Progress®
Kemp® LoadMaster®

Technical Note FIPS LoadMaster

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: FIPS 140-2 Compliance 4
Document Purpose 4

Chapter 2: LoadMaster Functionality/Configuration that is not Supported in FIPS 5

Chapter 3: Best Practices when Initially Setting up FIPS 6
FIPS Initial Setup Best Practices for a New System 6
FIPS Initial Setup Best Practices for a Configured System 7

Chapter 4: Certificates 9
Generate a Certificate Signing Request (CSR) 9
Manage Certificates 11
Backup/Restore Certificates 12
Cipher Sets 13
WUI Authentication and Authorization 14
Admin WUI Access 15

1

FIPS 140-2 Compliance

The National Institute of Standards and Technology (NIST) issued the Federal Information Processing Standard (FIPS) Publication 140-2 to coordinate the requirements and standards for cryptography modules that include both hardware and software components. Federal agencies and departments can validate that the module in use is covered by an existing FIPS 140-2 certificate that specifies the exact module name, hardware, software, firmware, and/or applet version numbers. The cryptographic modules are produced by the private sector or open source communities for use by the U.S. government and other regulated industries (such as financial and health-care institutions) that collect, store, transfer, share and disseminate sensitive but unclassified (SBU) information.

FIPS 140-2 defines four levels of security, 'Level 1' to 'Level 4'. LoadMaster products have an overall compliance level of Level 1 with the FIPS 140-2 standard.

Related Links

- Document Purpose

Document Purpose

The FIPS and non-FIPS LoadMaster products are very similar. For details on most of the LoadMaster functionality, you can refer to the LoadMaster documentation. The purpose of this document is to describe some functionality that is specific to the FIPS LoadMaster.

2

LoadMaster Functionality/Configuration that is not Supported in FIPS

There is some LoadMaster functionality that is not supported in FIPS:

- Remote Access Dial In User Service (RADIUS) authentication
- Single-arm network topology configurations
- Software Defined Networking (SDN) adaptive load balancing

Some functionality is not available in FIPS, for example:

- **TLS1.3 Cipher Selection** - In FIPS mode, TLS 1.3 ciphers are presented in the cipher sets (unlike in the base non-FIPS system). There are only two FIPS-approved TLS 1.3 ciphers. They can be removed by creating and using a custom cipher set, if desired.
- **Supported TLS Protocols** - In FIPS mode, the only supported protocols are TLS 1.2 and TLS 1.3. Support for those can be configured by adding and removing ciphers from the predefined cipher sets.
- **OpenSSL version** - In FIPS mode, you cannot change the version of OpenSSL used.
- **Update Verification File** - In non-FIPS LoadMasters you can optionally upload a **Verification File** when updating the LoadMaster software. In FIPS, it is mandatory to upload a **Verification File**.

3

Best Practices when Initially Setting up FIPS

There are some best practices to be aware of when initially setting up FIPS. Refer to the relevant section below, depending on whether you are setting up FIPS on a new system, or you have an existing system that is already configured and you want to switch it to FIPS mode.

Related Links

- FIPS Initial Setup Best Practices for a New System
- FIPS Initial Setup Best Practices for a Configured System

FIPS Initial Setup Best Practices for a New System

When configuring the system for FIPS operation, best practice is to only perform basic configuration tasks on the LoadMaster before configuring the system into FIPS mode. Additional configuration should be performed after the system is switched over to FIPS mode and rebooted.

Note: If you have an existing system that is already configured with logins, Virtual Services, SSL certificates, and so on, that you want to use in FIPS mode, follow the procedure in the **FIPS Initial Setup Best Practices for a Configured System** section. Failure to follow the procedure in the next section could lead to unexpected behavior after moving the system to FIPS mode.

1. If you have a hardware unit, place the unit in a rack and connect the cables:
    1. Connect the **eth0** network interface to a switch. This is the system management interface.

    2. Connect a monitor and keyboard to the system.
    3. Connect any power cables.
    4. Flip the power switch to the "on" position.
    5. Skip step 2, which relates to virtual units.
2. If you have a virtual unit, start the unit in your hypervisor.
3. When the boot sequence completes, a login prompt is displayed on the console/monitor. Log in using these credentials:
    1. Userid: **bal**
    2. Password: **1fourall**
4. The system prompts for the following information:
    1. Set the management IP address (using CIDR format; for example, 192.168.0.11/24).
    2. Set the Nameserver IP address.
    3. Set the Gateway IP address.
    4. If required, set the Proxy IP address (this can be left blank).
5. Use a browser to connect to **https://<IPAddress>**, where **<IPAddress>** is the management IP address assigned in the previous step. This leads you through:
    1. Licensing the system.
    2. Setting a new password for the **bal** user account.
6. Set the NTP server address (in **System Configuration > System Administration > Date/Time**).
7. Enable Software FIPS Mode:
    1. Go to **Certificates & Security > Remote Access > Enable Software FIPS Mode**.
    2. Click through multiple confirmation screens.
    3. Reboot (**System Configuration > System Administration > System Reboot > Reboot**).
8. Connect to the management IP address and log in as the **bal** user using the new password you set above.
9. Set the WUI to use the **Default** cipher set (**Certificates & Security > Remote Access > Outbound Connection Cipher Set**).
10. Set the machine name and DNS domain (**System Configuration > Network Setup > Host & DNS Configuration**).
11. Obtain a TLS certificate for the unit using the **Hostname** set above.
12. Import the above TLS certificate and assign it as the device management certificate:
    1. Go to **Certificates & Security > SSL Certificates > Import Certificate**.
    2. When the certificate is imported, select the imported certificate from the **Administrative Certificate** drop-down list at the bottom of the page and click **Use Certificate**.
13. Perform any additional configuration, as required.

FIPS Initial Setup Best Practices for a Configured System

If you have an existing system that is already configured with logins, Virtual Services, SSL certificates, and so on, that you want to use in FIPS mode, you must use the following procedure below to prepare the system for operation in FIPS mode. Failure to follow this procedure could result in issues after the system comes up in FIPS mode, including:

- SSL certificates securing the web UI and Virtual Services will not be usable; they must be manually reloaded onto the system.
- You will only be able to access the system console until the above issue is addressed. This will require contacting support for a one-time access password to address these issues.

To prepare the LoadMaster for operation in FIPS mode, follow these steps:

1. Log into the web UI.
2. Create a full backup of the system (including SSL certificates):
   1. **System Configuration > System Administration > Backup/Restore**
   2. **Certificates & Security > Backup/Restore Certs**
3. Perform a factory reset of the system (**System Configuration > System Administration > System Reboot > Reset Machine**).
4. Perform steps 1 to 7 (inclusive) of the procedure in the following section: FIPS Initial Setup Best Practices for a New System.
5. Restore the configuration from the backup archive taken previously, including the SSL certificates:
   1. **System Configuration > System Administration > Backup/Restore**
   2. **Certificates & Security > Backup/Restore Certs**
6. Reboot (**System Configuration > System Administration > System Reboot > Reboot**).

4

Certificates

Refer to the following sections for information regarding managing certificates on a FIPS LoadMaster.

Related Links

- Generate a Certificate Signing Request (CSR)
- Manage Certificates
- Backup/Restore Certificates
- Cipher Sets
- WUI Authentication and Authorization

Generate a Certificate Signing Request (CSR)

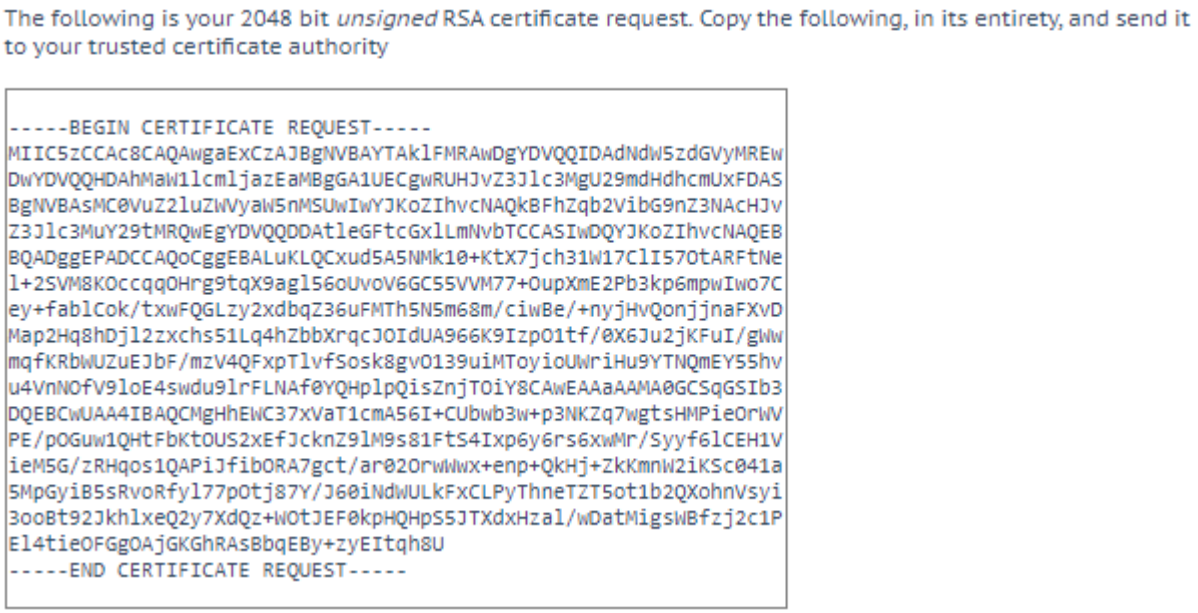
To create a CSR please complete the following steps:

1. In the main menu, go to **Certificates & Security > Generate CSR**.



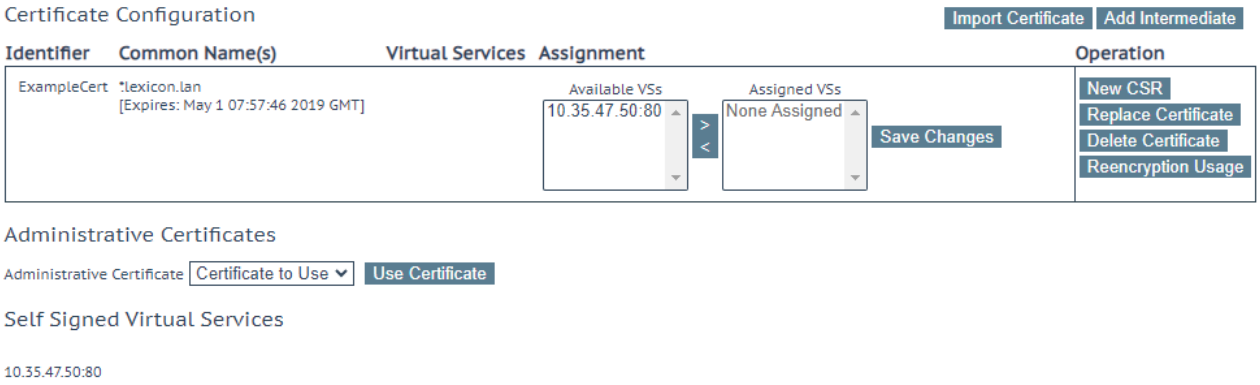
2. Fill in the details in the resulting screen. The **Common Name** field is mandatory, all other fields are optional.
3. Click **Create CSR**.

Note: The resulting key size will be 2048 bits.



4. The CSR id displayed. Copy the CSR into a file and send it to your Certificate Authority for signing. The Certificate Authority will provide you with the certificate which will be put on the server.

Manage Certificates



Shown above is the **Manage Certificates** screen (**Certificates & Security > SSL Certificates**). The options on this screen are described below.

Import Certificate - import a certificate.

Add Intermediate - add an intermediate certificate.

Identifier - the identifier that the certificate is known as on the LoadMaster.

Common Name(s) - is the FQDN (Fully Qualified Domain Name) for the site.

Virtual Services - lists any Virtual Services that the certificate is assigned to.

Assignment - the **Available VSs** box lists all of the SSL Virtual Services which are configured on the LoadMaster. The **Assigned VSs** box lists the Virtual Services which the certificate has been assigned to. The Virtual Services can be assigned/unassigned by selecting them and clicking the right/left arrow buttons and clicking **Save Changes**.

Operations -

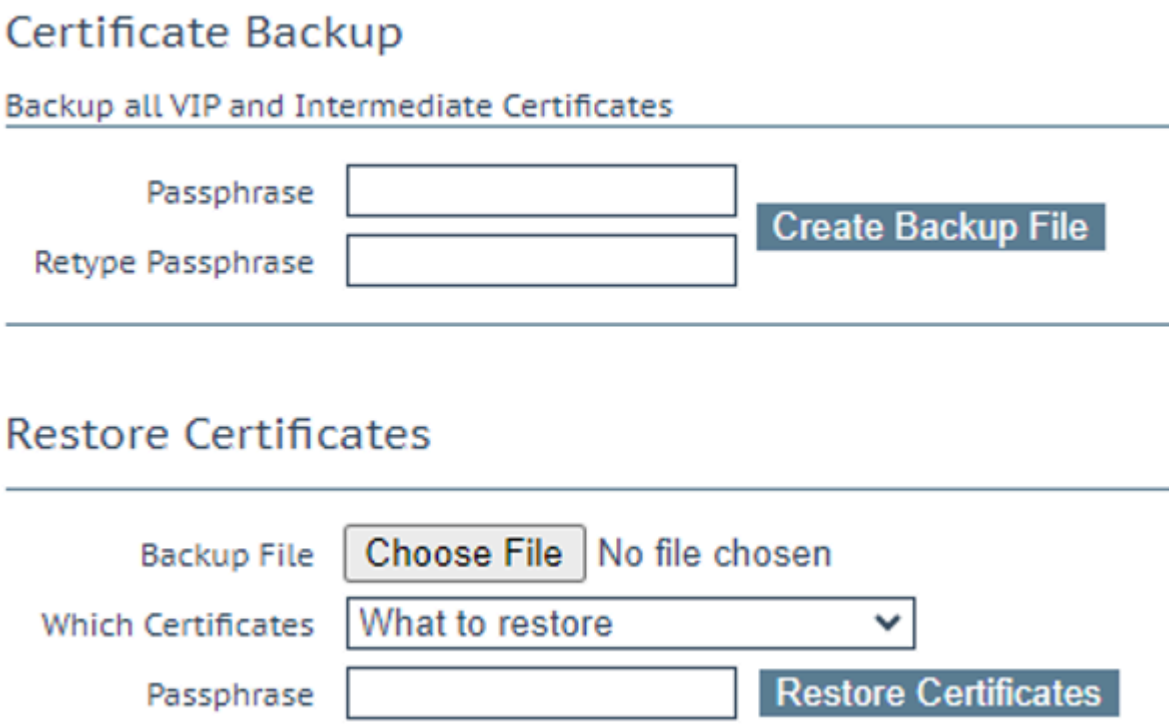
- **New CSR** - create a new Certificate Signing Request (CSR) based on the current certificate.
- **Replace Certificate** - update/replace the certificate stored in this file.
- **Delete Certificate** - delete this certificate file (this button is grayed out if the certificate is assigned to a Virtual Service)
- **Reencryption Usage** - Display the Virtual Services that are using this certificate as a client certificate when reencrypting.

When using FIPS in High Availability (HA) mode, ensure to only import certificates when both nodes are up.

Administrative Certificate - select the certificate to be used for the administrative interface. Click **Use Certificate** to apply the changes.

Backup/Restore Certificates

This section describes the **Backup/Restore** Certs screen in the FIPS LoadMaster.



Backup all VIP and Intermediate Certificates: Create a backup of all VIP and intermediate certificates. The backup will be encrypted with the given passphrase.

Note: Caution

When backing up certificates, a mandatory passphrase (password) needs to be entered twice. The parameters of the passphrase are that it must be alpha-numeric and it is case sensitive with a maximum of 64 characters. This passphrase is a mandatory requirement to restore a certificate. A certificate cannot be restored without the passphrase. If it is forgotten, there is no way to restore the certificate.

Backup File: browse to and select the intermediate certificate backup file

Which Certificates: Select what to restore. You can select from one of the following:

- **All VS and Intermediate Certs.**
- **Intermediate Certificates Only**
- **VS Certificates Only**

Passphrase: enter the passphrase associated with the certificate backup file

The FIPS LoadMaster supports exporting of intermediate certificates. The export file is designed to be used

for import into the same FIPS LoadMaster and is encrypted. You can export and import certificates using the WUI at **Certificates > Backup/Restore Certs**. Ensure to note the passphrase used to create the export because it is required to complete the import.

Cipher Sets

A cipher is an algorithm for performing encryption or decryption.

Each Virtual Service (that has **SSL Acceleration** enabled) has a cipher set assigned to it. This can either be the system-defined cipher set or a user-customized cipher set. You can select a system-defined cipher set to quickly and easily select and apply the relevant ciphers.

In the FIPS LoadMaster, there are three system-defined cipher sets; **Default**, **WUI** and **BestPractices**. Each of these cipher sets only contain ciphers that are supported by FIPS.

The list of ciphers in the **Default**, **WUI**, and **BestPractices** cipher set is the same in FIPS mode and is as follows:

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- AES128-SHA256
- AES128-GCM-SHA256
- AES256-SHA256
- AES256-GCM-SHA384
- DHE-DSS-AES128-SHA256
- DHE-DSS-AES128-GCM-SHA256
- DHE-DSS-AES256-SHA256
- DHE-DSS-AES256-GCM-SHA384
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES256-GCM-SHA384

The first two ciphers in the list above are the supported TLS 1.3 FIPS ciphers; the remainder are TLS 1.2 FIPS ciphers.

Note: The list of ciphers shown above are the only ciphers available in FIPS mode; no additional ciphers

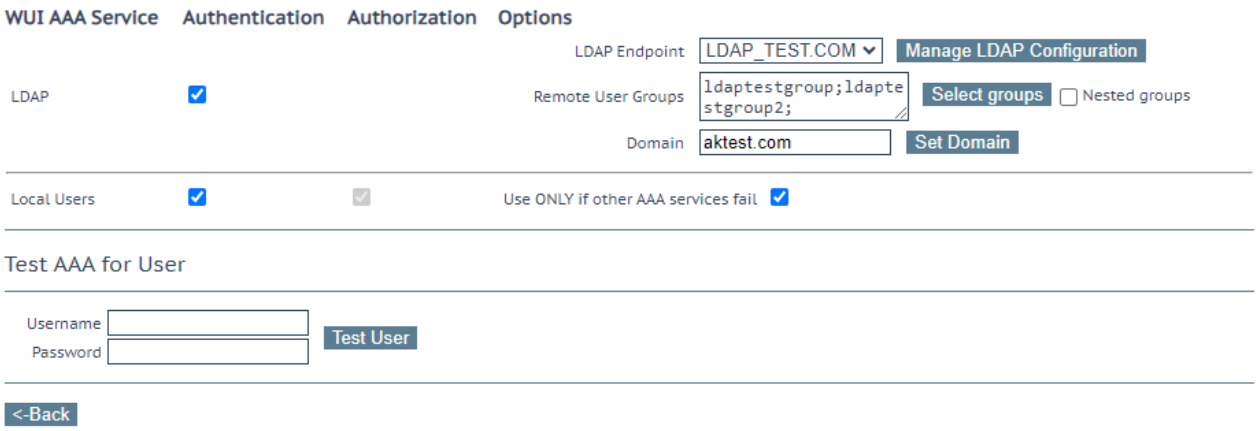
can be added to the system. If you attempt to use a certificate or key that employs ciphers not in the above list, you will generally get an Invalid Pass Phrase error (which is standard OpenSSL behavior).

You can edit the list of ciphers which are assigned to a Virtual Service by clicking **Modify Cipher Set**. If changes are made to a preconfigured cipher set, a new custom cipher set is created. You can create custom cipher sets and use them across different Virtual Services.

By default, the name for the custom cipher set is **Custom_**<*VirtualServiceID*>. We recommend changing the name of custom cipher sets because if another system-defined cipher set is modified, the name again defaults to **Custom_**<*VirtualServiceID*> and overwrites any existing cipher sets with that name.

Note: It is not possible to modify the list of ciphers in a system-defined cipher set. Instead, a new custom cipher is created when changes are made to the ciphers list.

WUI Authentication and Authorization



The **WUI Authentication and Authorization** screen (**Certificates & Security > Remote Access > WUI Authorization Options**) enables the administration of the available authentication (login) and authorization (allowed permissions) options.

Authentication

Users must be authenticated before logging on to the LoadMaster. The LoadMaster allows authentication of users to be performed using the LDAP authentication method as well as Local User authentication.

When all authentication methods are selected, the LoadMaster attempts to authenticate users using the authentication methods in the following order:

1. LDAP

2. Local Users

If the LDAP server is also not available, then Local User authentication methods are used.

If the LDAP authentication method is not selected, then the Local User authentication method is selected by default.

Authorization

LoadMaster allows the users to be authorized using Local User authorization. The user's authorization decides what level of permissions the user has and what functions on the LoadMaster they are allowed to perform.

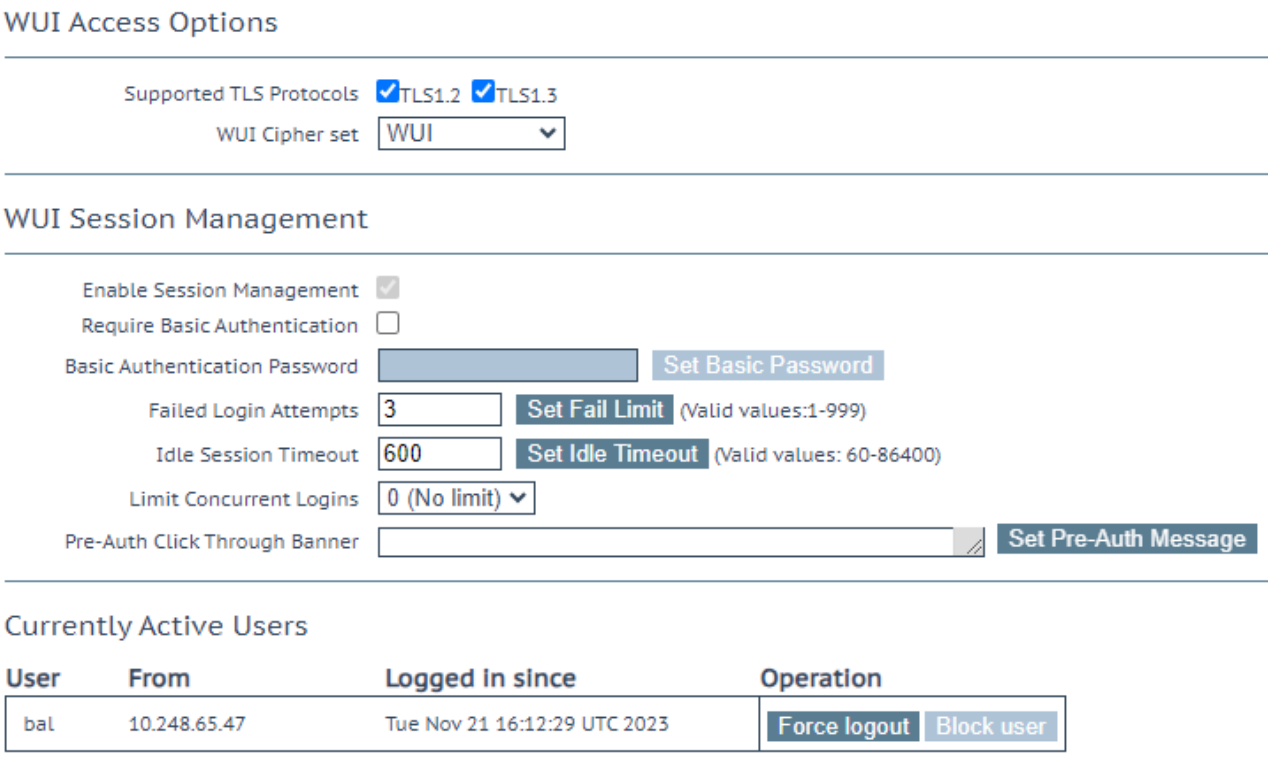
Authorization using LDAP is not supported.

Related Links

- Admin WUI Access

Admin WUI Access

This section describes the **Admin WUI Access** fields (**Certificates & Security > Admin WUI Access**).



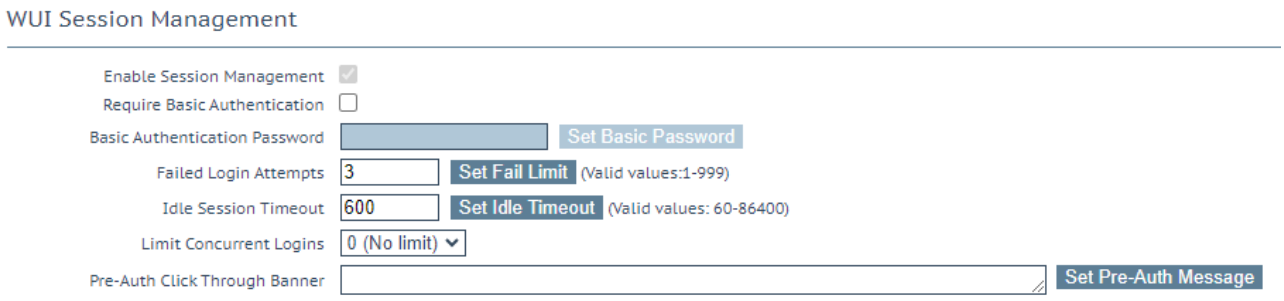
Supported TLS Protocols

Checkboxes are provided here which can be used to specify whether or not it is possible to connect to the LoadMaster WUI using the following protocols; TLS1.2 and TLS1.3. TLS1.2 and TLS1.3 are enabled by default. When connecting to the WUI using a web browser, the highest security protocol which is mutually supported by both the browser and the WUI is used.

WUI Cipher set

Select the relevant cipher set to use for WUI access. For information on each of the cipher sets available, refer to the **Cipher Sets** section.

WUI Session Management



When using a FIPS LoadMaster, Session Management is enabled and cannot be disabled.

Users with the 'All Permissions' permission set can view the **Enable Session Management**, **Require Basic Authentication** and the **Basic Authentication Password** fields. However, users with the 'All Permissions' permission set can configure the **Failed Login Attempts** and **Idle Session Timeout** values.

Users with the 'User Administration' permissions set can view the screen but all buttons and input fields are greyed out.

All other users cannot view the **WUI Session Management**, **Currently Active Users** or **Currently Blocked Users** sections of the **WUI Configuration** screen.

It is possible to use one or two steps of authentication.

If **Require Basic Authentication** is disabled, users only need to log in using their local username and password. Users are not prompted to log in using the **bal** or **user** logins.

If the **Require Basic Authentication** check box is enabled, there are two levels of authentication enforced 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.

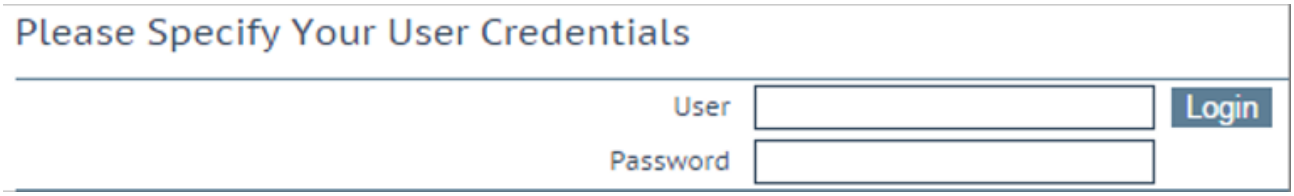
Once logged in using Basic Authentication, the user then must log in using their local username and password to begin the session.

Enable Session Management

Session Management is enabled by default and cannot be disabled when using a FIPS LoadMaster. This will force all users to login to the session using their normal credentials.

The user is required to log in to continue to use the LoadMaster.

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.

Require Basic Authentication

If Basic Authentication is enabled, there are two levels of authentication enforced 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 to begin the session.

Basic Authentication Password

The Basic Authentication password for the **user** login can be set by typing the password into the **Basic Authentication Password** text box and clicking **Set Basic Password**.

The password must 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**.

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 ten minutes before the bal user can login again. The **bal** user is unblocked if there are no login attempts at all for 10 minutes.

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 gives you the ability to limit the maximum number of concurrent login sessions to the LoadMaster WUI at any one time.

The values that can be selected range from 0 - 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.