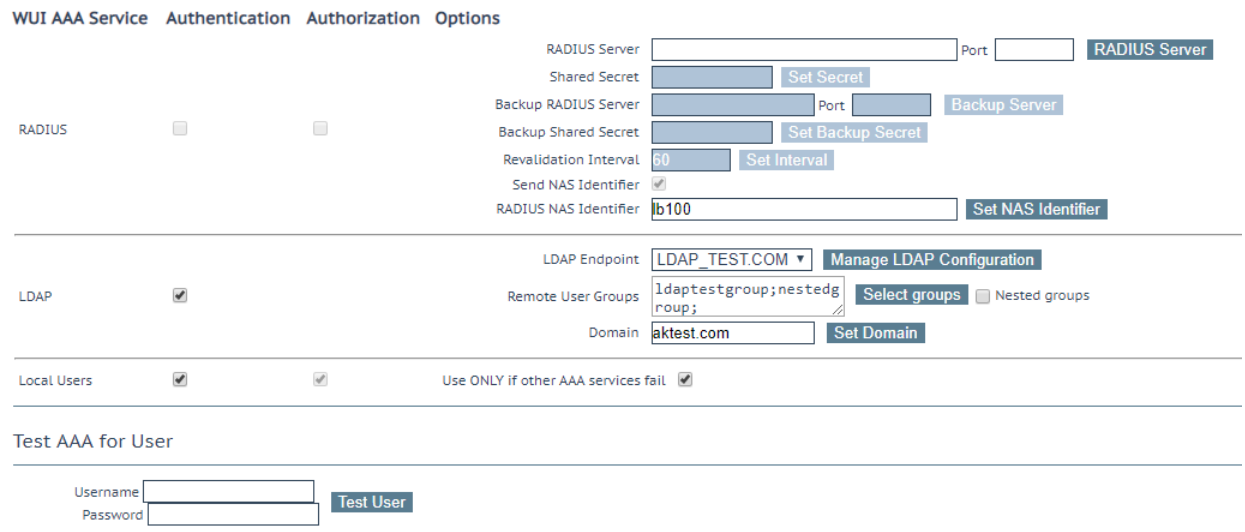
---

To do this, follow the steps below:

1. In the main menu, go to **Certificates & Security > Remote Access**.




2. Click **WUI Authorization Options**.




3. Select the relevant **LDAP Endpoint**.
4. Click **Select groups**.




5. Select the relevant groups.
6. Ensure the order is correct.

---

**Note:** The first group is checked first. On the first group match, access is enabled and no further groups are checked. If no groups are matched, user access fails and an appropriate log is reported in the syslog. If the user logs in using the group check, the matched group permissions are granted.

---

7. Click **Apply Selected Groups**.

---

**Note:** It is important to select and apply the group, or groups. If there are no groups selected, no group checking is performed and remote users can log in without a group check.

---

8. Enable or disable user nested groups using the **Nested groups** check box.
9. Enable the **LDAP Authentication** check box.

# 5

# References

## References

Unless otherwise specified, the following documents can be found at https://docs.progress.com/.

**RADIUS Authentication and Authorization, Technical Note**

**Web User Interface (WUI), Configuration Guide**

**DoD Common Access Card Authentication, Feature Description**