

NTLM

Feature Description

UPDATED: 28 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Table of Contents

1 Introduction **4**

1.1 Document Purpose 6

1.2 Intended Audience 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 Configure the Server Side SSO Domain 11

2.2.2 Configure the Client Side SSO Domain 13

2.2.3 Configure the Virtual Service 13

2.3 Configure Firefox to Allow NTLM (if needed) 16

2.4 Troubleshooting 17

2.5 JSON Web Token Validation 18

2.5.1 Configure JSON Web Token Validation 20

References **22**

Last Updated Date **23**

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

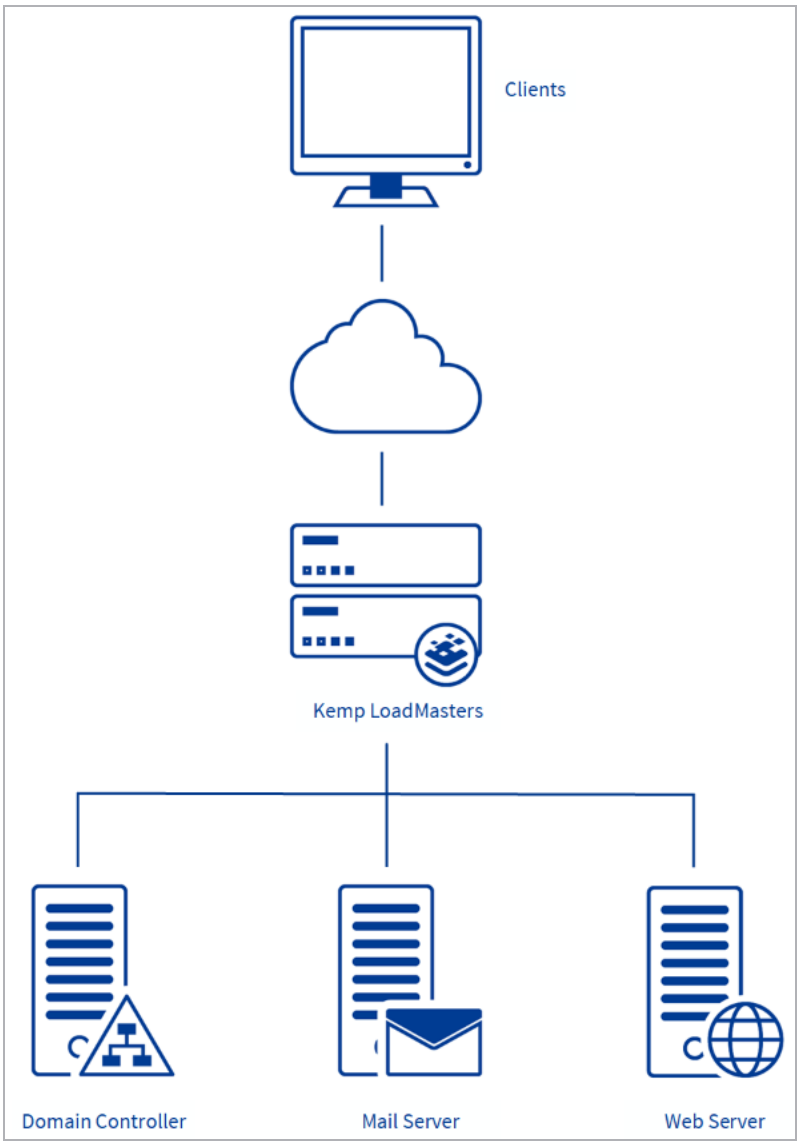
1 Introduction

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).

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



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.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

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.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

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.

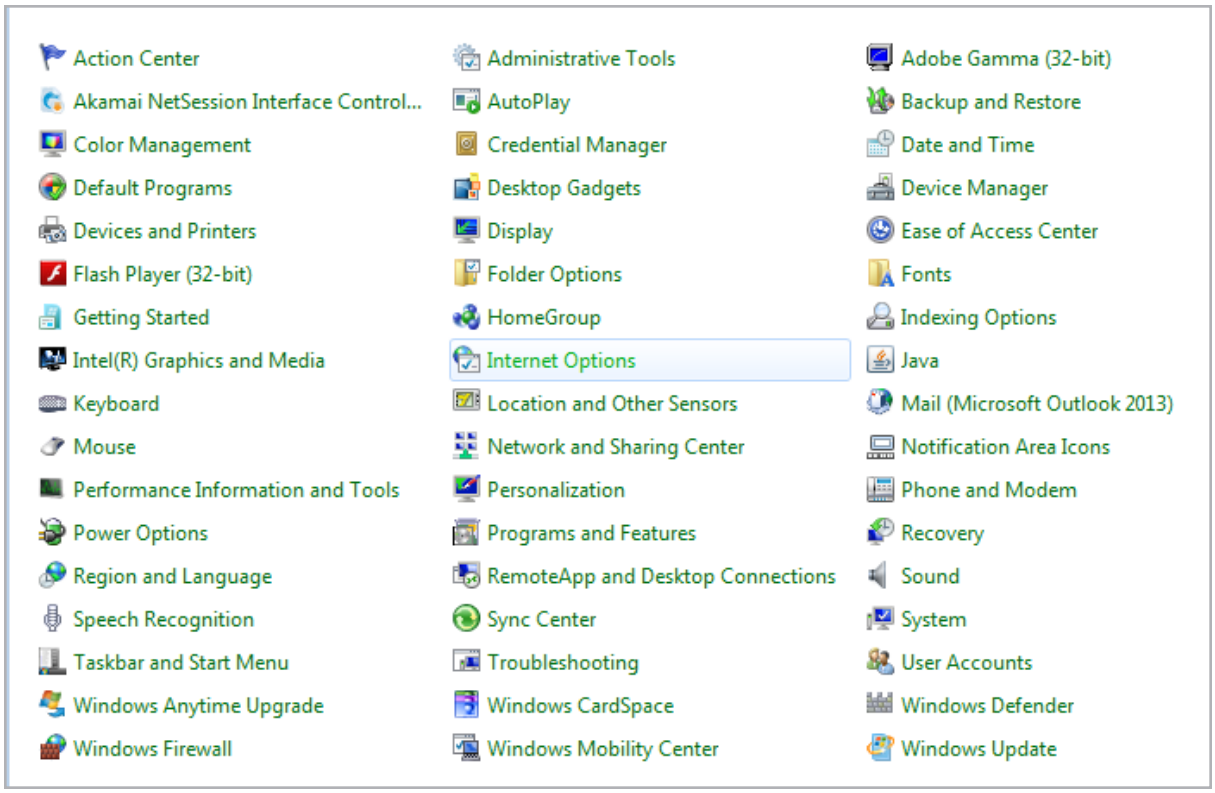
> NTLM authentication on the LoadMaster does not work with some Windows 10 security software, such as Credential Guard, which are designed not to support NTLM. As stated in the Credentials Guard documentation: “When you enable Windows Defender Credential Guard, you can no longer use NTLM classic authentication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

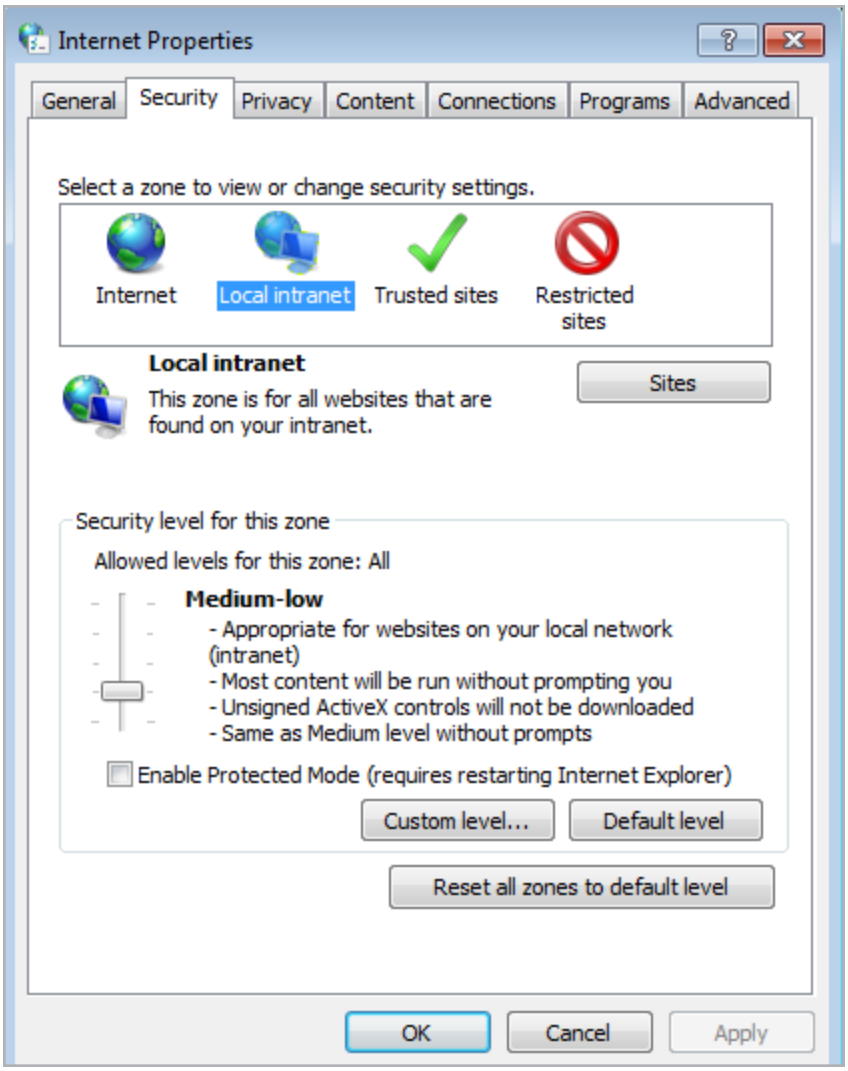
1. Click **Start** and select **Control Panel**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



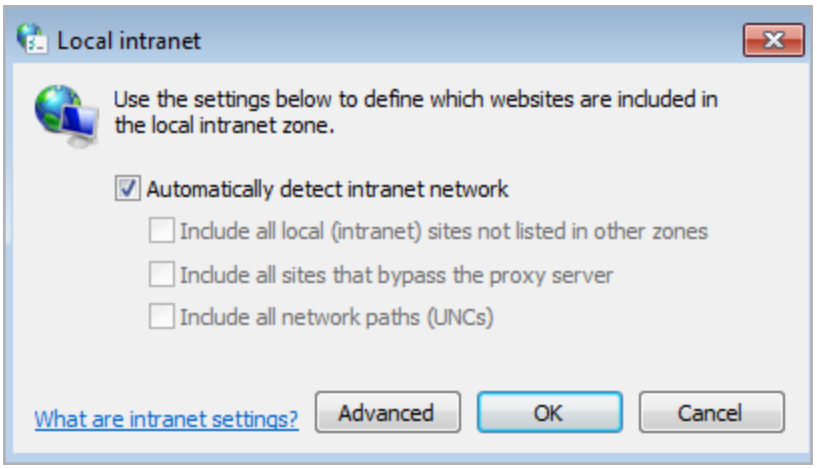
2. Click **Internet Options**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

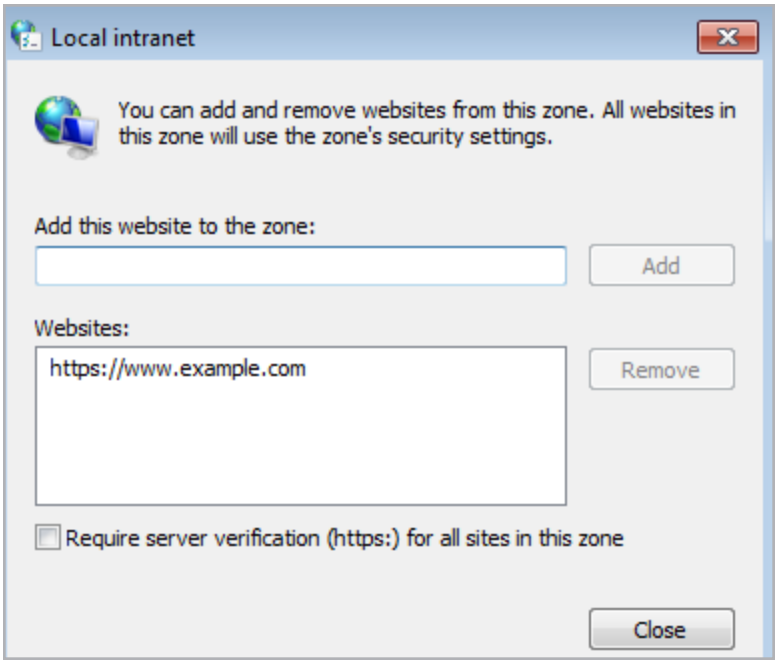


3. Select the **Security** tab.
4. Click **Local intranet**.
5. Click **Sites**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



6. Click **Advanced**.



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

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.2 Configure the LoadMaster

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.

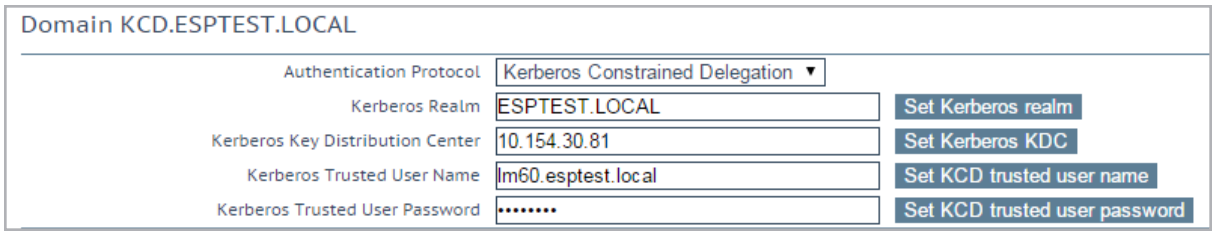
2.2.1 Configure the Server Side SSO Domain

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**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

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**.

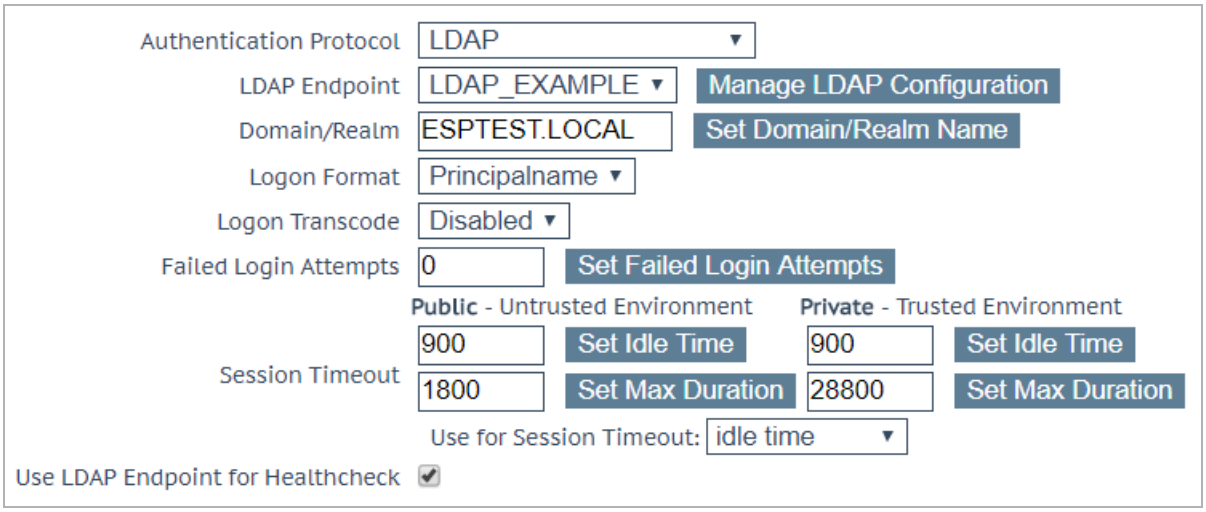
The **Kerberos Trusted User Name** needs to be the same as the LoadMaster host name. The trusted user represents the LoadMaster. Refer to the Kerberos Constrained Delegation, Feature Description document for some further key requirements relating to the trusted user account.

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**.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.2.2 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.

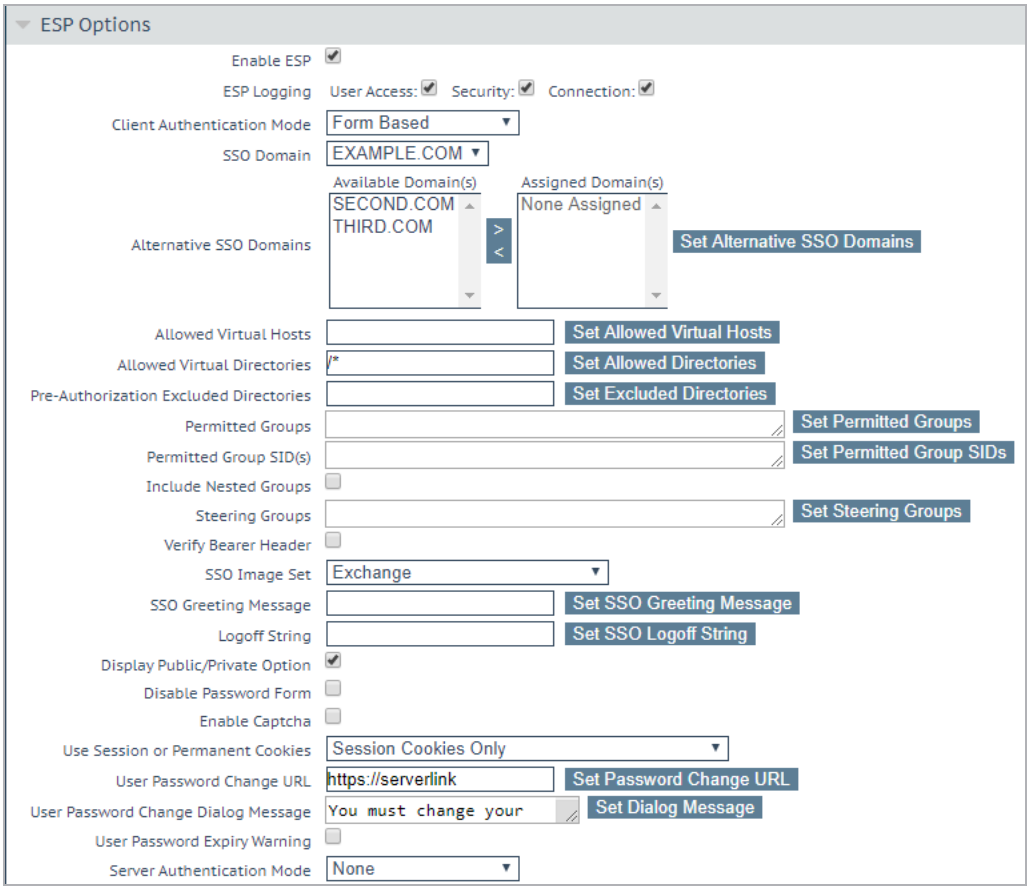
2.2.3 Configure the Virtual Service

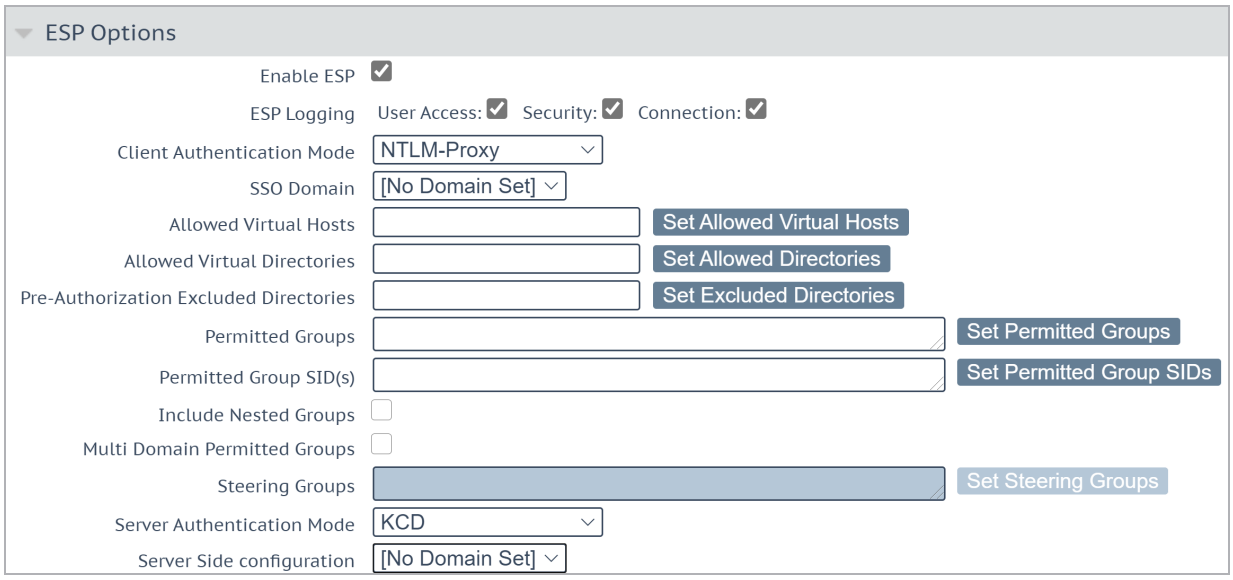
To configure a Virtual Service to use NTLM authentication, follow the steps below.

> 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. Expand the **ESP Options** section.

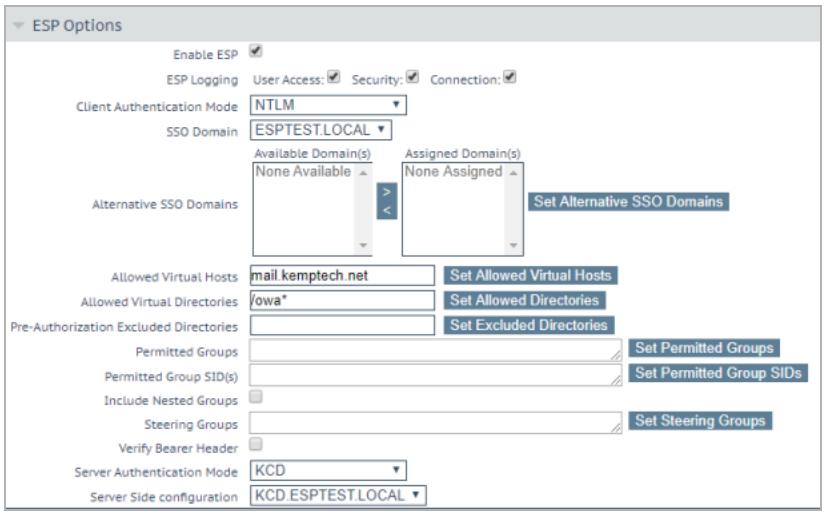
© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.





3. Expand the **ESP Options** section.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



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**

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

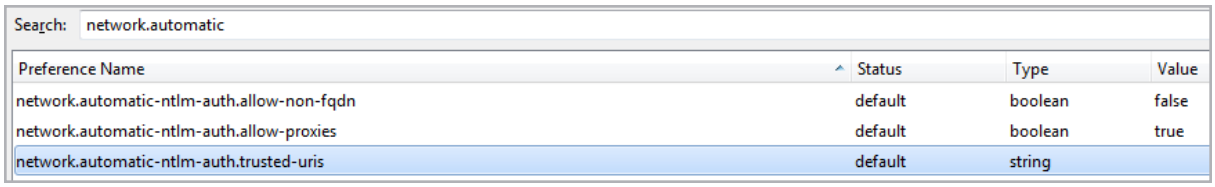
10. Select the server-side SSO domain that was created in the **Configure the Server Side SSO Domain** section in the **Server Side configuration** drop-down list.
11. Configure any of the other ESP settings as needed.

> 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:

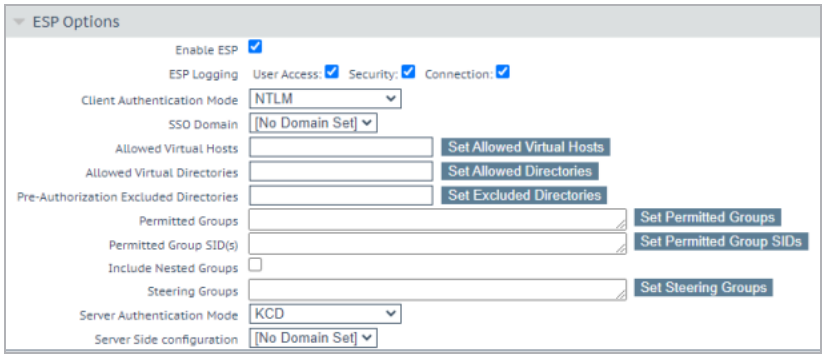
- network.automatic-ntlm-auth.trusted-uris
- network.negotiate-auth.delegation-uris
- network.negotiate-auth.trusted-uris

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

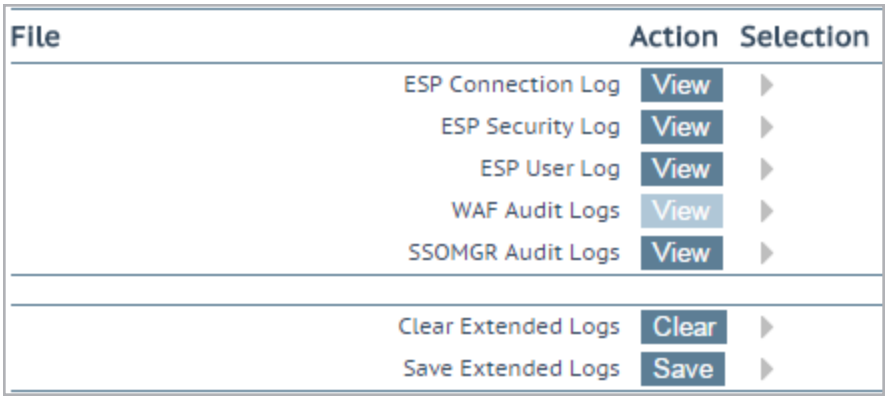
Also, the **signon.autologin.proxy** may need to be changed to **true** (double-click the parameter to change the value).

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.

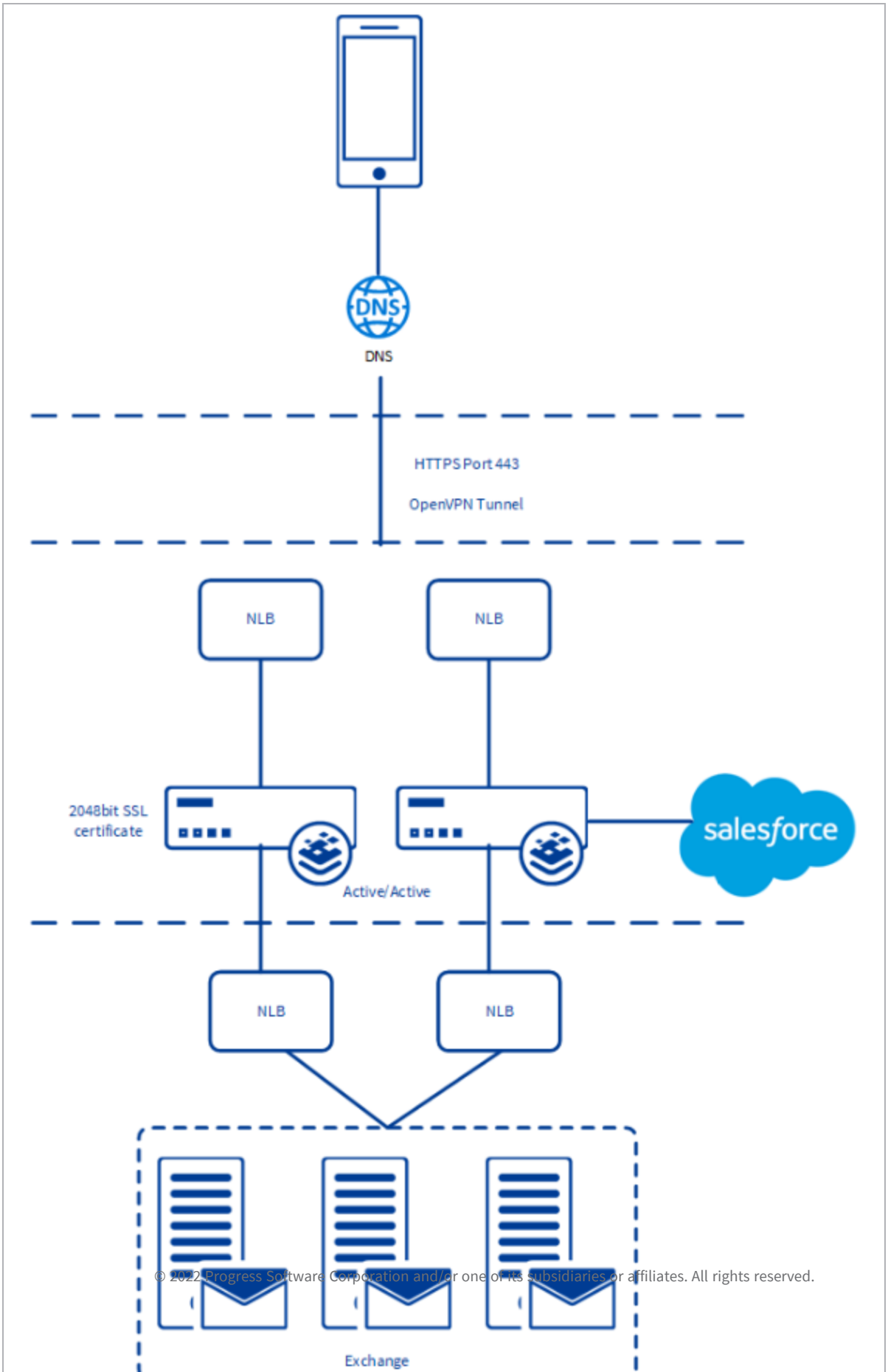


These logs can then be viewed by going to **System Configuration > Logging Options > Extended Log Files**. For further information on the ESP logging, refer to the Edge Security Pack (ESP), Feature Description.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

2.5 JSON Web Token Validation

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.



© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

The diagram above shows an example of the JSON web token validation workflow that is described below.

External client:

1. The external client makes a DNS request for mail.domain.com.
2. The client connects to AWS using OpenVPN tunnel.
3. The Network Load Balancer (NLB) forwards the request to the Kemp LoadMaster.
4. The LoadMaster decrypts and ESP authenticates the client using NTLM/KCD and packets are forwarded to the NLB.
5. The NLB forwards packets to the Exchange servers in the availability zone region.
6. The Salesforce (SFDC) plugin sends a bearer token into Exchange using an authenticated client over 443 and Content Policy.
7. The token is accepted and SFDC connects.

Internal client:

1. The internal client makes a request for mail.domain.com.
2. The client connects to the NLB.
3. The NLB forwards the request to the Kemp LoadMaster.
4. The LoadMaster decrypts and ESP authenticates the client using NTLM/KCD and packets are forwarded to the NLB.
5. The NLB forwards packets to the Exchange servers in the availability zone region.
6. The SFDC plugin sends a bearer token into Exchange using an authenticated client over 443 and Content Policy.
7. The token is accepted and SFDC connects.

2.5.1 Configure JSON Web Token Validation

To configure JSON web token validation, follow the steps below:

1. In the LoadMaster WUI, go to **Virtual Services > View/Modify Services** and click **Modify** on the relevant Virtual Service.
2. Expand the **ESP Options** section.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

3. Ensure **NTLM** is selected as the **Client Authentication Mode**.

4. Configure any other settings as needed and as detailed throughout this document.

5. Select the **Verify Bearer Header** check box.

6. Select the relevant certificate/key used to decrypt the bearer header token from the **Bearer Header Validation Certificate** drop-down list (this must first be uploaded to the LoadMaster by going to **Certificates & Security > SSL Certificates > Import Certificate**).

7. You can enter up to five bearer header validation strings (comma-separated list) in the **Bearer Header Validation Text** field.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

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

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

Last Updated Date

This document was last updated on 28 July 2023.

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.