NTLM

Feature Description

UPDATED: 19 March 2021

Copyright Notices

Table of Contents

1 Introduction 4

1.1 Document Purpose 6

1.2 Intended Audience 6

1.3 Related Firmware Version 6

2 Configure NTLM Authentication 7

2.1 Configure Internet Options on the Client Machine 7

2.2 Configure the LoadMaster 11

2.2.1 Enable NTLM Proxy Mode 13

2.2.2 Configure the Server Side SSO Domain 13

2.2.3 Configure the Client Side SSO Domain 15

2.2.4 Configure the Virtual Service 15

2.3 Configure Firefox to Allow NTLM (if needed) 17

2.4 Troubleshooting 18

References 19

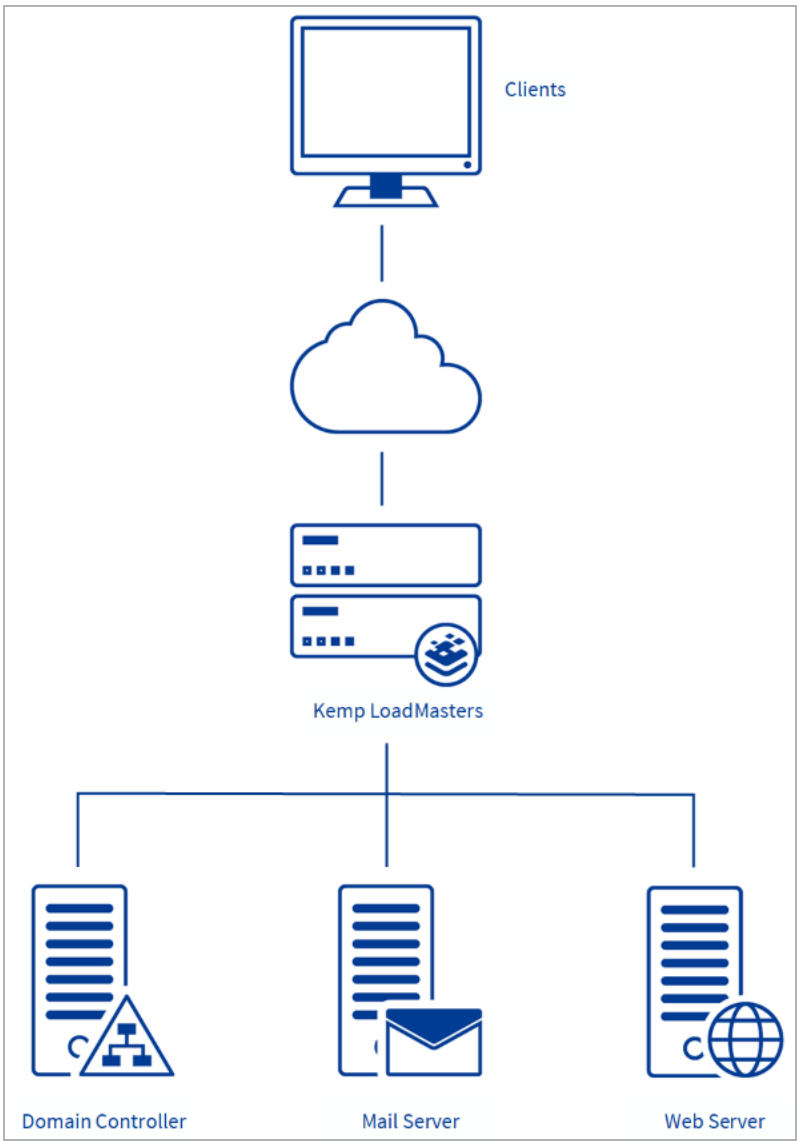
Last Updated Date 20

1 Introduction

NT LAN Manager (NTLM) is a Windows Challenge/Response authentication protocol that is often used on networks that include systems running the Windows operating system and Active Directory.

Kerberos authentication adds greater security than NTLM systems on a network and provides Windows-based systems with an integrated single sign-on (SSO) mechanism. While Kerberos is often the preferred authentication method, certain client/server scenarios may require NTLM, such as when a firewall is preventing access to Kerberos services.

NTLM credentials are based on data obtained during the interactive logon process and consist of a domain name, a user name. NTLM uses an encrypted challenge/response mechanism to authenticate a user without sending the user's password over the wire. Instead, the system requesting authentication must perform a calculation that proves it has access to the secured NTLM credentials. This process consist of three messages being exchanged, commonly referred to as Type 1 (negotiation), Type 2 (challenge) and Type 3 (authentication).



Interactive NTLM authentication over a network typically involves two systems: a client system, where the user is requesting authentication, and a domain controller, where information related to the user's password is kept. Non-interactive authentication, which may be required to permit an already logged-on user to access a resource such as a server application, typically involves three systems: a client, a server (typically an Exchange server) and a domain controller that does the authentication on behalf of the server.

The Edge Security Pack (ESP) on the Kemp LoadMaster supports multiple authentication methods including NTLM. This enables users to seamlessly authenticate to ESP-protected virtual services and be securely proxied to backend applications such as Microsoft Exchange and SharePoint.

1.1 Document Purpose

The purpose of this document is to provide step-by-step instructions on how to configure the LoadMaster to use NTLM authentication.

1.2 Intended Audience

This document is intended to be used by customers who are interested in finding out how to configure the LoadMaster to use NTLM authentication and who already have some understanding of the NTLM protocol.

1.3 Related Firmware Version

Published with LMOS version 7.2.48.4 LTS. This document has not required substantial changes since 7.2.48.4 LTS. However, the content is in sync with the latest LoadMaster LTS firmware.

2 Configure NTLM Authentication

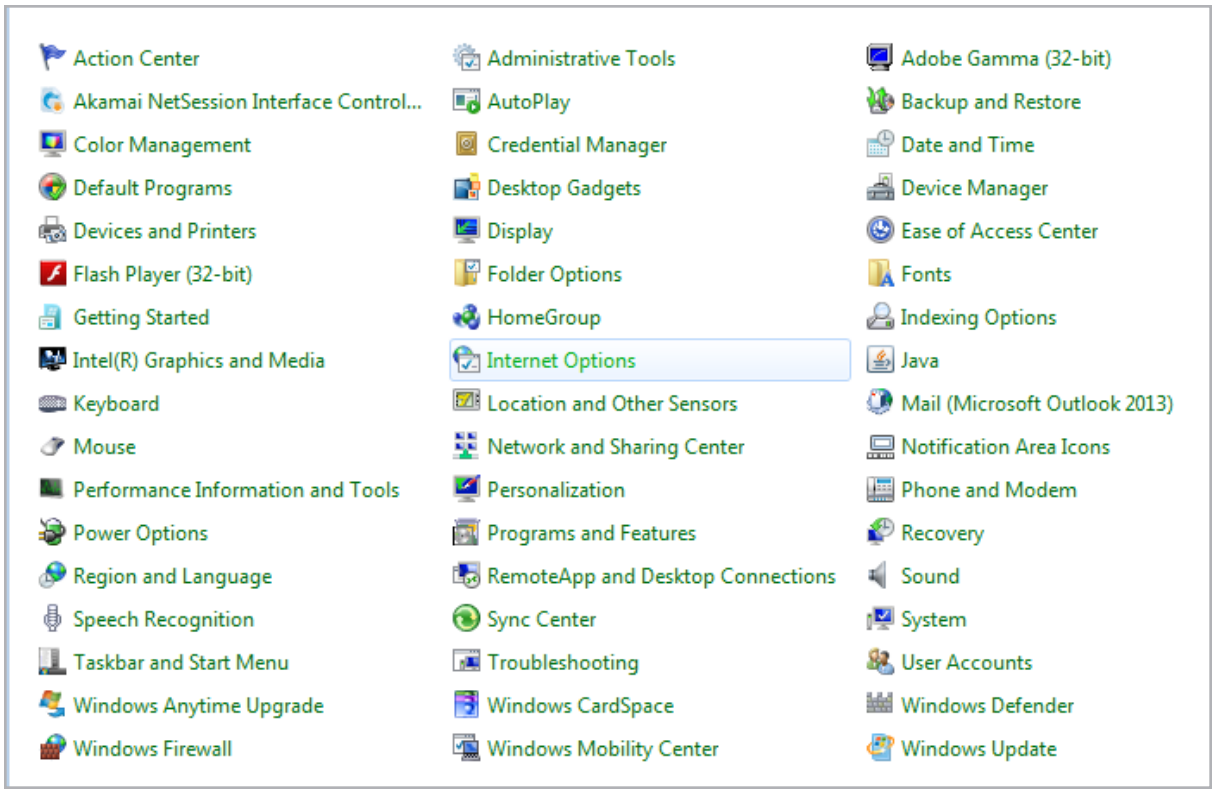
A number of steps are required in order to set up and configure NTLM authentication with Kemp LoadMaster and ESP. Refer to the sections below for step-by-step instructions.

> NTLM authentication on the LoadMaster does not work with some Windows 10 security software, such as Credential Guard, which are designed not to support NTLM. As stated in the Credentials Guard documentation: “When you enable Windows Defender Credential Guard, you can no longer use NTLM classic authentication for Single Sign-On.”

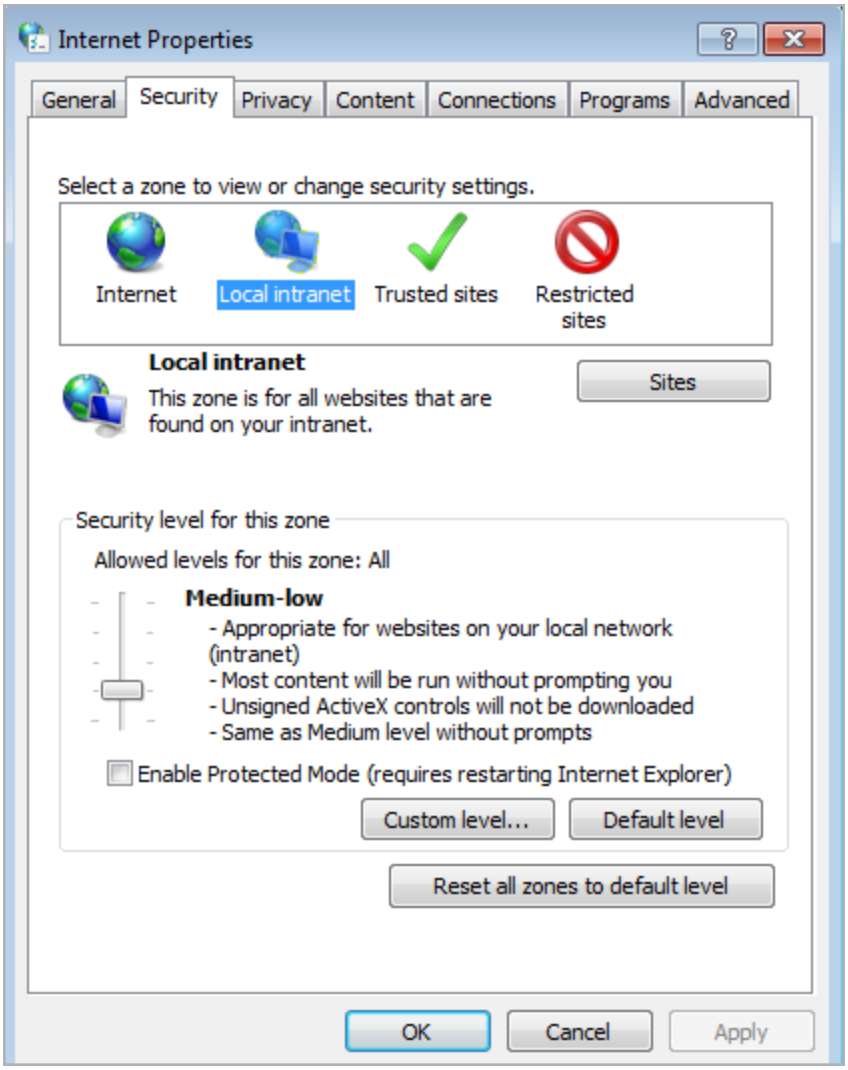
2.1 Configure Internet Options on the Client Machine

The security site address needs to be added to the local intranet zone on the client machine. To do this, follow the steps below:

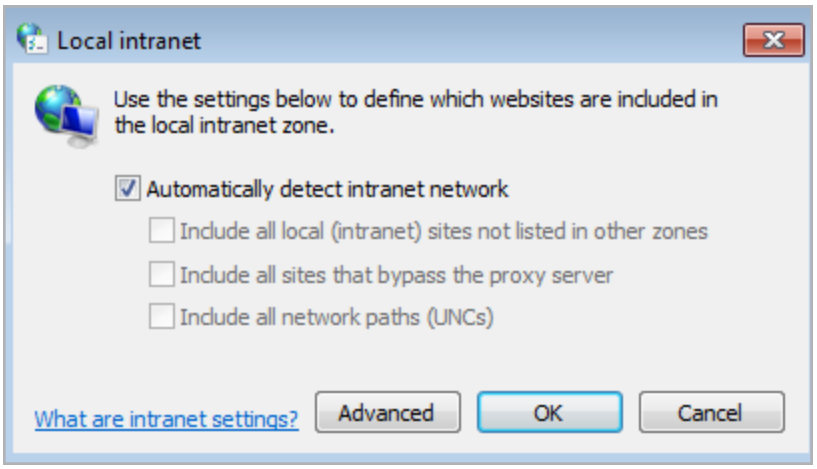
1. Click **Start** and select **Control Panel**.



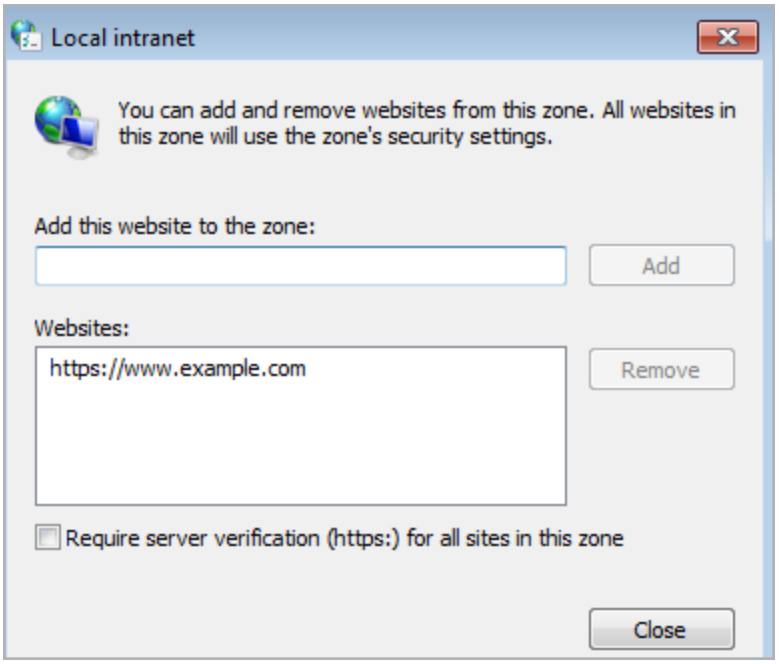
2. Click **Internet Options**.



3. Select the **Security** tab.
4. Click **Local intranet**.
5. Click **Sites**.



6. Click **Advanced**.



7. Enter the address of the security site and click **Add**.
8. Click **Close**.
9. Click **OK**.
10. Click **OK** again.

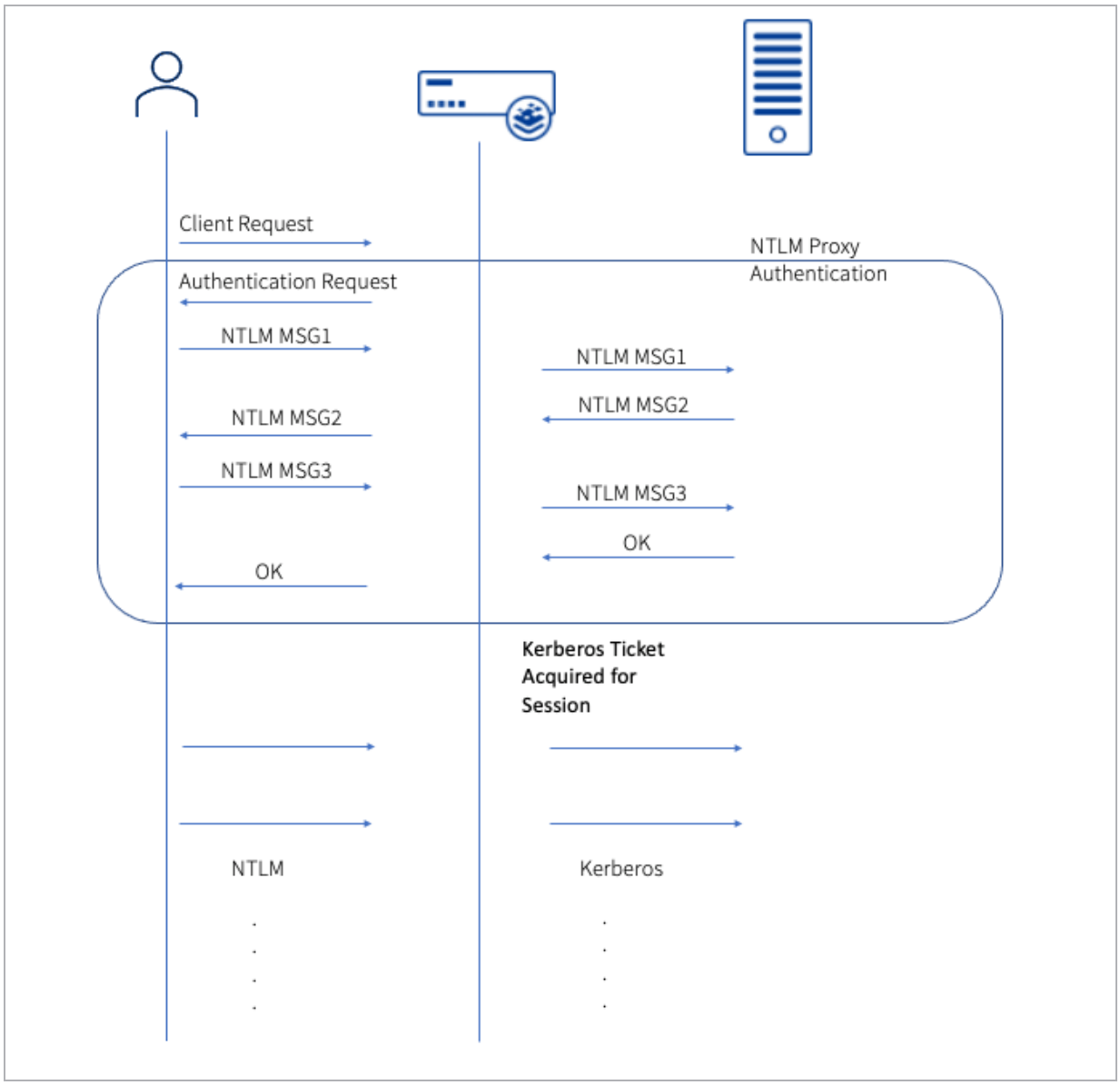
2.2 Configure the LoadMaster

In LoadMaster firmware version 7.2.48.4 Long Term Support (LTS) and 7.2.53, a new **NTLM Proxy Mode** option was added to the LoadMaster. When upgrading from an older version of LoadMaster firmware to one of these versions (or above) the **NTLM Proxy Mode** option is not enabled by default. As a result, you must manually enable **NTLM Proxy Mode** after upgrading.

For all new deployments of LoadMasters after 7.2.48.4 LTS or 7.2.53 and above, **NTLM Proxy Mode** is enabled by default.

NTLM Proxy Mode increases the security of Client Authentication by proxying NTLM Authentication with the Real Server. Authentication is verified by validating that a successful NTLM handshake has taken place with the Real Server before performing the proceeding steps (such as performing the required Server Side Kerberos Authentication where the Server Side configuration is set to KCD). This requires that the Real Server support NTLM Authentication. The legacy “NTLM” user authentication mode verified user credentials through a configured LDAP endpoint. With **NTLM Proxy Mode**, the Client Side SSO configuration only requires an LDAP endpoint in the case where Permitted Groups or Steering Groups are in use.

For example, below is a diagram of a typical flow using NTLM Proxy Mode with Server Side Authentication of KCD.



Kemp highly recommends ensuring that **NTLM Proxy Mode** is enabled.

If you want to configure the following ESP fields, you must ensure **KCD** is set as the **Server Authentication Mode** and an LDAP End point is configured in the Client SSO configuration.:

- **Pre-Authorization Excluded Directories**
- **Permitted Groups**

- Permitted Group SID(s)
- Include Nested Groups
- Steering Groups

For instructions on how to add these SSO domains on the LoadMaster, refer to the sections below.

2.2.1 Enable NTLM Proxy Mode

To ensure **NTLM Proxy Mode** is enabled, follow these steps in the LoadMaster Web User Interface (WUI):

1. In the main menu, go to **System Configuration > Miscellaneous Options > L7 Configuration**.
2. Ensure **NTLM Proxy Mode** is enabled.

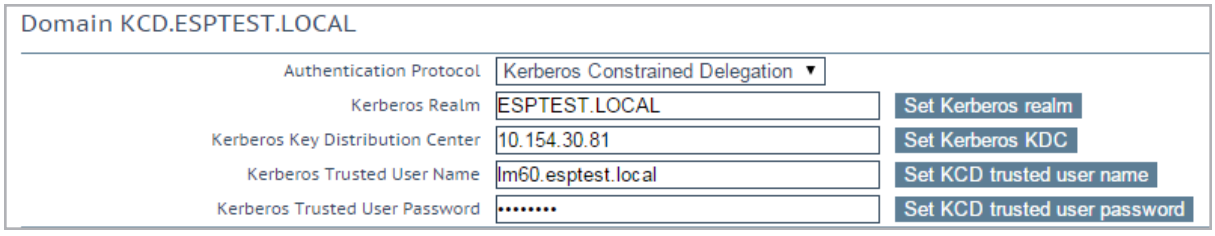
When **NTLM Proxy Mode** is enabled globally, the **Client Authentication Mode** in Virtual Services is called **NTLM-Proxy**. If **NTLM Proxy Mode** is disabled globally, the **Client Authentication Mode** in Virtual Services is called **NTLM**.

2.2.2 Configure the Server Side SSO Domain

To configure the server side SSO domain, follow the steps below in the LoadMaster WUI:

1. In the main menu, select **Virtual Services > Manage SSO**.

2. In the **Server Side Single Sign On Configurations** section, enter the name of the Single Sign On (SSO) domain in the **Name** text box and click **Add**.



3. Select **Kerberos Constrained Delegation** as the **Authentication Protocol**.
4. Enter the **Kerberos Realm** address and click **Set Kerberos realm**. Click **OK**.

The Kerberos realm is usually the domain. The Kerberos realm should be a name (not an IP address), such as **kemptech.local**. If an IP address is specified, authentication will not work. This field only accepts one name.

Double quotes are not allowed in this field.

5. Enter the **Kerberos Key Distribution Center name** and click **Set Kerberos KDC**. Click **OK**.

This field only accepts one Key Distribution Center. The Key Distribution Center address is usually the IP address of the Active Directory instance.

Double quotes are not allowed in this field.

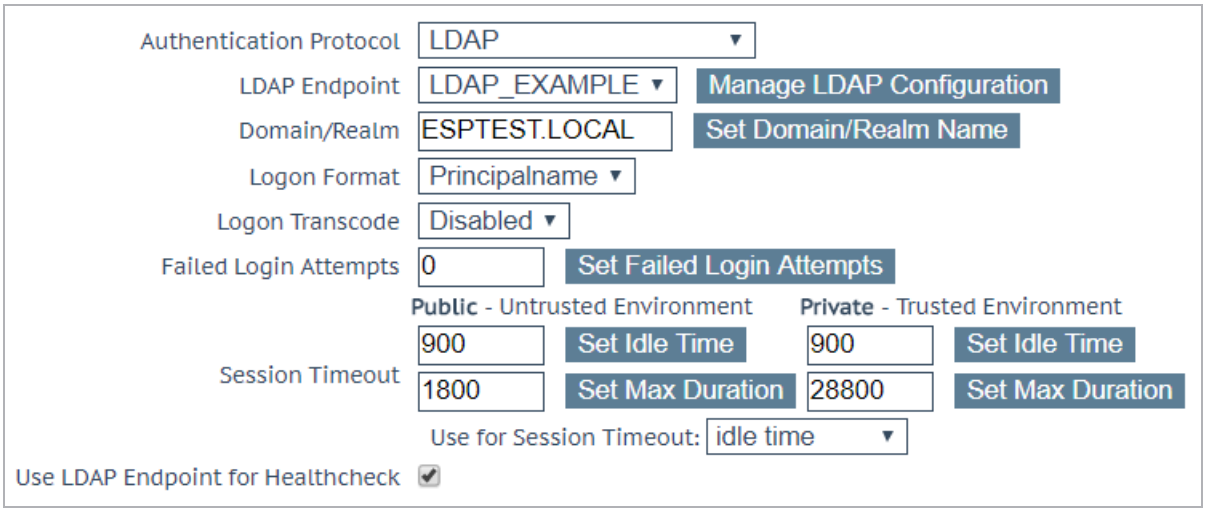
6. Enter the **Kerberos Trusted User Name** and click **Set KCD** trusted user name. Click **OK**.

The **Kerberos Trusted User Name** needs to be the same as the LoadMaster host name. The trusted user represents the LoadMaster. Refer to the **Kerberos Constrained Delegation, Feature Description** document for some further key requirements relating to the trusted user account.

Double and single quotes are not allowed in the **Kerberos Trusted User Name** field.

7. Enter the **Kerberos Trusted User Password** and click **Set KCD** trusted user password. Click **OK**.

2.2.3 Configure the Client Side SSO Domain



The client side SSO domain can be created by going to **Virtual Services > Manage SSO > Add** (in the **Client Side Single Sign On Configurations** section) and filling out the details as needed. The **Authentication Protocol** must be set to **LDAP** for NTLM authentication to work. An LDAP endpoint is required if Permitted Groups or Steering Groups are in use.

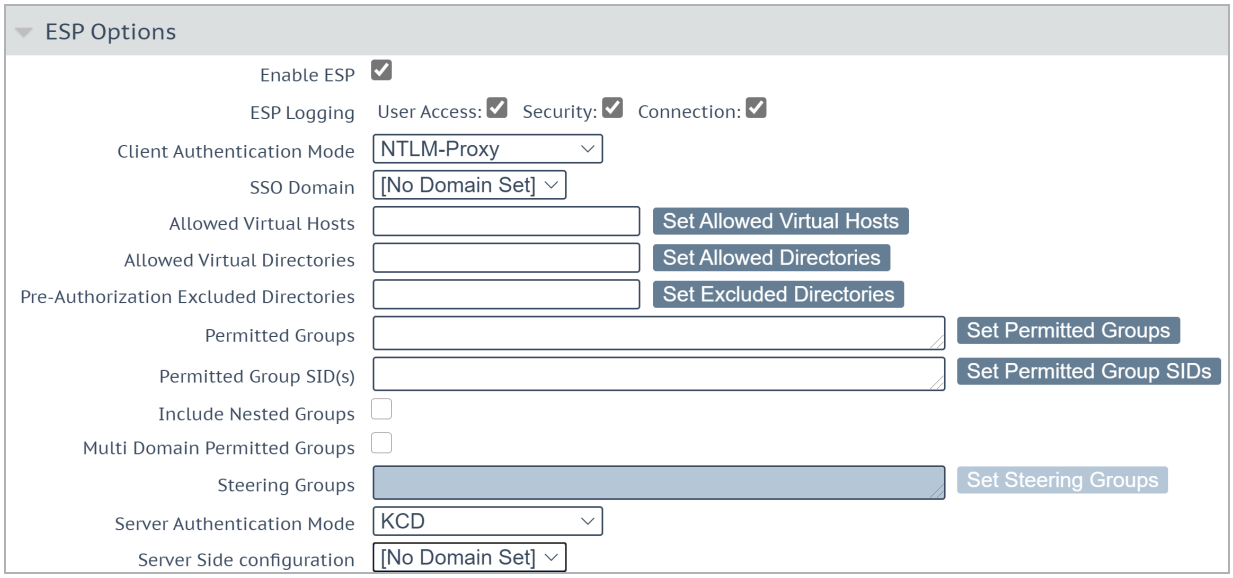
For information on configuring an LDAP endpoint, refer to the following knowledge base article: How to Configure an LDAP Endpoint.

2.2.4 Configure the Virtual Service

To configure a Virtual Service to use NTLM authentication, follow the steps below.

> These steps assume that the Virtual Service has already been set up and configured as needed (apart from the ESP settings). For further information on Virtual Services in general, refer to the **Virtual Services and Templates, Feature Description**. For further information on the different fields in the LoadMaster WUI, please refer to the **Web User Interface (WUI), Configuration Guide**.

1. In the main menu of the LoadMaster WUI, go to **Virtual Services > View/Modify Services**.
2. Click **Modify** on the relevant Virtual Service.
3. Expand the **ESP Options** section.



4. Select the **Enable ESP** check box to turn ESP on.

5. Select **NTLM** or **NTLM Proxy** as the **Client Authentication Mode**.

6. Select the client-side SSO domain that was created in the **Configure the Client Side SSO Domain** section in the **SSO Domain** drop-down list.

7. You can optionally assign **Alternative SSO Domains** if needed.

8. Set any **Allowed Virtual Hosts** and **Allowed Virtual Directories**, as needed.

9. Select the **Server Authentication Mode**.

You must ensure that NTLM is available as part of Integrated Windows Authentication (IWA) and that this is enabled on the Real Server for server-side authentication to work in both KCD and NTLM-Proxy Server Side authentication modes.

You must set the **Server Authentication Mode** to **KCD** and ensure there is an Server Side **SSO Domain** selected to use the following fields:

- **Pre-Authorization Excluded Directories**
- **Permitted Groups**
- **Permitted Group SID(s)**
- **Include Nested Groups**
- **Steering Groups**

10. Select the server-side SSO domain that was created in the **Configure the Server Side SSO Domain** section in the **Server Side configuration** drop-down list.

11. Configure any of the other ESP settings as needed.

> For further information on the ESP WUI options and ESP in general, please refer to the **Edge Security Pack (ESP), Feature Description**.

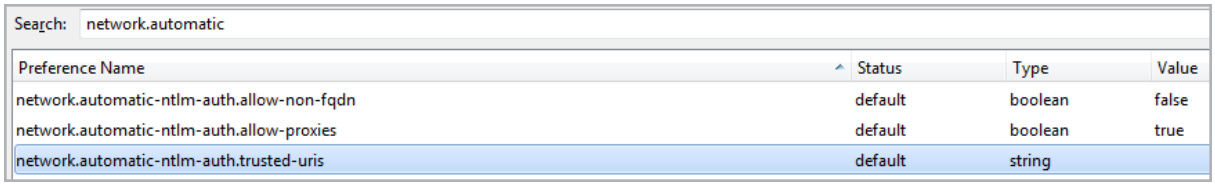
2.3 Configure Firefox to Allow NTLM (if needed)

In many organizations, Internet Explorer is configured to allow NTLM on internal sites, but Firefox is not. To configure Firefox to allow certain sites, follow the steps below:

1. Open Firefox.

2. In the address bar, type **about:config**.

3. A warning may appear, click the button to continue.



4. In the **Search** text box, enter **network.automatic**.

5. Double-click the network.automatic-ntlm-auth.trusted-uris entry.

6. Enter the relevant site address(s).

> Multiple sites can be added by separating them with a comma.

7. Click **OK**.

> Firefox may need to be restarted for the changes to take effect.

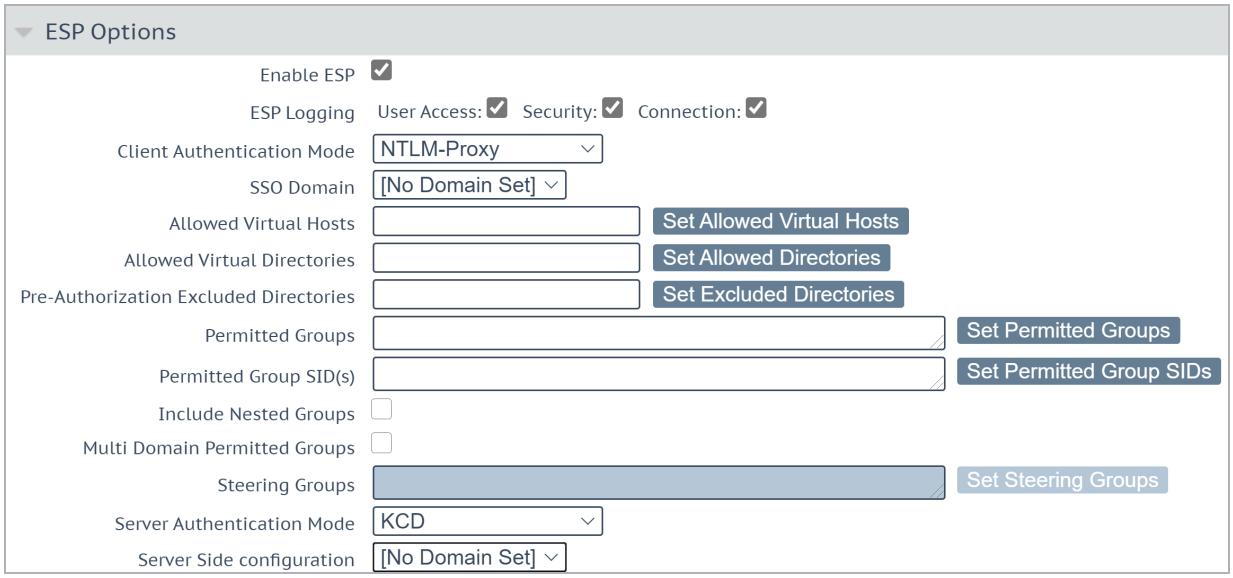
In some environments, the following three parameters might need to be updated:

- network.automatic-ntlm-auth.trusted-uris
- network.negotiate-auth.delegation-uris
- network.negotiate-auth.trusted-uris

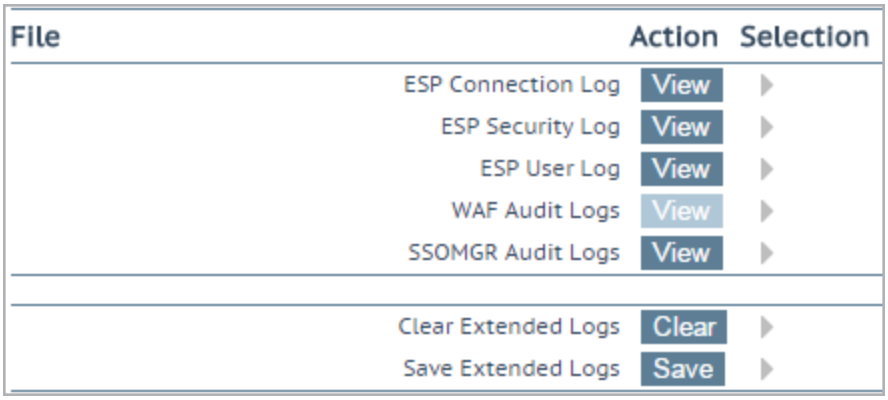
Also, the **signon.autologin.proxy** may need to be changed to **true** (double-click the parameter to change the value).

2.4 Troubleshooting

When troubleshooting problems with NTLM authentication in the LoadMaster, it can be useful to look at the ESP logs.



Various levels of ESP logs can be enabled per-Virtual Service by enabling the check boxes in the **ESP Logging** section.



These logs can then be viewed by going to **System Configuration > Logging Options > Extended Log Files**. For further information on the ESP logging, refer to the **Edge Security Pack (ESP), Feature Description**.

References

Unless otherwise specified, the following documents can be found at http://kemptechnologies.com/documentation.

Edge Security Pack (ESP), Feature Description

Web User Interface (WUI), Configuration Guide

Virtual Services and Templates, Feature Description

Kerberos Constrained Delegation, Feature Description

Last Updated Date

This document was last updated on 19 March 2021.