Progress®
Kemp® LoadMaster®

Technical Note Configuring LoadMaster for Common Criteria Conformance

Generated on: 10 April 2025

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: Common Criteria Configuration Instructions 4

1

Common Criteria Configuration Instructions

The Common Criteria is a key industry standard for which LoadMaster has achieved and continues to maintain certification.

This document details the configuration settings that must be modified from their default values so that LoadMaster operation and behavior conform to the standard.

Complete the steps in the following sections to configure an installed and licensed LoadMaster into Common Criteria (CC) conformance operational mode. These instructions apply to LoadMaster Operating System (LMOS) Version 7.2.48.5 and all subsequent releases.

Log In and Install the User Interface (UI) Certificate in Your Local Certificate Store

1. Log in to the UI through HTTPS using the IP address assigned during installation, the **bal** administrative login, and the password you specified during installation.
2. Download the LoadMaster issuing CA RSA certificate and install it in the management workstation certificate store and/or the browser certificate store.

Set the Minimum Password Length

In the left menu, click **System Configuration > System Administration > User Management** to set the desired **Minimum Password Length** (default is 8).

Set ECC Ciphers for Self-Signed Certificates and Outbound Connections

1. In the left menu, click **Certificates & Security > Remote Access**.
2. In the **Self-Signed Certificate Handling** drop-down, select **EC Certs with an RSA signature**. This autogenerates a new self-signed LoadMaster certificate and assigns it to the UI.
3. Download the LoadMaster ECC Issuing CA Certificate and install in the management workstation certificate store and/or browser certificate store.
4. In the **Self-Signed Certificate Handling** drop-down, select **EC Certs with an EC signature**. This autogenerates a new self-signed LoadMaster certificate and assigns it to the UI. If you did not download and install the LoadMaster ECC issuing CA certificate, you will no longer be able to use the UI. Use the console and perform a factory reset and start over. Performing a factory reset does not change the **bal** password.

   Note: When set to this value, all Certificate Signing Requests generated on the **Certificates & Security > Generate CSR** page will also use EC signatures.

5. In the **Outbound Connection Cipher Set** drop-down, select an appropriate Custom ECC Cipher Suite Set.

Secure Remote Logging

In the left menu, click **System Configuration > Logging Options > Syslog Options**.

1. Add a remote log collector by entering an IP address into the **Syslog host** box, specify the logging level to export, and click **Add Syslog Host**.
2. In the **Remote Syslog Port** text box, enter *any port other than 601* and click **Set Port** to enable log export over secure TCP on that port.
3. Ensure that **Remote Syslog Protocol** is configured as TLS so that the system can talk to the Remote Syslog server over SSL.
4. For server certification validation, ensure that the **Server Certificate Validation** option is enabled.

Note: The secure syslog channel is restricted to TLSv1.1 and TLSv1.2.

Set the Admin UI for Certificate Login, TLS, and Custom ECC Cipher Suite Set

1. In the left menu, click **Certificates & Security > Intermediate Certs** and use the controls there to upload the issuing CA and associated Root CA certificate needed to validate admin client connections to the UI.
2. In the left menu, click **Certificates & Security > Admin WUI Access**:
   1. In the **WUI Cipher set** drop-down, select an appropriate Custom ECC Cipher Suite Set that has been generated. The Custom Cipher Suite Set can be generated from **Security & Certificates > Cipher Sets**
   2. Enable/disable **TLS Protocols** as required.
   3. Set a **Pre-Auth Click Through Banner** (this is required for certificate-based authentication to the UI).

3. In the left menu, click **System Configuration > System Administration > User Management**
   1. Create a user account that exactly matches the Principal Name on the certificate you will use for administrative access (select the option to create the account without a password)
   2. Assign privileges to the account just created. Use “All Rights” for the first account added.
4. In the left menu, click **Certificates & Security > Remote Access**.
5. Set the **Admin Login Method** to **Password or Client Certificate**.
6. Test logging in using the associated certificate. If this fails, clear cookies, close the browser, reopen the browser and try again. If this still fails, clear cookies, close the browser, reopen the browser, bypass the certificate request and sign in using the **bal** account.

Disable SSH Access

In the left menu, click **Certificates & Security > Remote Access**, and disable the **Allow Remote SSH Access** check box.

Enable Online Certificate Status Protocol (OCSP) Checking and Stapling

In the left menu, click **Certificates & Security > OCSP Configuration**:

1. Enter the **OCSP Server** IP address and click **Set Address**.
2. Enter the **OCSP Server Port** and click **Set Port**.
3. Enter the **OCSP URL** and click **Set Path**.
4. Enable the **Enable OCSP Checking** check box.

OCSP Notes:

- The **Use SSL** option must be *disabled* for OCSP checking in Common Criteria operating mode, and the OCSP server must be configured to accept unencrypted connections from LoadMaster.
- The **Authority Information Access** (AIA) certificate field is an X.509 v3 certificate extension. It *may* contain the following information:
  - The CA issuer access method: how to retrieve information about the certificate issuer.
  - The OCSP access method: the address of the OCSP server from which revocation information can be retrieved.
  - If present, the AIA field is given precedence and will be used. If the AIA is not present or appears invalid, the **OCSP Server** configuration details above will be used. Also note the following:
    - **LDAPS**: AIA information from the server certificate is honored if **Certificates & Security > OCSP Configuration > OCSP Checking** is enabled.
    - **Syslog-NG**: AIA information from the server certificate is honored if **Certificates & Security > OCSP Configuration > OCSP Checking** is enabled.
    - **UI Authentication**: AIA information from the client certificate is honored if the **Certificates & Security > Remote Access > Administrator Access > Admin Login Method** field is set to **Client certificate required (Verify via OCSP)**.

Set the Command Line Interface (CLI) Banner

In the left menu, click **Certificates & Security > Remote Access**, type an **SSH Pre-Auth Banner** and click **Set Pre-Auth Message**. This banner is also used for the CLI (even if SSH is disabled).

Disable CLI Virtual Service (VS) Administration

To disable CLI VS administration (to meet logging requirements):

1. In the left menu, click **System Configuration > Logging Options > System Log Files**.
2. In the page at right, click **Debug Options**.
3. Click **Disable CLI VS Management** [Note that the button and label now read: **Enable CLI VS Management**.]

Set Up Admin Access through LDAP

1. To set up an LDAP domain, click **Certificates & Security > LDAP Configuration**. For further details, refer to the following section: LDAP Configuration.
2. To set up admin UI (**bal** account) access through LDAP/Active Directory (AD):
   1. In the left menu, click **Certificates & Security > Remote Access**.
   2. Click **WUI Authorization Options**. For further details, refer to the following section: WUI Authentication and Authorization.

   Note: The LDAPS channel is restricted to TLSv1.1 and TLSv1.2.

Lock down Admin UI logon to Certificate Only with OCSP validation

In the left menu, click **Certificates & Security > Remote Access**.

1. Set the **Admin Login Method** to **Client Certificate Required (Verify via OCSP)**.
2. Sign out, clear cookies in the browser, close the browser, reopen the browser, and verify that certificate logon works.
3. If login fails, you will need to use the console interface to reset the web administrative settings to allow you to sign in using a password.

Enable Logging for Admin UI logon

In the left menu, click **System Configuration > Miscellaneous Options > Network Options** and set the **Log SSL errors** to **“All errors”.**

After completing these steps, your system is configured into Common Criteria mode.