Progress®
Kemp® LoadMaster®

Feature Description Edge Security Pack ESP

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: Introduction 5

LoadMaster and Azure Entra Integration 5

Chapter 2: The LoadMaster Edge Security Pack (ESP) 6

End Point Authentication for Pre-Auth. 8

Chapter 3: ESP Web User Interface (WUI) Options 10

ESP Options 10

SMTP Virtual Services and ESP 32

Limitations of Using Regular Expressions in the LoadMaster WUI 33

LDAP Configuration. 33

Manage SSO Options 35

Single Sign On Domains 36

Backup/Restore. 49

Debug Options 52

Enable SSOMGR Debug Traces 52

Flush SSO Authentication Cache. 54

SSO LDAP Server Timeout 54

Linear SSO Log Files 54

Miscellaneous Options 54

L7 Configuration 54

Network Options. 56

Logging Options 57

Chapter 4: Setting up a Virtual Service with ESP 61

Create a Single Sign-On (SSO) Domain. 61

Create a Virtual Service 63
Configure a Simple Mail Transfer Protocol (SMTP) ESP Service 69

Chapter 5: Client Certificate Authentication with No Server Side Authentication 71

Chapter 6: RADIUS Two Factor and LDAP Authentication. 72

Chapter 7: PIV Smart Card Support 73

Chapter 8: Troubleshooting. 75

Chapter 9: Support for Additional Security Headers Added 76

Chapter 10: References 77

Chapter 11: Appendix A - Expected Normalization Results (for LDAP Only) from Example Configurations 78

1

Introduction

Progress Kemp has built a large and loyal install base across a range of market segments, applications and geographies. These include a large number of customers who have deployed Progress Kemp's LoadMaster load balancers in conjunction with Microsoft workloads. As a part of the solution for Microsoft workloads, a key component has historically been Microsoft's Forefront Threat Management Gateway (TMG). One key feature of TMG was that it offered customers a way to publish and protect workload servers such as Exchange Client Access Servers, especially in Internet-facing deployments where a clean separation between critical infrastructure and the public internet is essential.

Since the TMG product is no longer supported, Progress Kemp has extended the LoadMaster platform with the Edge Security Pack (ESP), to replace and enhance the functionality that was available in TMG. This separately available feature pack builds on the existing core technologies that have enabled successful joint deployments of TMG and LoadMaster in internet-facing Microsoft workloads.

Note: ESP functionality is only available on certain subscriptions. Please contact a Progress Kemp representative if needed.

Contents

- LoadMaster and Azure Entra Integration

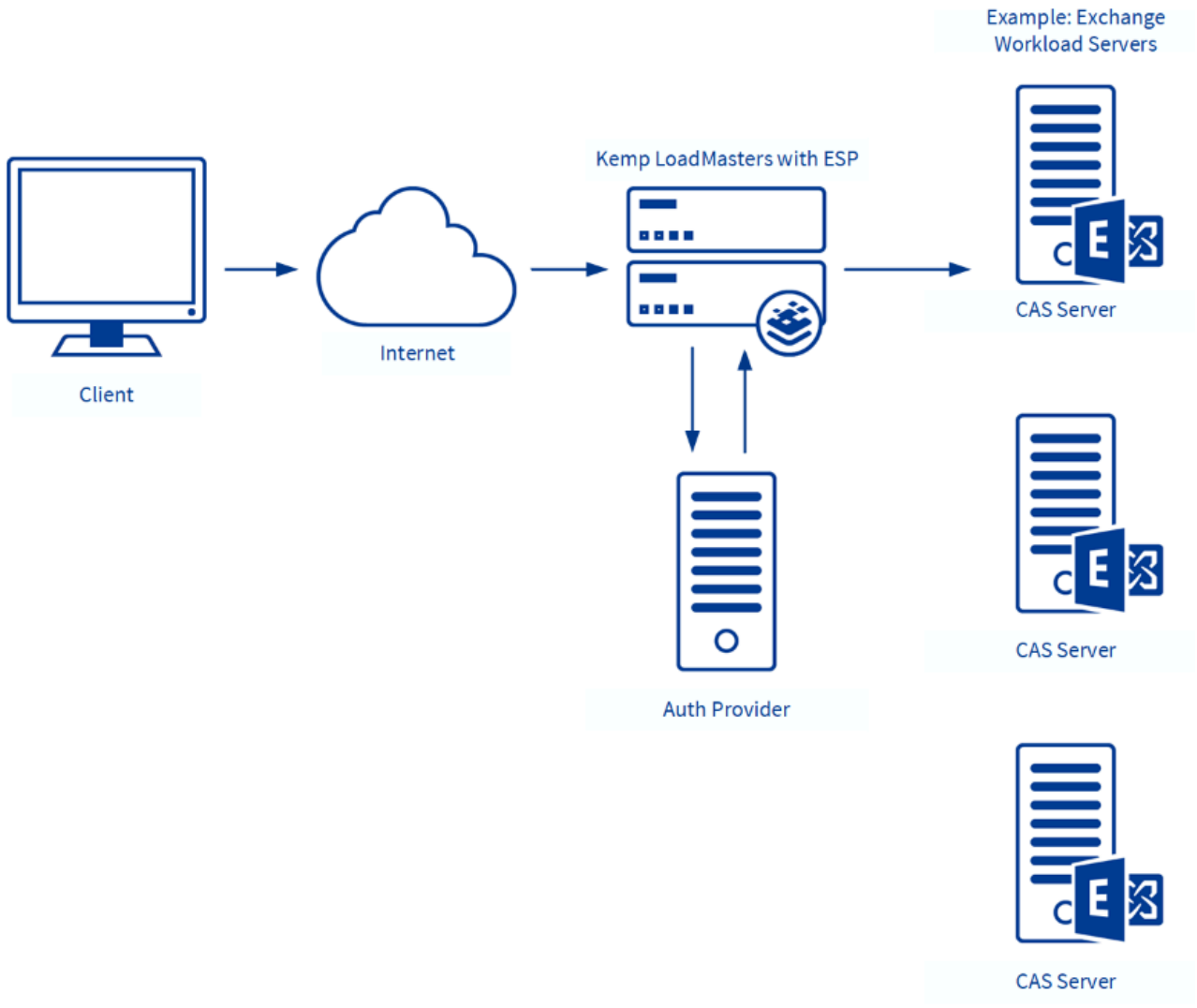
LoadMaster and Azure Entra Integration

For details and step-by-step instructions on integrating the LoadMaster with Microsoft Entra, refer to the following Microsoft tutorial: Microsoft Entra SSO integration with Kemp LoadMaster Microsoft Entra integration.

2

The LoadMaster Edge Security Pack (ESP)

The LoadMaster along with the Edge Security Pack (ESP) delivers a solution to customers who would have previously deployed TMG to publish their Microsoft applications.



The basic flow for ESP authentication is shown in the diagram above:

- Traffic from the client goes to the LoadMaster.
- The LoadMaster may present an authentication form asking the user to enter credentials.
- The Authentication Provider server then allows or rejects the request.
- If successful, the traffic is passed to the Real Servers.

To help protect a service from threat actors, the LoadMaster can perform authentication for HTTP/HTTPS services before the user can gain access to a web resource. To do this, you can leverage ESP to create a Single Sign On (SSO) that offers the following features:

- End point authentication for pre-authentication
- Persistent logging and reporting for user logging
- Single Sign-On (SSO) across Virtual Services
- LDAP Authentication from the LoadMaster to the Active Directory
- Basic authentication communication from a client to the LoadMaster

- Dual-factor authentication including Azure Multi-Factor Authentication (MFA) or RSA tokens
- CAPTCHA verification

Note: A reboot is required after upgrading older versions of the LoadMaster to an ESP license.

Contents

- End Point Authentication for Pre-Auth

End Point Authentication for Pre-Auth

Clients who are trying to access Virtual Services on the LoadMaster will have to provide Authentication information which is used by the ESP to validate the clients' right to access the service. In the event of success, the client is permitted to access the service, and in the event of failure the client is blocked until valid credentials are provided.

Persistent Logging and Reporting for User Logging

When clients try to access a service, an appropriate message is logged to allow monitoring by the administrator.

Single Sign-On Across Virtual Services

The LoadMaster is designed to handle multiple Virtual Services supporting unique workloads. Access to these services can be authenticated through a single point of contact, by associating them with the same Single Sign-On (SSO) Domain.

Note: The Virtual Services need to be on the same domain for this to work, for example **ecp.example.com** and **www.example.com**.

SSO in ESP will enable clients to only enter the authentication information when accessing the first Virtual Service and then this same information is used to access other services associated with the Single Sign-On Domain. Therefore, a client accessing Exchange will also be able to access SharePoint and other workloads if they are associated with the same Single Sign-On Domain.

LDAP Authentication from the LoadMaster to the Active Directory

Active Directory is the standard Authentication Provider for Microsoft workloads. LoadMaster will support the key connection types between the LoadMaster and the Active Directory.

Note: For instructions on how to set up the server-side configuration, please refer to the relevant vendor's documentation.

Basic Authentication Communication from a Client to the LoadMaster

LoadMaster with ESP currently supports basic and form-based authentication between the client and the LoadMaster, providing clients with an optimum authentication experience.

Large and small businesses are deploying large numbers of internet-facing applications to support ever expanding business requirements. This rapidly growing number of servers needs to be scalable and highly reliable. Above all, the access to these servers and services needs to be secure. With the addition of ESP, the LoadMaster will continue to deliver on customer security requirements for internet facing applications in a world without Microsoft Forefront TMG, while continuing to address requirements for feature-rich and cost-effective scalability and high reliability.

Note: For instructions on how to set up the server-side configuration, please refer to the relevant vendor's documentation.

Dual-factor Authentication

Some authentication mechanisms assume a dual-factor approach where both the Active Directory and a secondary mechanism are used in sequence. For these, the form includes the username, password and also a passcode which is checked after the username and password.

3

ESP Web User Interface (WUI) Options

The sections below describe the ESP WUI Options. These sections refer to various different sections of the LoadMaster WUI. To log in to the LoadMaster WUI, navigate to **https://<WUIIPAddress>** in a web browser and enter credentials.

Contents

- ESP Options
- LDAP Configuration
- Manage SSO Options
- Backup/Restore
- Debug Options
- Miscellaneous Options
- Logging Options

ESP Options

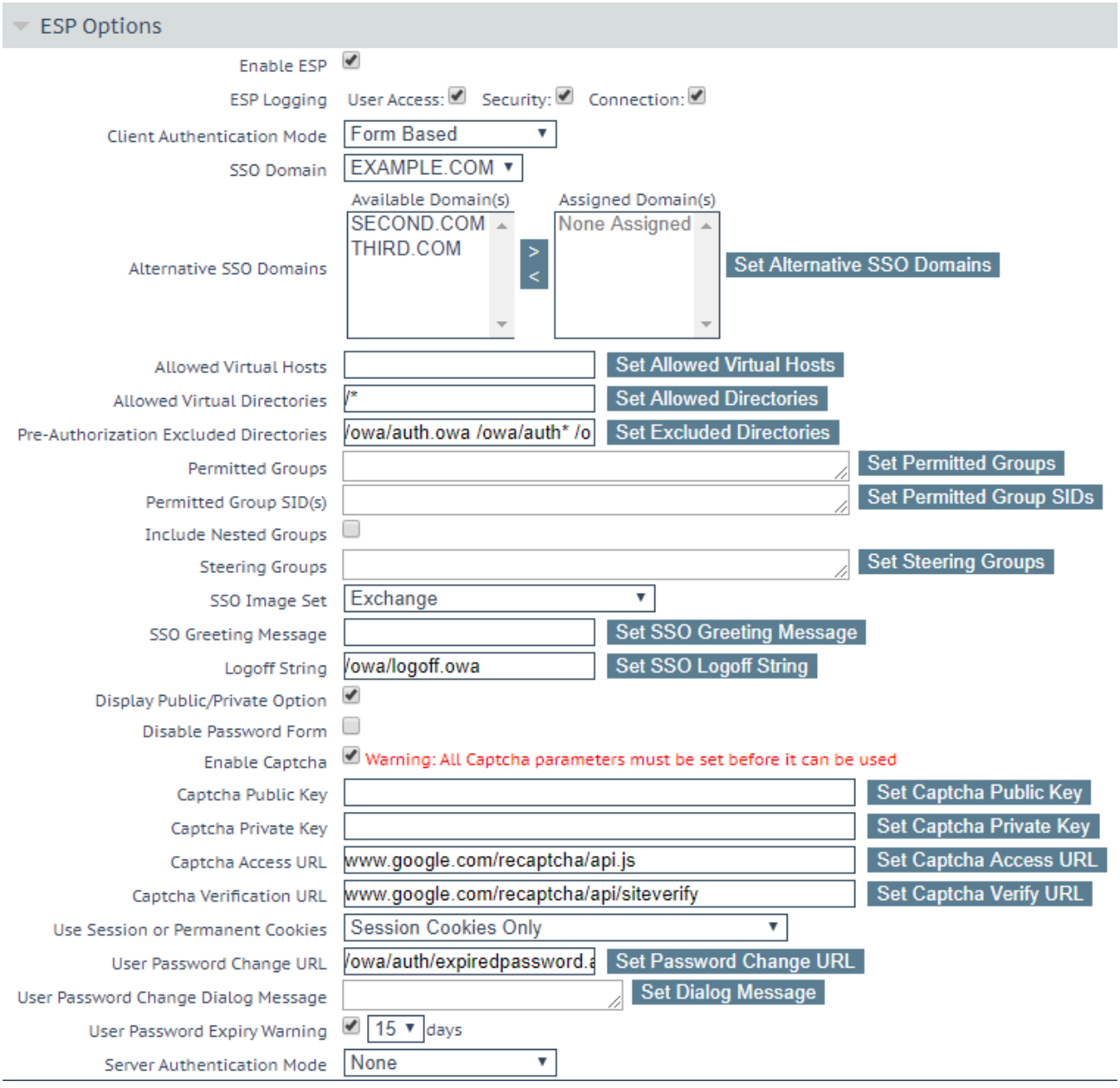
This section refers to the **ESP Options** section of the Virtual Service modify screen. To get to this section – in the LoadMaster WUI go to **Virtual Services > View/Modify Services**, click **Modify** on the relevant Virtual Service and then expand the **ESP Options** section. The **ESP Options** are also available for SubVSes.

The ESP feature must be enabled before the options can be configured. To enable the ESP function, please select the **Enable ESP** checkbox.



The full **ESP Options** will appear.

Note: The ESP feature can only be enabled if the Virtual Service is an HTTP, HTTPS, or SMTP Virtual Service.



Enable ESP

Enable or disable the ESP feature set by selecting or deselecting the **Enable ESP** checkbox.

ESP Logging

There are three types of logs stored in relation to the ESP feature. Each of these logs can be enabled or disabled by selecting or deselecting the relevant checkbox. The types of log include:

- **User Access:** logs recording all user logins. These logs include the full URL the client IP has requested, along with the Uniform Resource Identifier (URI).
- **Security:** logs recording all security alerts
- **Connection:** logs recording each connection

Logs are persistent and can be accessed after a reboot of the LoadMaster. The ESP logs can be found by navigating to **System Configuration > Logging Options > Extended Log Files** in the main menu of the LoadMaster WUI.

Note: When using SNMP monitoring of ESP-enabled Virtual Services that were created using a template, ensure to monitor each SubVS directly rather than relying on the master service. This is because the Authentication Proxy sub-service will always be marked as up and, as a consequence, so will the master service.

Client Authentication Mode

Specifies how clients attempting to connect to the LoadMaster are authenticated. The following are the types of methods available:

- **Delegate to Server:** the authentication is delegated to the server
- **Basic Authentication**: standard Basic Authentication is used
- **Form Based:** clients must enter their user details within a form to be authenticated on the LoadMaster

---

Note: Please keep in mind - if UTF-8 encoding is utilized, the maximum number of characters for the username or password which is used to access an ESP-enabled Virtual Service is (in theory) 30 characters each. However, if a combination of 1 and 2 byte characters are used, this limit could be increased. The maximum limit is 63 characters each if the characters are all 1 byte encoded.

- **Client Certificate:** clients must present the certificate which is verified against the issuing authority
- **NTLM/NTLM-Proxy:** NTLM credentials are based on data obtained during the interactive logon process and consist of a domain name, a user name and a one-way hash of the user’s password

---

Note: NTLM does not forward credentials to the LoadMaster when Windows 10 Credential Guard is enabled.

- **SAML:** The LoadMaster supports SAML, playing the role of a SAML service provider. The service provider provides secure, gated access to a resource.
- **Pass Post:** In LoadMaster firmware version 7.2.53, a new mode called **Pass Post** was introduced. With this change introduced, users with valid credentials using the Workspace client app can successfully log in (using Single Sign On (SSO)) using POST-based authentication on the client side and **Form Based** Authentication (FBA) on the server side and access is granted to the VDI workspace.

- **OIDC/OAUTH:** Open ID Connect (OIDC) is an authentication protocol based on the OAuth2 protocol used to enable Single Sign On of users across multiple applications via a single Identity Provider. OIDC uses the standardized message flows from OAuth2 to provide identity services.

Note: The remaining fields in the **ESP Options** section will change based on what is selected as the **Client Authentication Mode**.

SSO Domain

Select the Single Sign-On (SSO) Domain within which the Virtual Service is included.

Please refer to the Create a Single Sign-On (SSO) Domain section for further information on configuring SSO Domains. An SSO Domain must be configured to correctly configure the ESP feature.

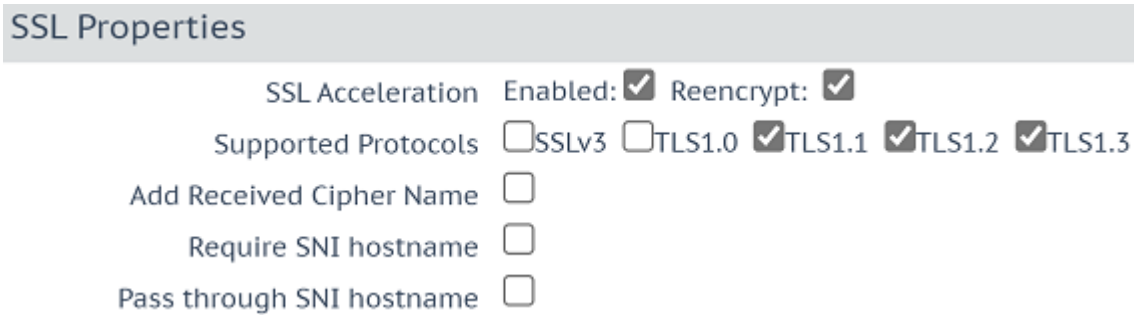
Note: Only SSO domains with the **Configuration type** of **Inbound Configuration** are shown as options in this **SSO Domain** field.

Alternative SSO Domains

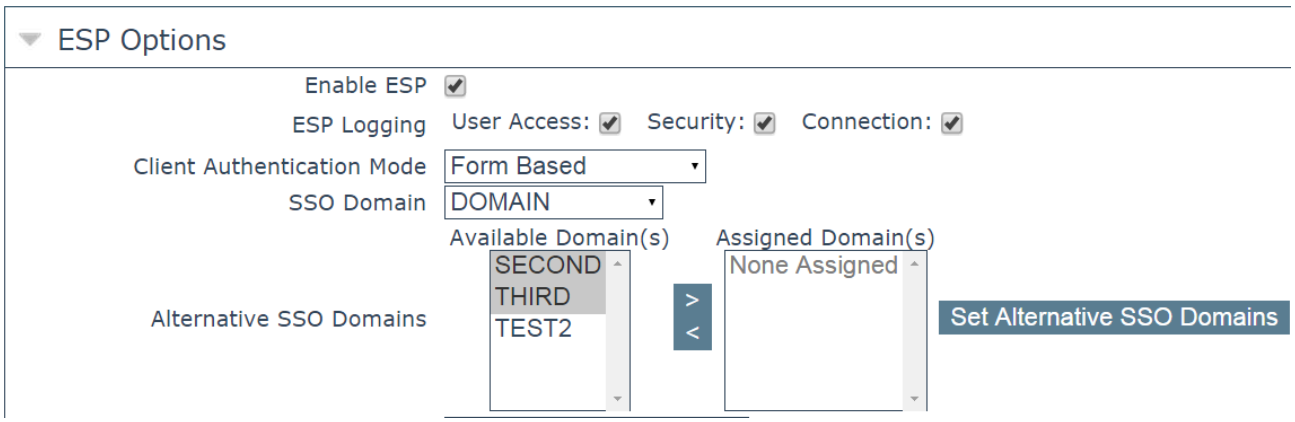
Many organizations use extranets to share information with customers and partners. It is likely that extranet portals will have users from two or more Active Directory domains. Rather than authenticating users from individual domains one at a time, assigning **Alternative SSO Domains** gives the ability to simultaneously authenticate users from two or more domains using one Virtual Service.

Note: This option appears only when more than one domain has been configured and when the **Authentication Protocol** for the SSO domains are set to **LDAP**.

Please refer to the Create a Single Sign-On (SSO) Domain section for further information on configuring **SSO Domains**.

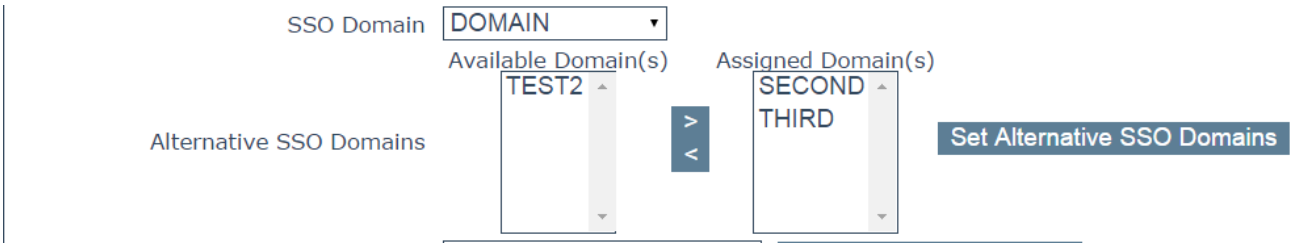


Before configuring the **ESP Options** to use **Alternative SSO Domains** ensure that, in the **SSL Properties** section, the **Enabled** and **Reencrypt** tick boxes are selected.



The domain name which appears in the **SSO Domain** drop-down list is the default domain. This is also the domain which is used if only one is configured.

Previously configured alternative domains appear in the **Available Domain(s)** list.



To assign alternative SSO Domains:

1. Highlight each of the domains you wish to assign and click the **>** button. An assigned domain is a domain which can be authenticated using a particular Virtual Service. All domains which appear as available may be assigned to a Virtual Service.
2. Click the **Set Alternative SSO Domains** button to confirm the updated list of Assigned Domain(s).
3. Choose **Basic Authentication** from the **Server Authentication Mode** drop-down list.

Note: When logging in to a domain using the ESP form, users should enter the name of the SSO Domain if an alternative domain needs to be accessed. If no domain name is entered in the username, users are, by default, logged on the domain entered in the default SSO Domain drop-down list.

To view the status of the Virtual Services, click **Virtual Services** and **View/Modify Services**.

A list of the **Virtual Services** displays showing the current status of each service.

If alternative domains are assigned and there is an issue with a particular domain, the affected domain name is indicated in the **Status** column.

Allowed Virtual Hosts

The Virtual Service will only be allowed access to specified virtual hosts. Any virtual hosts that are not specified are blocked.

Enter the virtual host name(s) in the **Allowed Virtual Hosts** field and click the **Set Allowed Virtual Hosts** button to specify the allowed virtual hosts. Multiple, space-separated host names can be entered here.

If a Virtual Service is configured with non-standard HTTP/HTTPS ports, ensure the Virtual Service WebsiteName:Port is entered in the **Allowed Virtual Hosts** text box to allow the HTTP/HTTPS request to pass the ESP check. For example, if the requested Virtual Service website name is **sample.com** and the non-standard port is **8888**, ensure the **Allowed Virtual Hosts** text box contains **sample.com:8888**. Alternatively, you could use a wildcard symbol (*****) to allow any port number, for example, **sample.com:***.

Multiple domains may be specified within the text box allowing many domains to be associated with the SSO Domain.

The use of regular expressions is allowed within this text box. The LoadMaster supports Shell regular expressions in this field, where ***** is a wild card and **?** is a single character. An example is ***.example.com** which indicates all sub-domains under example.com.

Note: If you use quotes in regular expressions in the LoadMaster WUI, there are limitations. For more information, refer to the section Limitations of Using Regular Expressions in the LoadMaster WUI.

Note: If this text box is left blank, the Virtual Service is blocked.

Note: If the Virtual Service IP address is entered in the **Allowed Virtual Hosts** field, the login process will fail. For testing purposes, please modify your Hosts file if a proper DNS entry cannot be made.

Allowed Virtual Directories

The Virtual Service will only be allowed access to the specified virtual directories, within the allowed virtual hosts. Any virtual directories that are not specified are blocked.

Enter the virtual directory name(s) in the **Allowed Virtual Directories** text box and click the **Set Allowed Virtual Directories** button to specify the allowed virtual directories. Multiple space-separated names can be entered here.

The use of Shell regular expressions is allowed within this text box.

Pre-Authorization Excluded Directories

Any virtual directories specified within this field will not be pre-authorized on this Virtual Service and are passed directly to the relevant Real Servers. Multiple space-separated directories can be entered here.

The use of Shell regular expressions is allowed within this text box.

Permitted Groups

Specify the groups that are allowed to access this Virtual Service. When set, if a user logs in to a service published by this Virtual Service, the user must be a member of at least one of the groups specified.

Note: When using the **Permitted Groups** field in **ESP Options**, ensure that the selected Permitted Groups must exist inside the configured SSO domain. For example, if the **SSO Domain** is set to webmail.example and the selected permitted groups are part of .example.com domain instead of webmail domain, it will not work. In this case user needs to set the domain .example.com to function correctly.

If a user attempts to log in and they are not a member of a permitted group, a message will appear in the logs, similar to the example below:

Blocked access, user exampleuser primary group qa not in approved groups for VS172.21.42.11

Multiple groups are supported per Virtual Service up to a maximum of 2048 characters in length. Performance may be impacted if a large number of groups are entered. Groups entered in this field are validated using a Lightweight Directory Access Protocol (LDAP) query.

Some guidelines about this field are as follows:

- All groups specified must be valid on the Active Directory behind the SSO domain associated with the Virtual Service
- Multiple groups must be separated by a semi-colon

Note: A space-separated list does not work because most groups contain a space in the name, for example **IT Users**.

- Do not use the **Domain Users** group because it is a default primary group for new users.
- The authentication protocol of the SSO domain must be LDAP
- The groups should be specified by Common Name, not by fully distinguished name, for example **Test Group**
- When using permitted groups in SubVSs, if you have groups called **OWAGroup** and **ECPGroup**, for example, users in each group have access to each other's SubVS. This is due to the single sign on nature of ESP.
- Permitted groups only work when the LDAP Endpoint has a username in the format *username***@***domain***.com** or just administrator/Admin (as long as it is an administrator account), or if there is no username configured.
- Do not enter the same group name in both the **Permitted Groups** and **Steering Groups** fields. This causes a conflict. When you specify a steering group, it is assumed to behave like a permitted group, so you do not need to enter the same group in both the **Permitted Groups** and **Steering Groups** fields.

Permitted Groups SID(s)

This field is the equivalent of the **Permitted Groups** field. If specifying permitted groups, you can complete either the **Permitted Groups** field or the **Permitted Groups SID(s)** field (security identifiers).

In the **Permitted Group SID(s)** field you can specify the Group SIDs that are allowed to access this Virtual Service. After you type the groups, click **Set Permitted Group SIDs**.

This field allows a list of group SIDs of up to 64 bytes in length (192 characters in the format *NN NN NN*).

Each group is separated by a semi-colon. Spaces are used to separate bytes in certain group SIDs. Here is an example:

S-1-5-21-3763804817-1170992687-1336323834-1151

SIDs can be found by using the **get-adgroup-Identity GroupName** command.

Include Nested Groups

This field relates to the **Permitted Groups** setting. Enable this option to include nested groups in the authentication attempt. If this option is disabled, only users in the top-level group are granted access. If this option is enabled, users in both the top-level and first sub-level group are granted access. There is a

theoretical limit of approximately six nested groups.

Multi Domain Permitted Groups

In LoadMaster firmware version 7.2.52, a new check box was added to the **ESP Options** section of the Virtual Service modify screen called **Multi Domain Permitted Groups**. This check box is configurable with the following client authentication modes:

- Basic Authentication
- Form Based
- Client Certificate
- NTLM

When **Multi Domain Permitted Groups** is enabled, the LoadMaster checks for permitted group membership within all sub-domains under the top-level domain.

Note: The **Multi Domain Permitted Groups** option works with the **Permitted Groups**, **Permitted Group SID(s)**, and **Include Nested Groups**.

If **Multi Domain Permitted Groups** is disabled, users must be in the same domain or sub-domain that the user profile is defined, or the group check fails.

The **Multi Domain Permitted Groups** option is disabled by default.

The **Include Nested Groups** option works with **Multi Domain Permitted Groups**. For example, if you have group1 in server1 and group2 inside group1 in the same server with different users, those users can be authenticated if both **Include Nested Groups** and **Multi Domain Permitted Groups** are enabled.

Steering Groups

Steering groups can be used to steer client traffic to individual Real Servers in a Virtual Service based on the Active Directory (AD) group membership of users initiating client traffic. An example scenario would be a Virtual Service which has four Real Servers. Two Real Servers could be configured to have a primary association with Active Directory Group 1 and two Real Servers could be configured to have a primary association with AD Group 2. When a user attempts to access the Virtual Service, their group membership will be verified and the information used to steer their request to the appropriate Real Servers. If the Real Servers selected based on group membership are not available, the default behavior is to fall back to the assigned scheduling method for the Virtual Service.

For further information, refer to the ESP Steering Groups Technical Note.

Note: Steering groups are not available if using **Basic Authentication**, **Client Certificate**, or **SAML** authentication.

Enter the Active Directory group names that will be used for steering traffic in the Steering Groups field and click **Set Steering Groups**.

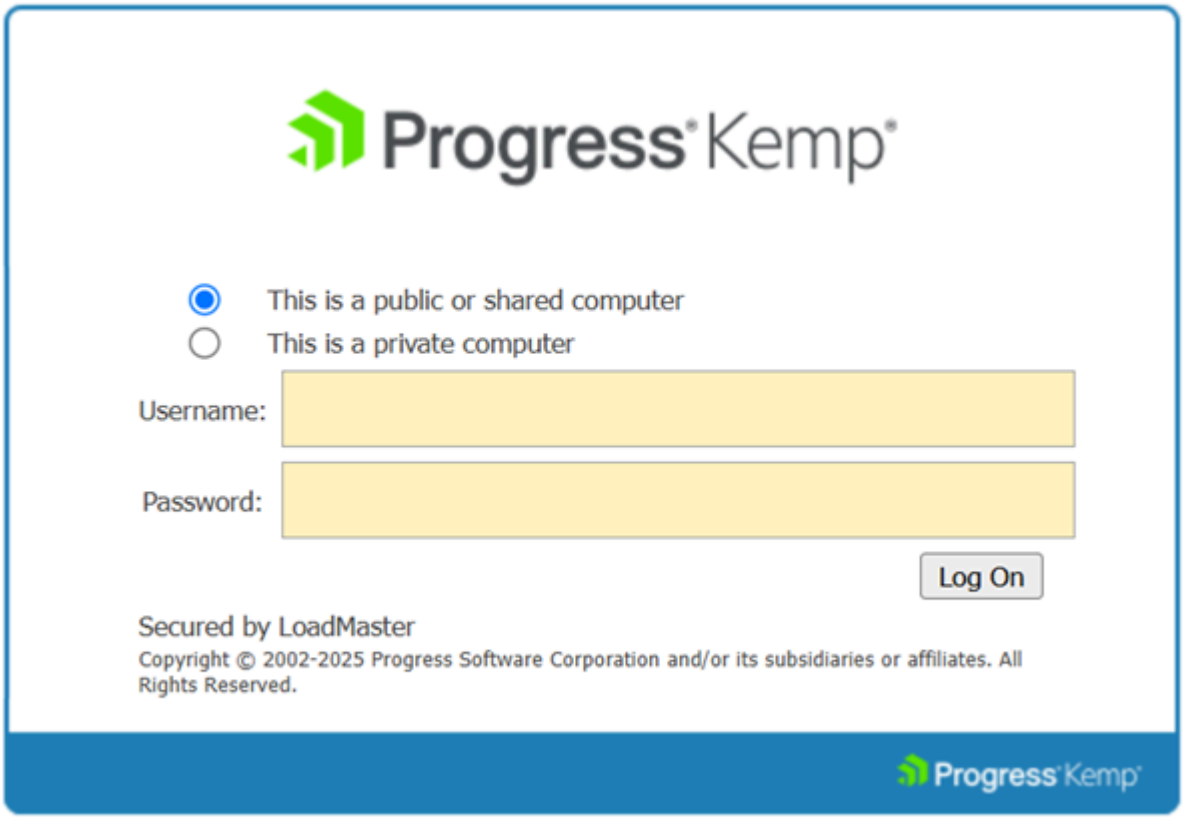
Use a semi-colon to separate multiple group names. Multiple groups are supported per Virtual Service up to a maximum of 2048 characters in length.

The steering group index number will correspond to the location of the group in this list.

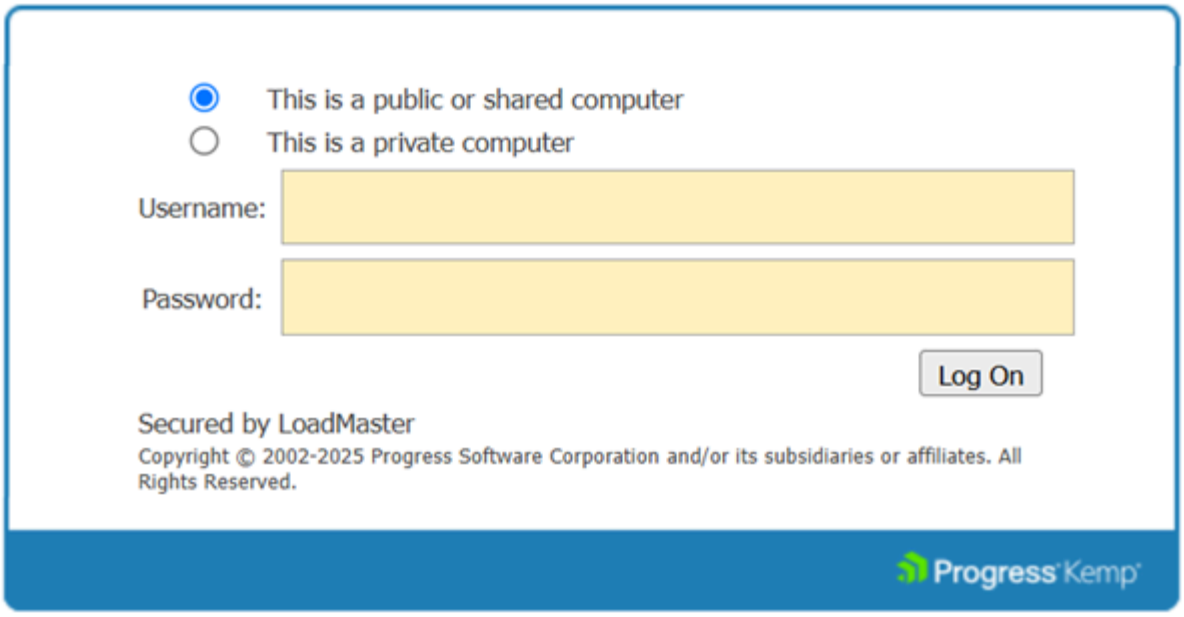
Do not enter the same group name in both the **Permitted Groups** and **Steering Groups** fields. This causes a conflict. When you specify a steering group, it is assumed to behave like a permitted group, so you do not need to enter the same group in both the **Permitted Groups** and **Steering Groups** fields.

SSO Image Set

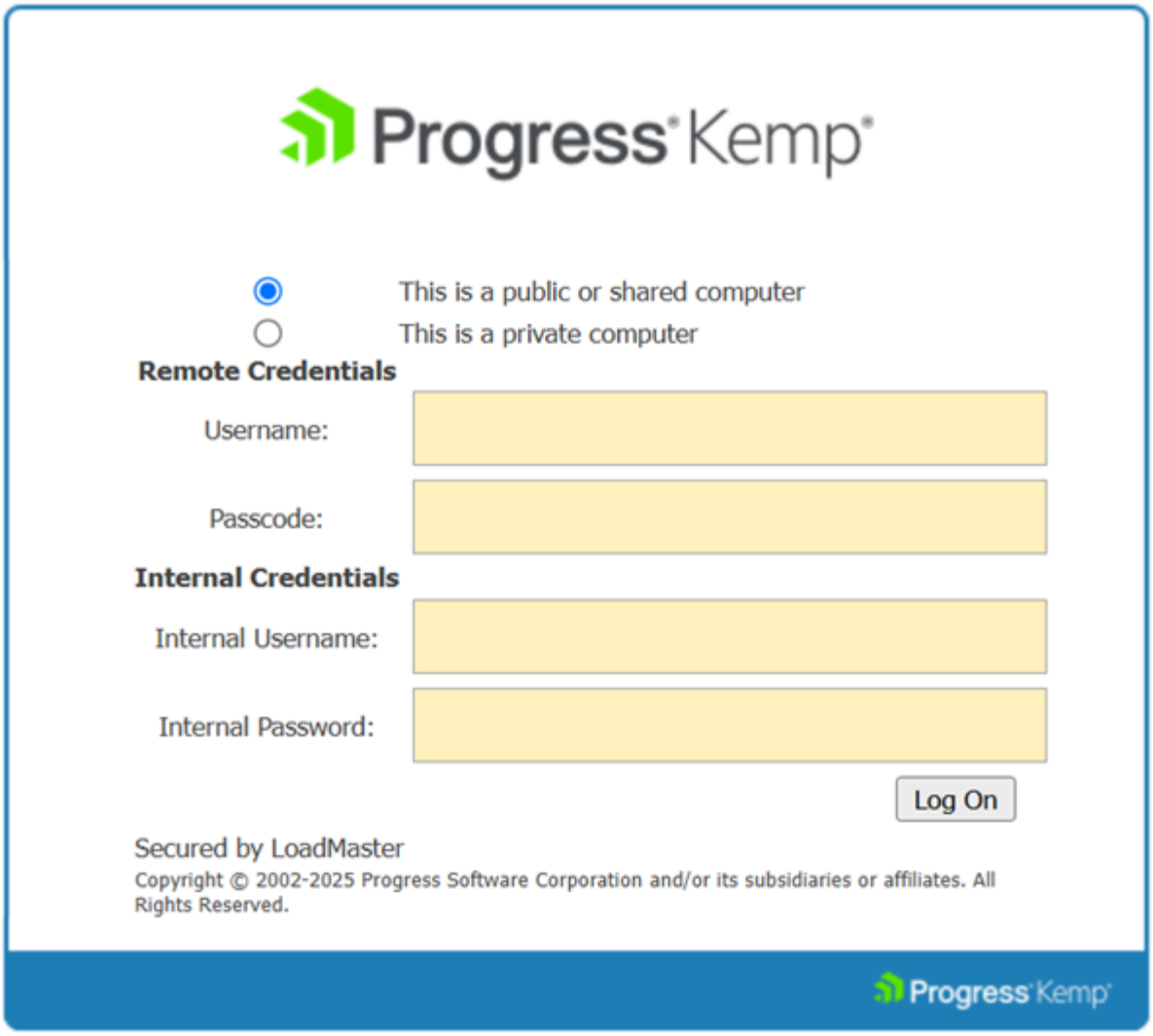
This option is only available if **Form Based** is selected as the **Client Authentication Mode**. There is an option for which form to use to gather the user's Username and Password. There are three default form options; **Exchange**, **Blank** and **Dual Factor Authentication**. English is the default language for the image sets. There are also options to display the form and error messages in other languages – Brazilian Portuguese and French Canadian.



The **Exchange Form** contains the Progress Kemp Logo.



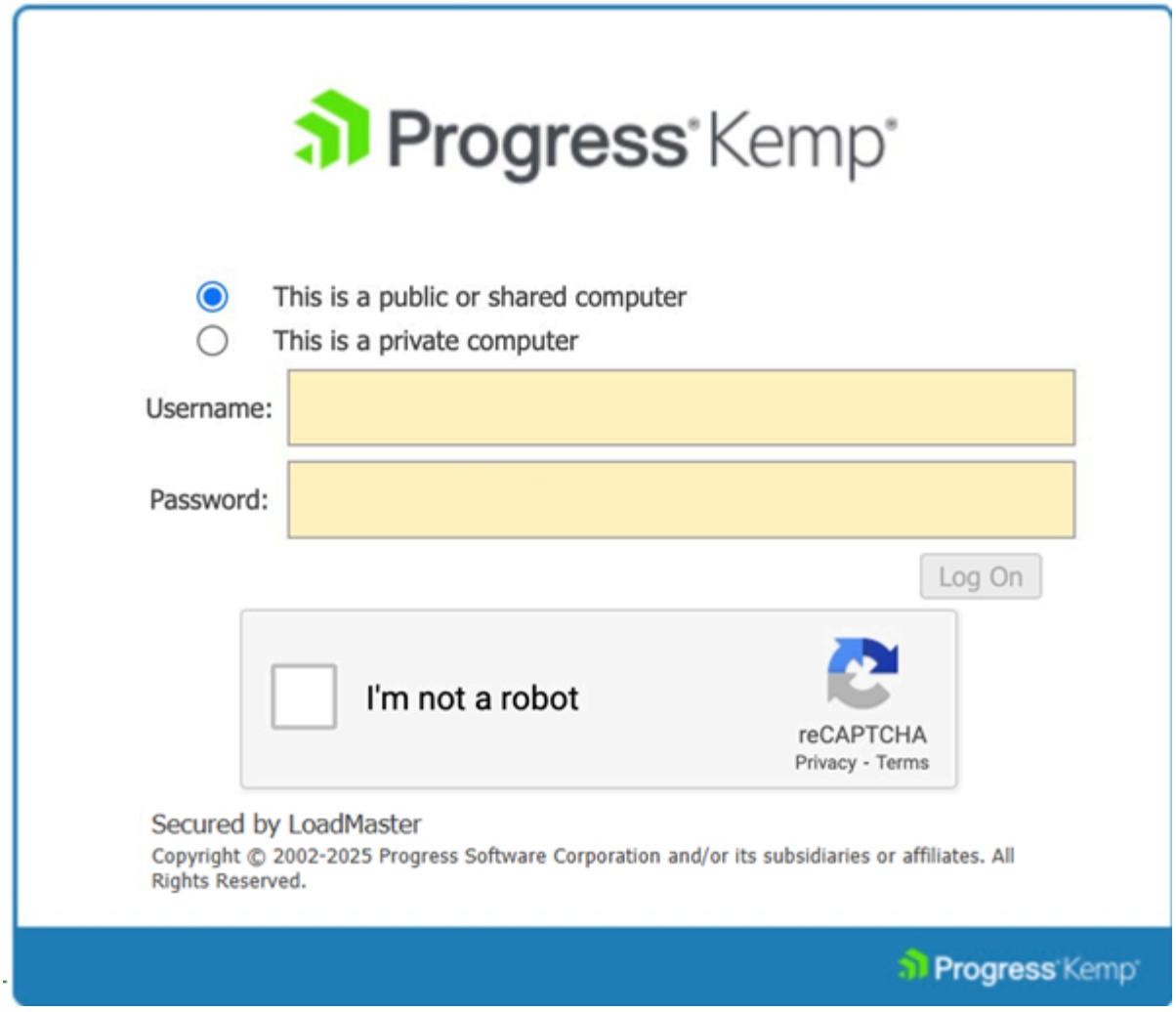
The **Blank Form** does not contain the Progress Kemp logo.



The **Dual Factor Authentication** form contains four fields - two for the remote credentials and two for the internal credentials.

Note: The **Dual Factor Authentication** image set should only be used with the **RADIUS and LDAP** authentication protocol.

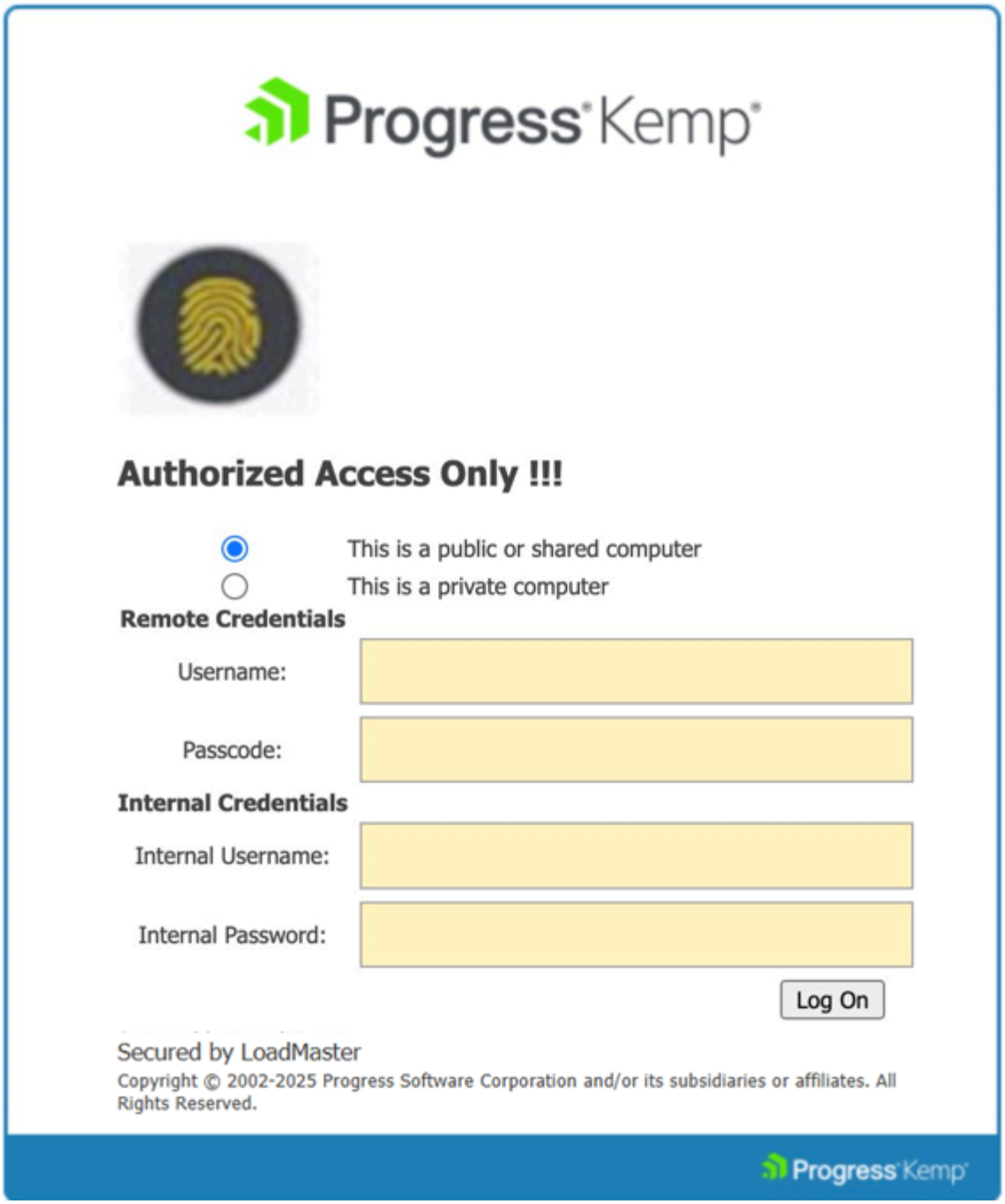
It is possible to upload a custom SSO image set. For more information, refer to the Custom Authentication Form, Technical Note



If CAPTCHA is enabled, the CAPTCHA box appears on the ESP login page.

SSO Greeting Message

The login forms can be further customized by adding text (for example the **Authorized Access Only!** text in the following screenshot). Enter the text to appear on the form within the **SSO Greeting Message** text box and click the **Set SSO Greeting Message** button.



Note: The **SSO Greeting Message** displays up to 255 characters. Any ASCII character is accepted and will be displayed in the message, with two exceptions: the grave accent character (` ) and the single quote ( **'** ).If a grave accent character is used in the SSO Greeting Message, the character will not display in the output, for example **a`b`c** becomes **abc**. If a single quote is used, users will not be able to log in.

Note: In addition to ASCII characters, HTML-encoded characters are also accepted and can be used to display non-ASCII characters in the login form; just type HTML-encoded characters into the **SSO Greeting Message** text box in the LoadMaster. For example, for the letter **Ä**, you must type the HTML-encoded code for this letter, for example, **Ä**. For further information, please see: List of XML and HTML character

entity references.

Logoff String

This option is only available if **Form Based** or **SAML** is selected as the **Client Authentication Mode.** Specify the string that the LoadMaster should use to detect a logout event. Normally this field should be left blank. For OWA Virtual Services, the **Logoff String** should be set to **/owa/logoff.owa**; or, in customized environments, a modified **Logoff String** needs to be specified in this text box. Multiple logoff strings can be specified by using a space-separated list. You can enter up to 255 characters in this field.

Note: If the URL to be matched contains sub-directories before the specified string, the logoff string will not be matched. Therefore, the LoadMaster will not log the user off.

Additional Authentication Header

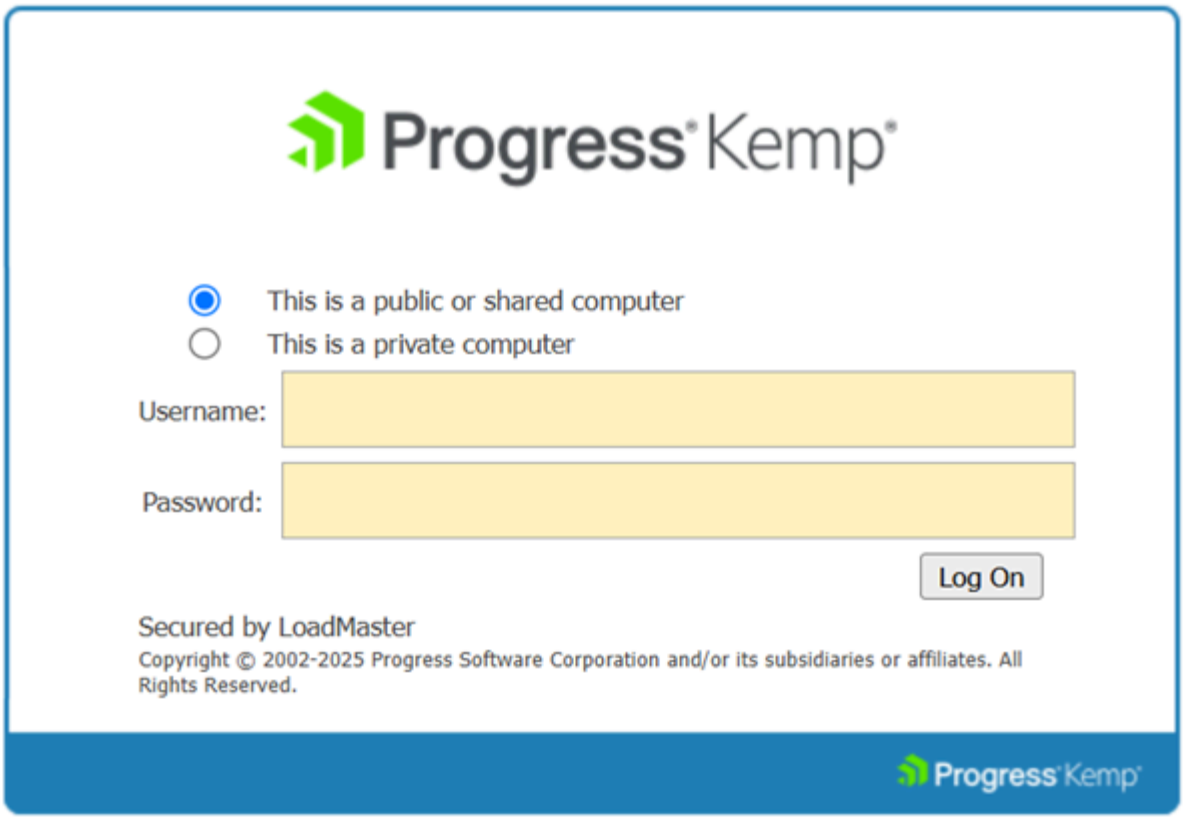
This option is only available if **SAML** or **OIDC/OAUTH** is selected as the **Client Authentication Mode**. Specify the name of the HTTP header. This header is added to the HTTP request from the LoadMaster to the Real Server and its value is set to the user ID for the authenticated session. You can enter up to 255 characters in this field.

When validating the token from the Identity Provider (IdP), the LoadMaster checks the claims (attributes) in the following sequence:

- preferred_username
- UPN
- unique_name
- email

For example, if the preferred_username is not available then the UPN is used. If the UPN is also not available, then unique_name or email is used for token validation.

Display Public/Private Option



Enabling this check box displays a public/private option on the login page. The session and idle timeout depend on what option the user selects when logging in. If the user selects **This is a private computer**, then their credentials are saved on the client computer. If the user is on a public or shared computer, they should use the default option, which does not save their credentials locally.

Disable Password Form

Enabling this option removes the password field from the login page. This may be needed when password validation is not required, for example if using RSA SecurID authentication in a singular fashion. By default, this option is disabled.

Enable Captcha

Select this check box to allow CAPTCHA verification on the login page.

Note: The LoadMaster only supports CAPTCHA v2.

Note: The Client Authentication Mode must be set to Form Based for the Enable Captcha check box to be visible.

CAUTION: All CAPTCHA parameters must be set before it can be used.

CAUTION: Both the LoadMaster and the client machine must be able to access Google for this to work.

Before the CAPTCHA has been correctly answered, the submit button on the login form is disabled.If the user does not submit the form within two minutes of answering the CAPTCHA, the CAPTCHA times out (Google-specified timeout), and the user must verify a new CAPTCHA (the submit button is disabled until the new CAPTCHA has been verified).

Use Session or Permanent Cookies

Three options are available to select for this field:

- **Session Cookies Only:** This is the default and most secure option
- **Permanent Cookies only on Private Computers:** Sends permanent cookies only on private computers
- **Permanent Cookies Always:** Sends permanent cookies in all situations

---

Note: Permanent cookies only work with Internet Explorer (IE) and IE must be set to accept **Third Party Cookies** and the site must be added to the **Trusted Sites**.

Note: The expiry time of a permanent cookie can be set by configuring the **Session Timeout** fields in the modify SSO screen. The maximum value is 7 days (**604800** seconds).

Specify if the LoadMaster should send session or permanent cookies to the client browser when logging in.

Note: Permanent cookies should only be used when using single sign on with services that have sessions spanning multiple applications, such as SharePoint.

Cookie SameSite Processing

This option allows the SameSite attribute to be explicitly specified for cookies used by the LoadMaster Edge Security Pack. This influences the way browsers will use cookies across sites.

The following are the available options to select for this field:

- **SameSite Option not Added**: This option availability is depend upon the global level configuration i.e. **Default ESP Cookie SameSite Processing** . If the option other than **SameSite Option Not Added** is configured for **Default ESP Cookie SameSite Processing** field (under **System Configuration > Miscellaneous Options > L7 Configuration** page) then only the **SameSite Option Not Added** option will appear in drop-down list for VS.
- **SameSite=None:** Signals that the cookie data can be shared with third parties/external sites (for advertising, embedded content, etc).
- **SameSite=LAX:** Signals that the cookie may be used as a first party cookie but may also be used when accessing the site from an external site via a link clicked by the user.
- **SameSite=Strict:** It is a subset of lax and only enables the cookie be used in first party context and excludes its use when accessing via an incoming link from an external site.
- **System Default**: By default this option is selected and VS will be using the Global level settings.

Note: When a new Virtual Service is created on the LoadMaster and ESP has **Form-based** enabled, then the **Cookie SameSite Processing** option is always configured to **System Default**. When this is the case,

---

the Virtual Service will use the default global settings configured on LoadMaster. When the user changes the configured System Default setting of the Virtual Service to some other option, then the configuration of the selected Virtual Service option overrides the Global SameSite configuration.

User Password Change URL

This is relevant when using client-side forms-based authentication and LDAP. Specify the URL that users can use to change their password, for example https://mail.kempqakcd.net/owa/auth/expiredpassword.aspx?url=/owa/auth.owa

If a user's password has expired, or if they must reset their password, this URL and the **User Password Change Dialog Message** is displayed on the login form.

This URL must be entered in the ESP **Pre-Authorization Excluded Directories** field - this is required to bypass pre-authentication.

If using this expired password functionality in an Exchange 2010 environment:

- The **Pre-Authorization Excluded Directories** must be set to **/owa/auth.owa /owa/auth* /owa/14.3.123.3****. 14.3.123.3 is the sub-path of the Exchange server that must be added to the excluded directories.
- When changing passwords, users cannot use a User Principal Name (UPN) (for example, joebloggs@example.com) in the **Domain\user name** field in the Change Password window, unless Exchange 2010 SP1 RU3 or later is deployed on the Client Access servers.

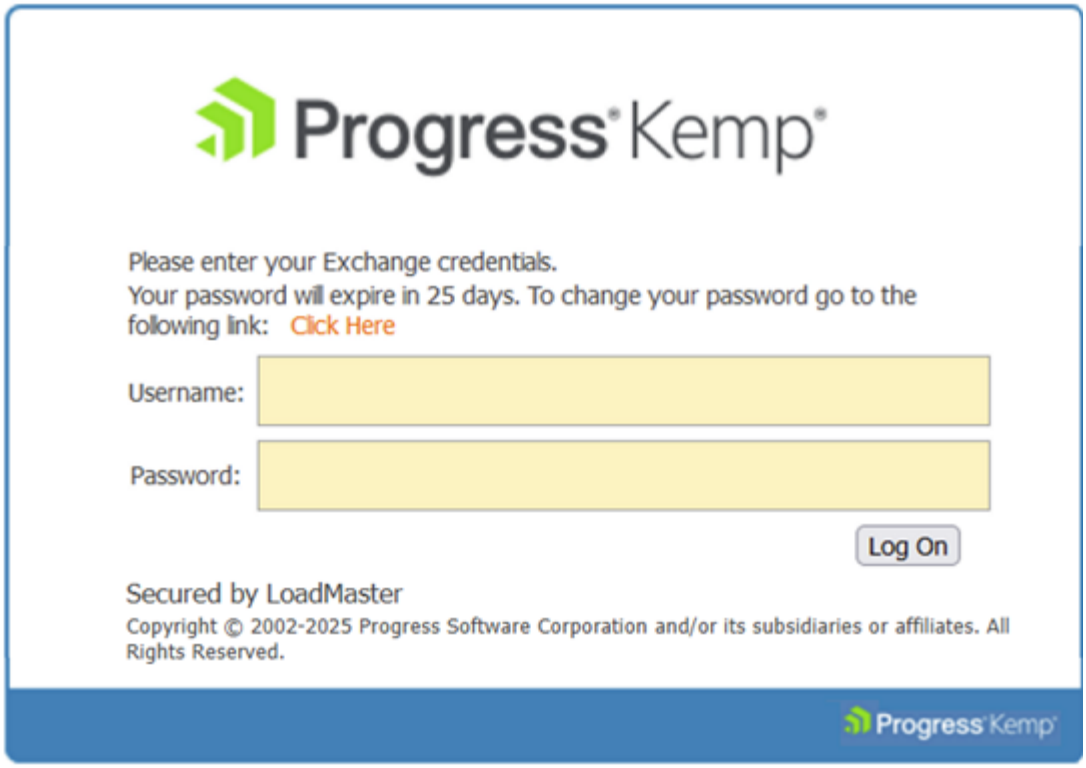
For further information, refer to the following Microsoft TechNet article: https://technet.microsoft.com/en-us/library/bb684904(v=exchg.141).aspx

User Password Change Dialog Message

This text box is only visible if something is set for the **User Password Change URL** text box. Specify the text to be displayed on the login form when the user must reset their password. Special characters are not permitted in this field.

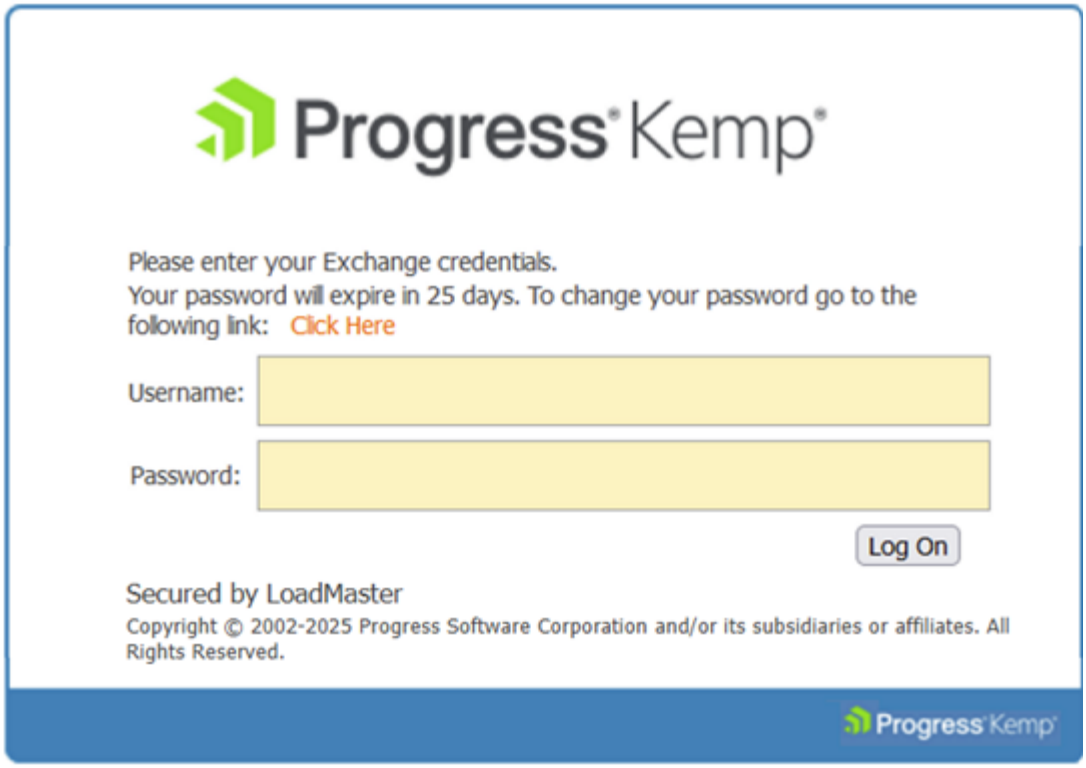
Note: If the **User Password Change URL** field is set, you must also set the **User Password Change Dialog Message** because both settings are required when a user attempts to change their password. If ESP is enabled on the SubVS level, you must set the password expiry/change configuration on the first SubVS in the SubVS list (for example, if the Exchange template is used this is the **Authentication Proxy** SubVS).

User Password Expiry Warning



By default, SSO users are notified about the number of days before they must change their password. If you disable this option, the password expiry notification will not appear on the login forms.

You can specify the number of days to show the warning before the password is expired. The default value for this field is **15 days**. The range is **1** to **30 days**. This field is only visible if the **Client Authentication Mode** is set to **Form Based** and the **User Password Change URL** is set.

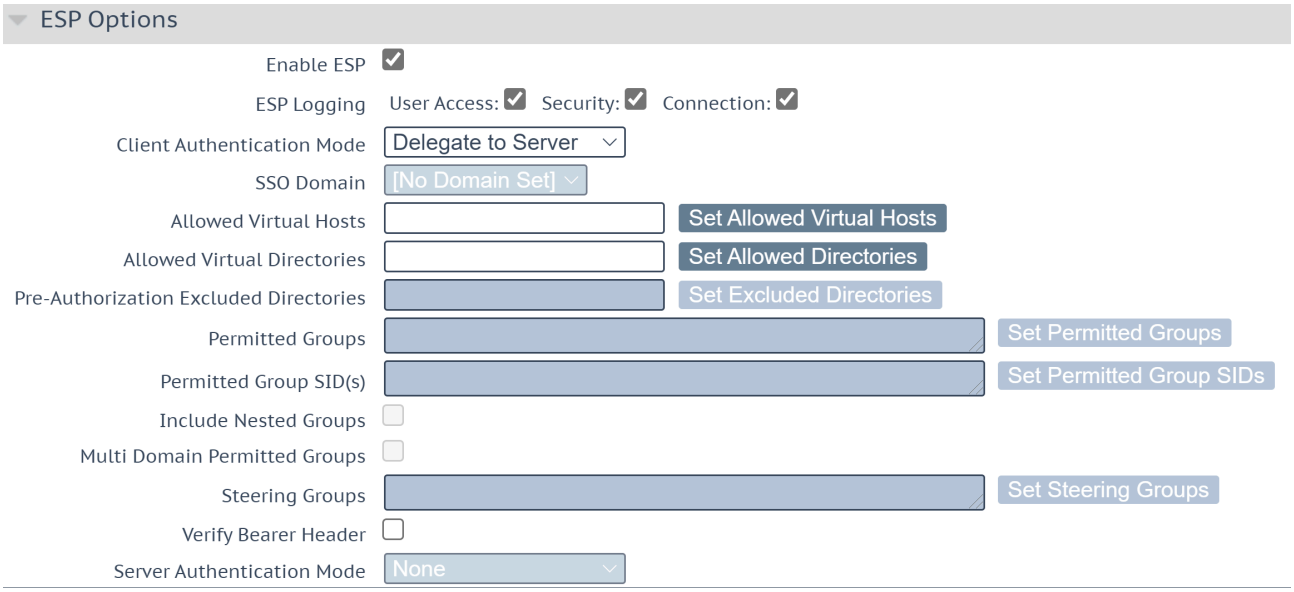


The user is notified when the password has expired. The language of the warning text is based on the **SSO Image Set** that is selected (English, French, or Portuguese).

Verify Bearer Header

Enable this check box to verify the authenticity of a JSON Web Token (JWT) included in the Authorizations header of incoming client requests. If the Authorization header field is present in the client request, it is passed back to the Real Server.

There is an additional capability that verifies if the token is valid. This is done by comparing the text provided in the **Bearer Header Validation Text** field to the contents of the "aud" field of the token included in the Auth header. If this text is present and the match fails - there is no connection made. Another capability is to also check the signature on the token. To do this, you must upload and select a certificate in the **Bearer Header Validation Certificate** drop-down list. If a certificate is selected and the validation fails - there is no connection made.



Note: The **Verify Bearer** Header field (and the two fields detailed below) are only available if the **Client Authentication Mode** is set to **Delegate to Server**.

Bearer Header Validation Certificate

This option is only visible if the **Verify Bearer Header** check box is selected.

Specify the name of the relevant certificate from the **Bearer Header Validation Certificate** drop-down list (this must be first uploaded to the LoadMaster by going to **Certificates & Security > SSL Certificates > Import Certificate**) containing a Public Key used to validate the authenticity of the bearer header token signature. If you are not performing signature validation, the certificate can be set to **None**.

Bearer Header Validation Text

This option is only visible if the **Verify Bearer Header** check box is selected.

You can optionally enter up to 5 comma-separated strings to match against the Audience Claim Field (aud) in the token. If provided, at least one string must match the Audience Claim Field's content or the token is rejected.

Server Authentication Mode

Specifies how the LoadMaster is authenticated by the Real Servers. There are three types of methods available:

- **None:** no client authentication is required
- **Basic Authentication**: standard Basic Authentication is used
- **KCD:** Kerberos Constrained Delegation (KCD) is used. For further information, refer to the Kerberos Constrained Delegation, Feature Description.
- **Server Token:** On reception and verification of the SAML response, the LoadMaster requests a long-lived token. The LoadMaster then builds a redirection URL with the token specified.

Note: You can only select **Server Token** as the **Server Authentication Mode** if **SAML** is selected as the **Client Authentication Mode**.

- **Form Based:** When **Form Based** authentication is selected, the **Form Authentication Path** field appears.

Note: You can only select **Form Based** as the **Server Authentication Mode** if **Foam Based** is selected as the **Client Authentication Mode**.

- When you enter a value in the **Form Authentication Path** field and click the **Set Path** button, the **Form POST Format** and **Post Format Username Only** fields appear. The username and password from the client-side, form-based authentication is injected into the form POST format to build the POST body.
- This is predominantly used in Microsoft Exchange deployments and has only been tested with Exchange 2013 and 2016. Therefore, the following strings do not need to be explicitly configured for Exchange 2013/2016. They are used by default in the implementation:
- **Form Authentication Path:** /owa/auth.owa
- **Form POST Format:**

```
destination=%s#authRedirect=true&amp;flags=4&amp;forcedownlevel=0&amp;username=%s&amp;passw
```

Note: The **Form POST Format** field only becomes visible when the **Form Authentication Path** is set.

Note: If the deployment is not Exchange, we recommend that the settings are evaluated based on the required interaction with the Real Server and subsequently set appropriately.

POST Format Username Only

Enable this option to send the username only (without the domain part) in the server-side form based authentication POST request.

When choosing a specific **Client Authentication Mode** protocol, it is important to understand what **Server Authentication Mode** protocols are compatible:

Client Authentication Mode	Compatible Server Authentication Mode
Delegate to Server	None
Basic Authentication	Basic Authentication

Client Authentication Mode	Compatible Server Authentication Mode
Form Based	Basic Authentication
	KCD
	Form Based
	None
NTLM	KCD
	None
NTLM-Proxy	NTLM-Proxy
NTLM-Proxy	KCD
Client Certificate	KCD
Client Certificate	None In LoadMaster firmware version 7.2.53, support was added for **Client Certificate** client authentication with no server side authentication. For further details, refer to the following section: Client Certificate Authentication with No Server Side Authentication.
SAML	KCD
SAML	None
SAML	Server Token

Server Side configuration

Note: This option is only visible when the **Server Authentication mode** value is set to **KCD**. For further information, please refer to the Kerberos Constrained Delegation, Feature Description.

Select the SSO domain for the server side configuration. Only SSO domains which have the **Configuration type** set to **Outbound Configuration** are shown here.

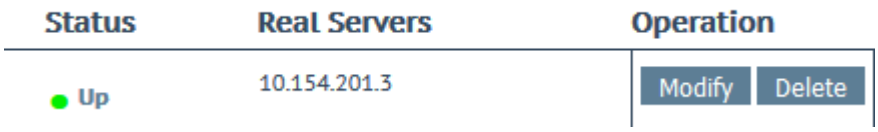
Token Server FQDN

Note: This option is only visible when the **Server Authentication mode** value is set to **Server Token**.

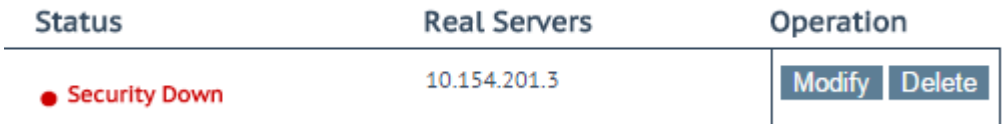
Set the FQDN for the token server. When set, LoadMaster contacts the token server at the given FQDN during sign-on and obtains a permanent access token from that token server. If this parameter is unset, then LoadMaster obtains the token from the Real Server (as in previous releases).

Virtual Service Status

When **View/Modify Services** is clicked in the main menu, the Virtual Service status is displayed.



When the health check status is OK, the **Status** on the Virtual Services screen is set to **Up**.



When ESP is enabled, a new status is available; **Security Down**.

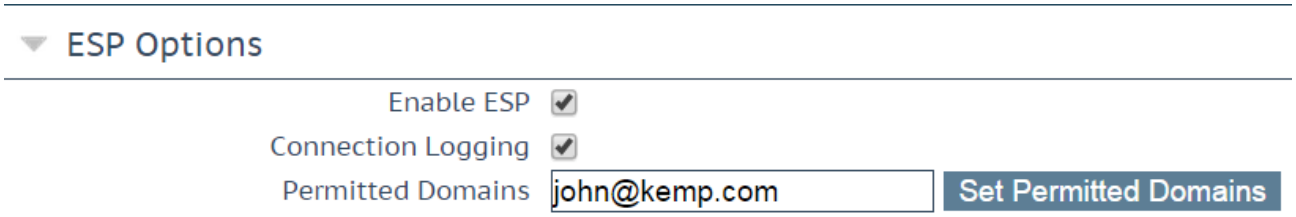
The LoadMaster will check the health status of the authentication server every 20 seconds. If the authentication server cannot be reached, then the Virtual Service goes into a **Security Down** state where no new users are allowed to access the Virtual Service. Existing connections will not be affected until their individual connection timeouts expire.

Contents

- SMTP Virtual Services and ESP
- Limitations of Using Regular Expressions in the LoadMaster WUI

SMTP Virtual Services and ESP

If an SMTP Virtual Service (with **25** as the port) is created, the ESP feature is enabled for the Virtual Service when the **Enable ESP** checkbox is selected, but with a reduced set of options.



Enable ESP

Enable or disable the ESP feature set by selecting or deselecting the **Enable ESP** check box.

Connection Logging

Logging of connections can be enabled or disabled by selecting or deselecting the **Connection Logging** check box. The ESP logs can be viewed and downloaded by going to **System Configuration > Logging Options > Extended Log Files**.

Permitted Domains

All the permitted domains that are allowed to be received by this Virtual Service must be specified here. For example, if the Virtual Service should receive SMTP traffic from john@progress.com, then the progress.com domain must be specified in this field. When entering more than one domain, separate them with a space.

The use of Shell regular expressions is allowed within this text box.

Note: If this text box is blank, no domains are allowed and all mail is stopped.

Limitations of Using Regular Expressions in the LoadMaster WUI

When using regular expressions in the LoadMaster WUI, you must use an even number of quotes (single or double). The quotes must also nest correctly, for example, if you use single quotes within double quotes, the single quotes must be matched inside the double-quotes. To use a single " (double-quote) character in a regex, use **\22** instead (or **\27** for a single quote).

If you want to use an uneven number of quotes in a regular expression, use the API instead of the WUI.

For example, trying to set the following **Match String** in the WUI results in an error that says **Please specify a pattern to be matched**:

/\<img([^\>\/]*)\ssrc\=\"([^\"]*)\"([^\>\/]*)\/?>/

However, it is possible to set this using the API, for example:

```
/access/
addrule?name=Example&pattern=/\<img([^\>\/]*)\ssrc\=\"([^\"]*)\"([^\>\/]*)\/?>/
```

LDAP Configuration

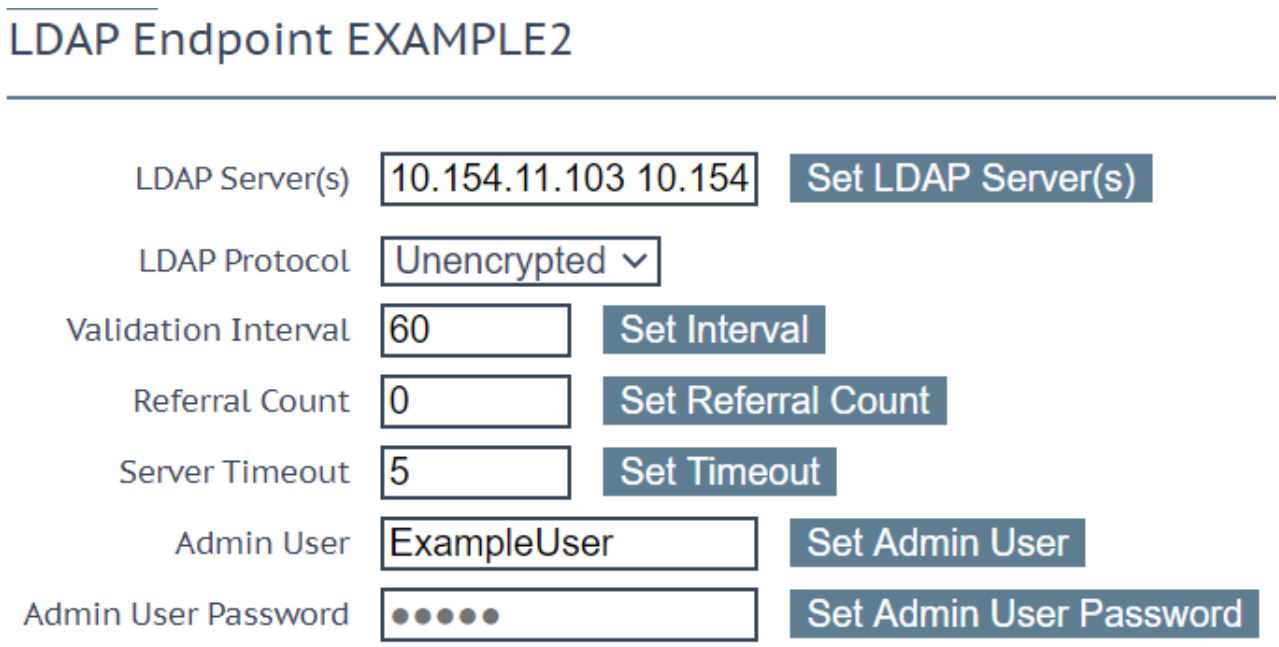
To get to the **LDAP Configuration** screen, expand **Certificates & Security** and click **LDAP Configuration**. This screen provides a management interface for LDAP endpoints. These LDAP endpoints may be used in three different areas:

- Health checks
- SSO domains
- WUI authentication



Any existing **LDAP Endpoints** are listed here, with an option to **Modify** and **Delete**. If an LDAP endpoint is in use it cannot be deleted.

There is also an option to add a new LDAP endpoint. Enter a name for the endpoint and click **Add**. Spaces and special characters are not permitted in the LDAP endpoint name.



LDAP Server(s)

Specify a space-separated list of LDAP servers to be used. For windows Admin Controller (AC)/Domain Controller (DC), the scope of access for multiple domains and Permitted Groups is set to universal. Port numbers can also be specified if required. If you have multiple domains and are using **Permitted Groups**, sometimes it is necessary to include the Global Catalog port number, otherwise the **Permitted Groups** will fail. The default port is **3268**. For example, **10.110.20.23:3268**.

LDAP Protocol

Select the transport protocol to use when communicating with the LDAP server.

Note: If you create an SSO domain with the **Authentication Protocol** set to **Certificates**, ensure to set the **LDAP Protocol** to **LDAPS** in the LDAP endpoint.

Validation Interval

Specify how often the user should be revalidated with the LDAP server. Valid values range from 10 to 86400 seconds.

Referral Count

The LoadMaster offers beta functionality to support LDAP referral replies from Active Directory Domain Controllers. If this is set to **0**, referral support is not enabled. Set this field to a value between **1** and **10** to enable referral chasing. The number specified will limit the number of hops (referrals chased).

Note: Multiple hops may increase authentication latency. There is a performance impact that depends on the number and depth of referrals required in your configuration.

Note: You must have intimate knowledge of your Active Directory structure to set the referral limit appropriately. The same credentials are used for all lookups, and so on.

Note: The use of Active Directory Global Catalog (GC) is the preferred configuration as the primary means of resolution instead of enabling LDAP referral chasing. A GC query can be used to query the GC cache instead of relying on LDAP and the referral process. Using Active Directory GC has little or no performance drag on the LoadMaster. For steps on how to add/remove the GC, refer to the following TechNet article: https://technet.microsoft.com/en-us/library/cc755257(v=ws.11).aspx

Server Timeout

Specify the LDAP server timeout in seconds. The default value is **5**. Valid values range from **5** to **60**.

Admin User

Enter the username of an administrator user in the format **admin@domain.com** or **domain\user**.

Note: This account must be in the Domain Admins group.

Admin User Password

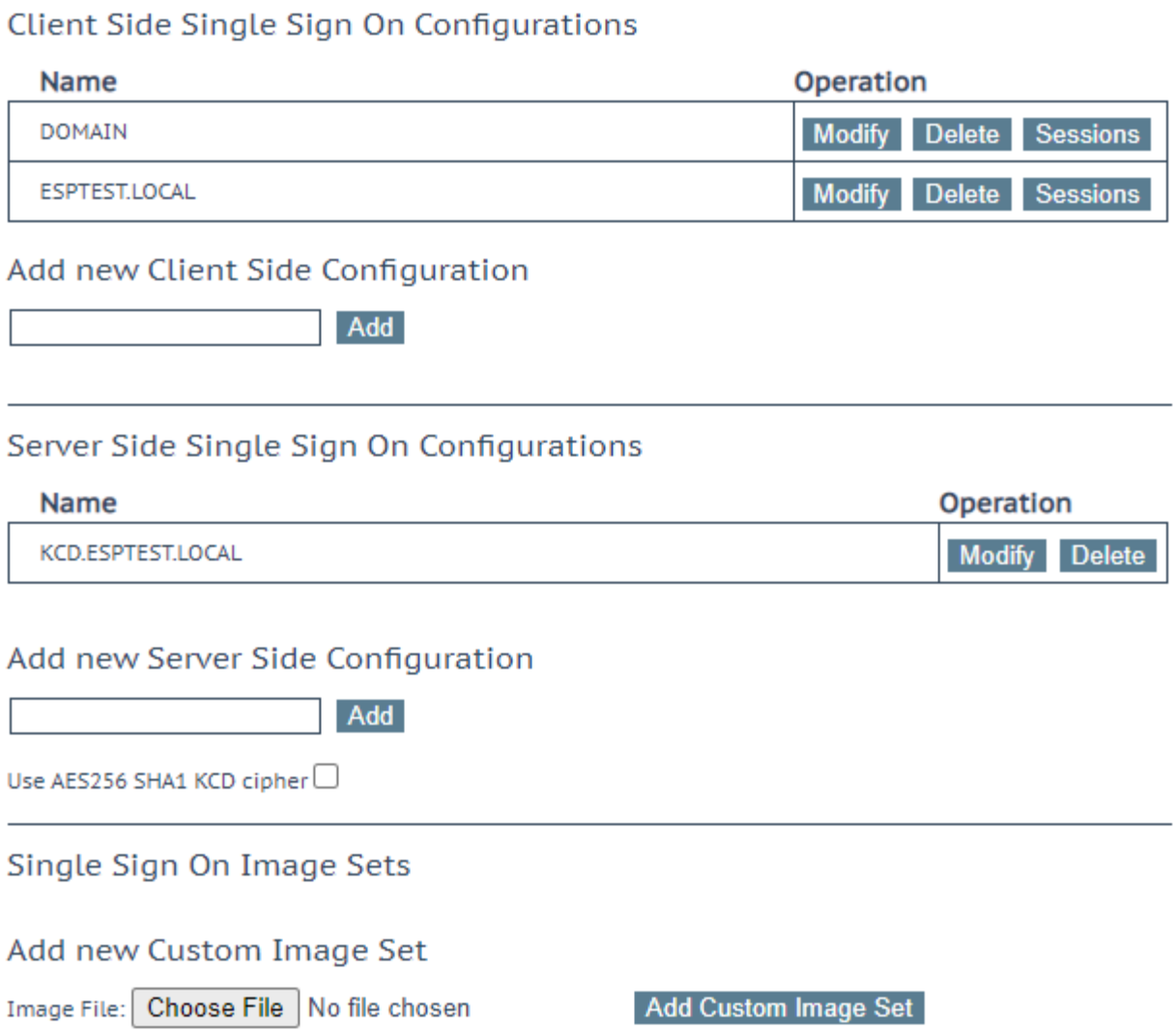
Enter the password for the specified administrator user.

Manage SSO Options

Before using the Edge Security Pack (ESP) the user must first set up a Single Sign-On (SSO) Domain on the LoadMaster. The SSO Domain is a logical grouping of Virtual Services which are authenticated by an LDAP server.

To get to the **Manage SSO** screen – in the main menu of the LoadMaster WUI, go to **Virtual Services > Manage SSO**.

Note: The maximum number of SSO domains that are allowed is 128.



Click the **Manage SSO Domains** menu option to open the **Manage Single Sign On Options** screen.

Contents

- Single Sign On Domains

Single Sign On Domains

Two types of SSO domains can be created – Client Side and Server Side. Client Side single sign on domains enable the configuration of how the LoadMaster authenticates clients including protocols used and authentication endpoints. A Server Side domain is required if utilizing Kerberos Constrained Delegation for the authentication of connections from the LoadMaster to the servers.

Client Side configurations allow you to set the **Authentication Protocol** to **LDAP**, **RADIUS**, **RSA-SecurID**, **Certificates**, **RADIUS and LDAP** or **RSA-SecurID and LDAP**.

Server Side configurations allow you to set the **Authentication Protocol** exclusively to **Kerberos Constrained Delegation** (KCD).

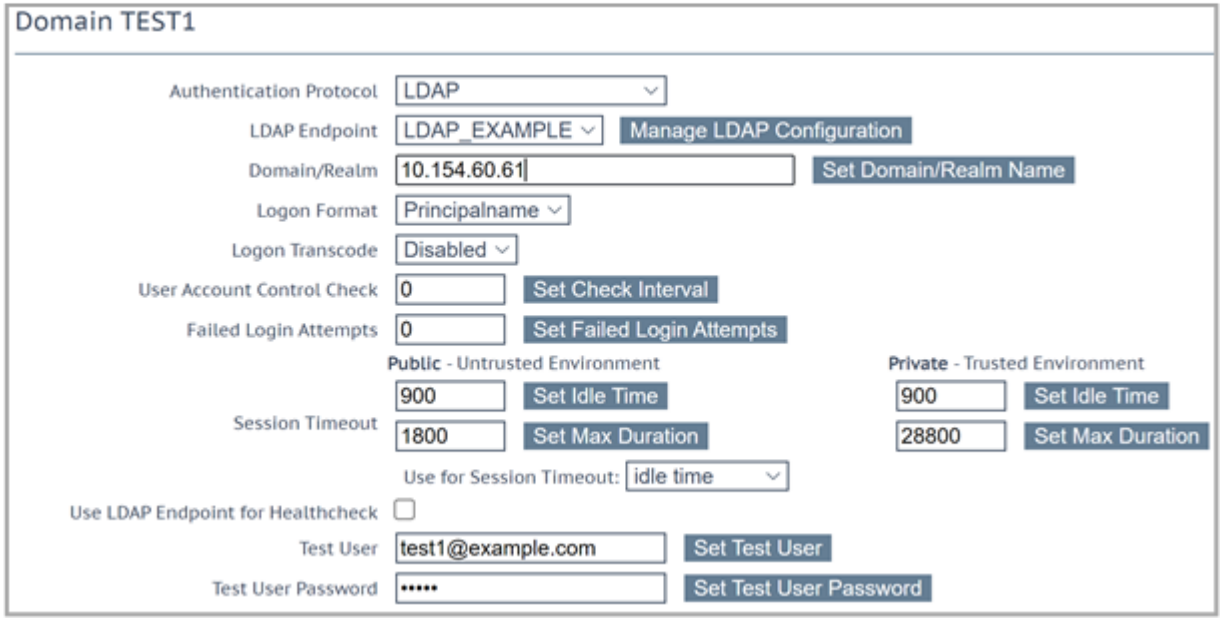
To add a new SSO Domain enter the name of the domain in the **Name** field and click the **Add** button. The name entered here does not need to relate to the allowed hosts within the Single Sign On Domain.

Note: If the **Domain/Realm** field is not set, the domain **Name** set when initially adding an SSO domain is used as the **Domain/Realm** name.

Contents

- Client Side (Inbound) SSO Domains
- Client Side (Inbound) SAML SSO Domains
- Client Side (Inbound) OIDC / OAUTH SSO Domains
- RADIUS Two-factor and LDAP Authentication
- Sessions
- Server Side (Outbound) SSO Domains

Client Side (Inbound) SSO Domains



Authentication Protocol

This dropdown allows you to select the transport protocol used to communicate with the authentication server. The options are:

- LDAP
- RADIUS
- RSA-SecurID
- Certificates

Note: If you create an SSO domain with the **Authentication Protocol** set to **Certificates**, ensure to set the

LDAP Protocol to **LDAPS** in the LDAP endpoint.

- RADIUS and LDAP
- RSA-SecurID and LDAP
- SAML
- OIDC / OAUTH

Note: The fields displayed on this screen will change depending on the **Authentication protocol** selected.

LDAP Endpoint

Select the LDAP endpoint to use. For further information on LDAP endpoints, refer to the LDAP Configuration section.

Note: This option is only available if the **Authentication Protocol** is set to **LDAP**, **RADIUS and LDAP** or **RSA-SecurID and LDAP**.

RADIUS/RSA-SecurID Server(s)

Type the IP address(es) of the server(s) which are used to authenticate the domain.

Multiple server addresses can be entered within this text box. Each entry must be separated by a space.

Radius Shared Secret

The shared secret to be used between the RADIUS server and the LoadMaster (48 character limit).

Note: This field is only available if the **Authentication Protocol** is set to **RADIUS** or **RADIUS and LDAP**.

Send NAS Identifier

If this check box is disabled (default), a NAS identifier is not sent to the RADIUS server. If it is enabled, a Network Access Server (NAS) identifier string is sent to the RADIUS server. By default, this is the hostname. Alternatively, if a value is specified in the **RADIUS NAS Identifier** text box, this value is used as the NAS identifier. If the NAS identifier cannot be added, the RADIUS access request is still processed.

Note: This field is only available if the **Authentication Protocol** is set to **RADIUS** or **RADIUS and LDAP**.

Sending the NAS identifier serves two purposes:

- It helps to classify the device type that is sending the request as opposed to simply sending the host IP address which makes troubleshooting and consuming logs easier.
- It enables customized authentication responses to be sent back from the server based on the identifier.

RADIUS NAS Identifier

If the **Send NAS Identifier** check box is selected, the **RADIUS NAS Identifier** field is shown. When specified, this value is used as the NAS identifier. Otherwise, the hostname is used as the NAS identifier. If

the NAS identifier cannot be added, the RADIUS access request is still processed.

Note: This field is only available if the **Authentication Protocol** is set to **RADIUS** or **RADIUS and LDAP** and the **Send NAS Identifier** check box is enabled.

Select Certificate to User Mapping

This option is only available when the **Authentication Protocol** is set to **Certificates**. The **Select Certificate to User Mapping** field has the following values:

- User Principal Name (default value)
- Subject
- Issuer and Subject
- Issuer and Serial Number

Note: In LoadMaster firmware version 7.2.53, support for Personal Identity Verification (PIV) smart cards was added. For further details, refer to the following section: PIV Smart Card Support.

If this option is enabled and the check fails, the login attempt will fail. If this option is not enabled, only a valid client certificate (with the username in the SubjectAltName (SAN)) is required to log in, even if the altSecurityIdentities attribute for the user is not present or not matching.

For more information, refer to the Kerberos Constrained Delegation, Feature Description.

Allow fallback to check Common Name

Enabling this option allows a fallback to check the Common Name (CN) in the certificate when the SAN is not available.

Note: This field only appears when the **Authentication Protocol** is set to **Certificates**.

Domain/Realm

The login domain to be used. This is also used with the logon format to construct the normalized username, for example;

- **Principalname:** <username>@<domain>
- **Username:** <domain>\<username>

Note: If the **Domain/Realm** field is not set, the **Domain** name set when initially adding an SSO domain is used as the **Domain/Realm** name.

RSA Authentication Manager Config File

Note: This option is only available when the **Authentication Protocol** is set to **RSA-SecurID**.

This file needs to be exported from the RSA Authentication Manager.

Note: For more information on the RSA authentication method, including how to configure it, refer to the RSA Two Factor Authentication, Feature Description.

RSA Node Secret File

Note: This option is only available when the **Authentication Protocol** is set to **RSA-SecurID**.

A node secret must be generated and exported in the RSA Authentication Manager.

Note: It is not possible to upload the RSA node secret file until the RSA Authentication Manager configuration file is uploaded. The node secret file is dependent on the configuration file.

Logon Format

This drop-down list allows you to specify the format of the login information that the client has to enter.

Note: The options available vary depending upon which **Authentication Protocol** is selected.

Not Specified: The username will have no normalization applied to it - it is taken as it is typed.

Principalname: Selecting this as the **Logon format** means that the client does not need to enter the domain when logging in, for example **username@domain**. The SSO domain added in the corresponding text box is used as the domain in this case.

Note: When using **RADIUS** as the **Authentication protocol** the value in this SSO domain field must exactly match for the login to work. It is case sensitive.

Username: Selecting this as the **Logon format** means that the client needs to enter the domain and username, for example **domain\username**.

Username Only: Selecting this as the **Logon Format** means that the text entered is normalized to the username only (the domain is removed).

Note: The **Username Only** option is only available for the **RADIUS** and **RSA-SecurID** protocols.

Logon Format (Phase 2 Real Server)

Specify the logon string format used to authenticate to the Real Server.

The **Logon Format (Phase 2 Real Server)** field only appears if the **Authentication Protocol** is set to one of the following options:

- RADIUS
- RSA-SecurID

Logon Format (Phase 2 LDAP)

Specify the logon string format used to authenticate to LDAP.

The **Logon Format (Phase 2 LDAP)** field only appears if the **Authentication Protocol** is set to one of the following options:

- RADIUS and LDAP
- RSA-SecurID and LDAP

For further details, refer to the following section: Appendix A - Expected Normalization Results (for LDAP Only) from Example Configurations

Logon Transcode

Enable or disable the transcode of logon credentials, from ISO-8859-1 to UTF-8, when required.

If this option is disabled, log in using the format that the client dictates. If this option is enabled, check if the client uses UTF-8. If the client does not use UTF-8, use ISO-8859-1.

User Account Control Check

If the UAC check interval value is set to 0 minutes (default value), then UAC is not performed periodically for users after successful login.

When you specify an interval value in the range of 1 to 300 minutes, the periodic UAC check is performed per user for the requests received after the interval expiry.

The UAC detects:

- Unknown users
- Disabled accounts
- Locked accounts
- Expired passwords on accounts

Extended ESP user logs provide the results of the UAC check. Additional information is logged for the user such as start session time, total duration, protocol information, KCD information, and blocked user events.

The check may occur on new connection establishment or as part of existing sessions. The **msDS-User-Account-Control-Computed** and **userAccountControl** attributes are used to determine the UAC status.

Failed Login Attempts

The maximum number of consecutive failed login attempts before the user is locked out. Valid values range from **0** to **99**. Setting this to **0** means that users will never be locked out.

Note: When a user is locked out, all existing logins for that user are terminated, along with future logins.

Reset Failed Login Attempt Counter after

When this time (in seconds) has elapsed after a failed authentication attempt (without any new attempts) the failed login attempts counter is reset to **0**. Valid values for this text box range from **60** to **86400**. This value must be less than the **Unblock timeout** value.

Unblock timeout

The time (in seconds) before a blocked account is automatically unblocked, that is, unblocked without administrator intervention. Valid values for this text box range from **60** to **86400**. This value must be greater than the **Reset Failed Login Attempt Counter after** value.

Session timeout

The **idle time** and **max duration** values can be set here for trusted (private) and untrusted (public) environments. The value that is used is dependent on whether the user selects public or private on their login form. Also, either **max duration** or **idle time** can be specified as the value to use.

Idle time: The maximum idle time of the session in seconds, that is, idle timeout.

Max duration: The max duration of the session in seconds, that is, session timeout.

Note: Valid values for these fields range from **60** to **604800** (seconds).

Use for Session Timeout: A switch to select the session timeout behaviour (**max duration** or **idle time**).

Note: The underlying network traffic may render the session active, even if there is no obvious user interaction.

Use LDAP Endpoint for Healthcheck

Select this check box to use the LDAP endpoint administrator username and password for health checking. If this is enabled, the **Test User** and **Test User Password** textboxes will not be available.

For more information on LDAP endpoints, refer to the LDAP Configuration section.

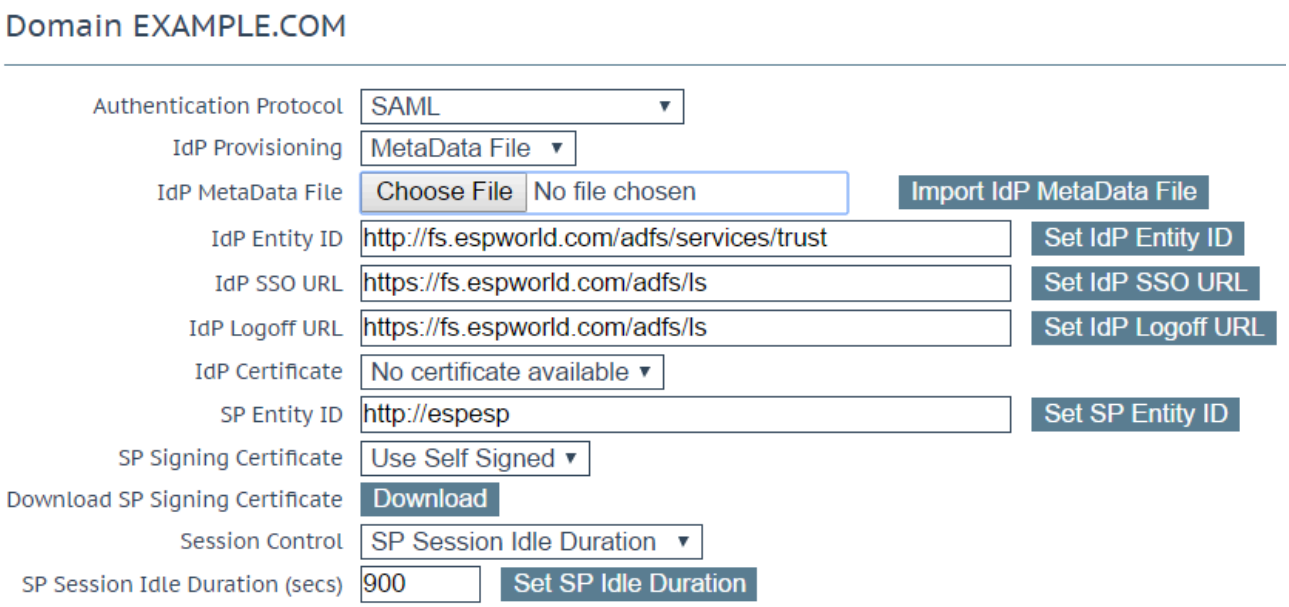
Note: This option is only available for the following protocols; **LDAP**, **Certificates**, **RADIUS and LDAP** and **RSA-SecurID and LDAP**.

Test User and **Test User Password**

In these two fields, enter credentials of a user account for your SSO Domain. The LoadMaster will use this information in a health check of the Authentication Server. This health check is performed every 20 seconds.

Client Side (Inbound) SAML SSO Domains

The fields vary when the Authentication Protocol is set to SAML. The SAML-specific fields are described below.



Idp Provisioning

The **Manual** option allows you to manually input details into the IdP fields.

The **MetaData File** option allows you to upload an **IdP MetaData File**. This simplifies the configuration of the IdP attributes, including the **IdP Entity ID**, **IdP SSO URL** and **IdP Logoff URL**. The metadata file can be downloaded from the IdP.

IdP Metadata File

This field is only visible if the **IdP Provisioning** field is set to **MetaData File**. To upload the file - click **Browse**, navigate to and select the relevant file and click **Import IdP MetaData File**.

IdP Entity ID

Specify the IdP entity identifier. The maximum number of characters permitted in this field is 255.

IdP SSO URL

Specify the IdP SSO URL. The maximum number of characters permitted in this field is 255.

IdP Logoff URL

Specify the IdP logoff URL. The maximum number of characters permitted in this field is 255.

IdP Certificate

The **IdP Certificate** is very important in terms of verification of the assertions that must be contained in the SAML response that is received from the IdP. Without the certificate, verification cannot proceed.

SP Entity ID

This is an identifier that is shared to enable the IdP to understand, accept and have knowledge of the entity when request messages are sent from the LoadMaster. This must correlate to the identifier of the relying party on the AD FS server. The maximum number of characters permitted in this field is 255.

SP Signing Certificate

It is optional to sign requests that are sent in the context of logon. Currently, the LoadMaster does not sign those requests.

In the context of log off requests – it is mandatory and these requests must be signed. This is to avoid any spoofing and to provide extra security in relation to log off functionality. This ensures that users are not being hacked and not being logged off unnecessarily.

In the **SP Signing Certificate** drop-down list, you can choose to use a self-signed certificate or third party certificate to perform the signing.

Download SP Signing Certificate

If using a self-signed certificate, click **Download** to download the certificate. This certificate must be installed on the IdP server (for example AD FS) to be added to the relying party signature.

The AD FS server requires this certificate for use of the public key to verify the signatures that the LoadMaster generates.

Session Control

The **IdP Session Max Duration** option does not appear to be usable when the IdP is AD FS. SAML and the LoadMaster supports it if present in the Authentication Response.

SP Session Idle Duration

Specify the session idle duration (in seconds).

Client Side (Inbound) OIDC / OAUTH SSO Domains

The fields vary when the **Authentication Protocol** is set to **OIDC / OAUTH**. The OIDC-specific fields are described below.

Application ID

Enter the Application (client) Identifier. The maximum number of characters permitted in this field is 255.

Redirect URI

Specify the redirect Uniform Resource Identifier (URI) or URIs (reply URLs). You can enter multiple URIs separated by a space. A maximum of 255 characters can be specified in the **Redirect URI** text box. Once a value is set for this field, you cannot unset it. For further details on the logic used when the **Redirect URI** field is set, refer to the OIDC Feature Description.

Authorization Endpoint URL

Enter the OAuth 2.0 authorization endpoint URL of the application. The maximum number of characters permitted in this field is 255.

Token Endpoint URL

Specify the OAuth 2.0 Token End Point URL of the application. The maximum number of characters permitted in this field is 255.

Logoff URL

Specify the Logout URL of the application. The maximum number of characters permitted in this field is 255.

Application Secret

Specify the value of the Client Secret of the application.

Session Control

Select the **Session Control**:

- **Session Idle Duration**
- **Session Max Duration**

Session Idle Duration/Session Max Duration

Specify the idle or max duration for the session (depending on what is selected for **Session Control**.

RADIUS Two-factor and LDAP Authentication

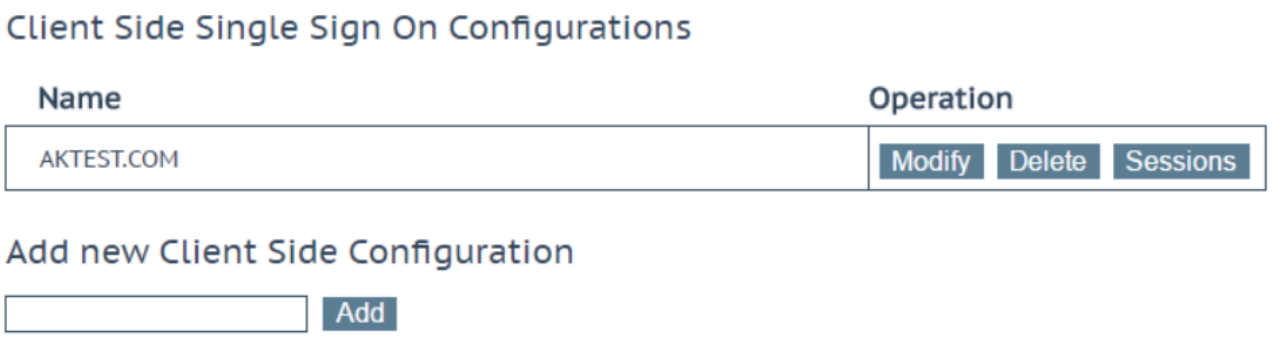
As of LoadMaster firmware version 7.2.52, RADIUS two-factor and LDAP authentication is supported. To configure this:

1. Select **RADIUS and LDAP** as the **Authentication Protocol** when adding or modifying a client-side Single Sign On (SSO) domain in **Virtual Services > Manage SSO**. If the RADIUS server is configured to use two-factor authentication, the LoadMaster will detect this automatically and perform RADIUS two-factor authentication.
2. Set the LDAP Endpoint and RADIUS Server(s) for this SSO domain.

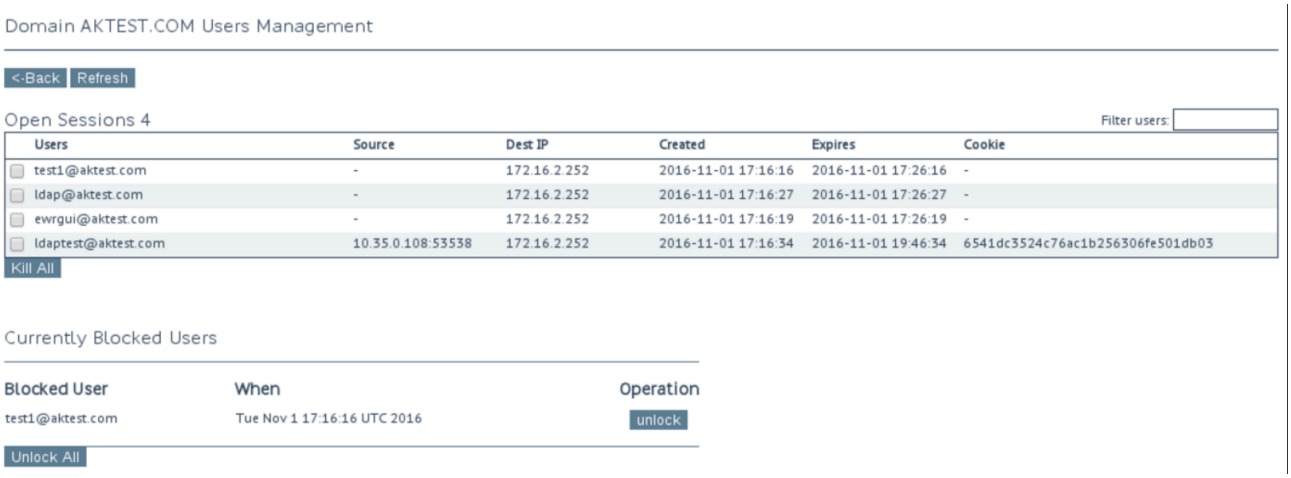
   Note: The LoadMaster uses the credentials specified for the LDAP Endpoint configuration to contact the RADIUS and LDAP servers and verify client SSO credentials. So, these administrative credentials must be configured on all the RADIUS and LDAP servers in the domain.

3. Select **Exchange** or **Blank** as the **SSO Image Set** in the **ESP Options** section of the Virtual Service **Modify** screen.
4. Set the other parameters as appropriate for your configuration.

Sessions



Clicking the **Sessions** button, for a client-side SSO domain, opens a screen listing the current open sessions on that domain.

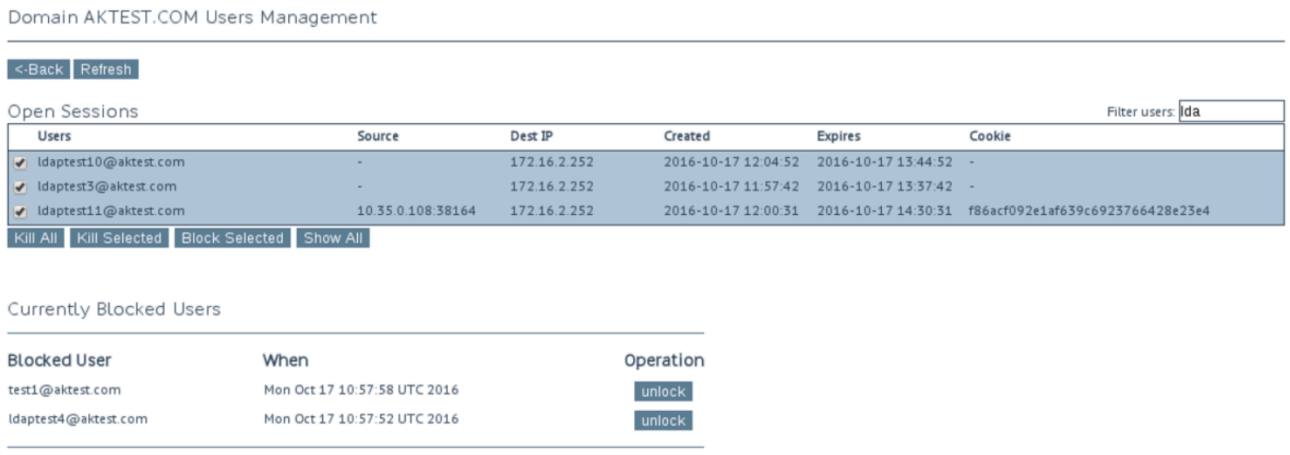


You can filter the list by entering a search term in the **Filter users** text box.

The following information is provided about each session:

- **Users:** The username/domain of the client.
- **Source:** The client (host) IP address and source port.
- **Dest IP:** The destination IP address of the connection.
- **Created:** The date and time that the connection was created.
- **Expires:** The date and time that the connection expires.
- **Cookie:** The cookie used in the connection.

Clicking the **Kill All** button kills all open sessions (flushes the SSO cache).



Selecting one or more sessions provides some further options:

- Kill Selected
- Block Selected
- Show All

Logs are added to the audit log for every kill session operation. For example:

- Kill 'non-cookie' session log:Nov 9 16:47:31 LM ssomgr: Deleted a session tester@aktest.com:- for domain AKTEST.COM
- Kill 'cookie' session log:Nov 9 16:47:31 LM ssomgr: Deleted a session ldaptest@aktest.com:420cf78373643b3c0171d95c757e7bf3 for domain AKTEST.COM
- Kill all domain sessions log:Nov 9 16:48:46 LM ssomgr: Deleted all domain AKTEST.COM user sessions

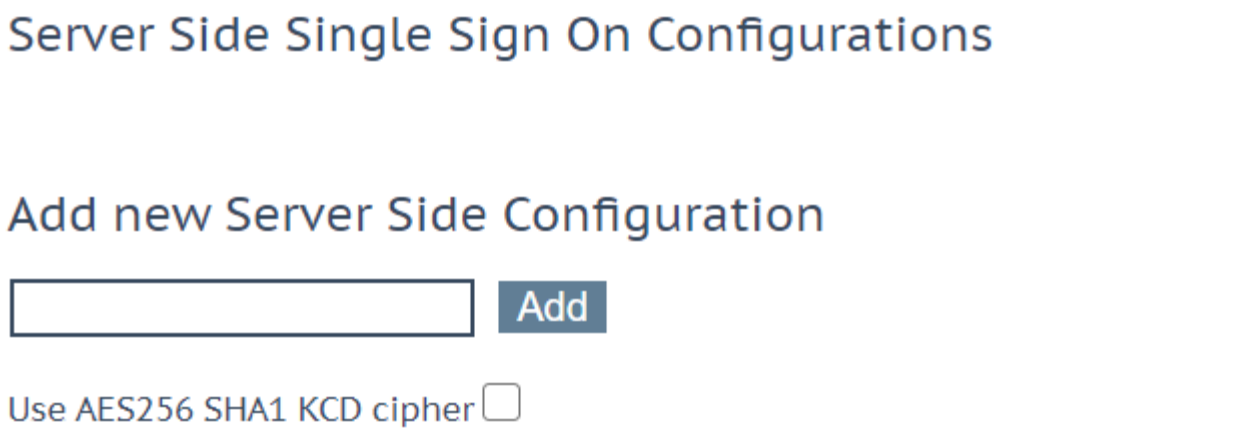
Currently Blocked Users

This section displays a list of users who are currently blocked and it also shows the date and time that the block occurred. It is possible to remove the block by clicking the **unlock** button in the Operation drop-down list.

Note: Different formats of the same username are treated as the same username, for example **administrator@progress.net**, **progress\administrator** and **progress.net\administrator** are all treated as one username.

Server Side (Outbound) SSO Domains

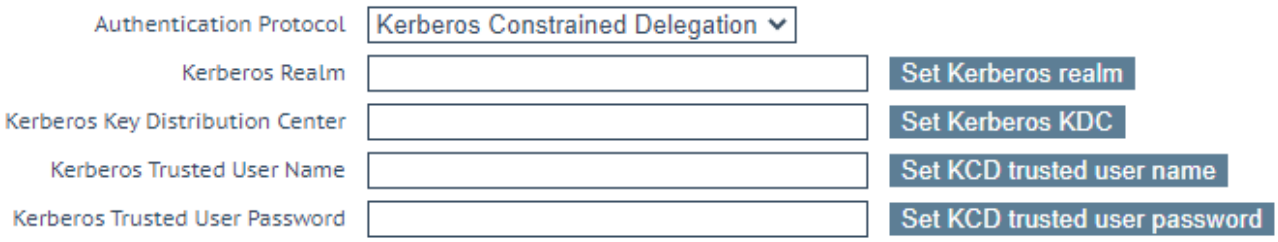
When using Kerberos Constrained Delegation as the Server Side Authentication Protocol it is a requirement to create a Server Side SSO domain. This contains all the configuration required to complete authentication on the LoadMaster to server connection.



In the **Server Side Single Sign On Configurations** section of the **Manage SSO** screen, on creating the Server Side SSO, you may choose to utilize **Use AES256 SHA1 KCD cipher** by selecting the checkbox (by default the RC4 cipher is used). While enabling/disabling the **Use AES256 SHA1 KCD cipher** checkbox, a pop-up message appears that says "The KCD cipher set has been changed. Click OK to activate immediately, which will stop existing sessions. Click Cancel to activate later when the Kerberos key table expires.". If you click **OK**, the SSO cache is flushed which stops existing sessions. If you click **Cancel**, the change activates later when the Kerberos key table expires.

Note: If you change the value of the Use **AES256 SHA1 KCD** cipher check box using the Chrome browser and you navigate to a different tab while the pop-up message is displayed, the pop-up disappears and the value of the check box gets set. Because you did not click **OK** on the pop-up, the SSO cache is not flushed.

To add a new server-side SSO, enter the name of the SSO configuration and click **Add**.



Authentication protocol

This dropdown allows you to select the transport protocol used to communicate with the authentication server. The only option available for outbound (server side) configurations is **Kerberos Constrained Delegation** (KCD).

For further information on KCD, please refer to the **KCD Feature Description** on the Documentation Page.

Kerberos Realm

The address of the Kerberos Realm.

Note: Colons, slashes and double quotes are not allowed in this field.

Note: This field only supports one address.

Kerberos Key Distribution Center (KDC)

The host name or IP address of the Kerberos Key Distribution Center. The KDC is a network service that supplies session tickets and temporary session keys to users and computers within an Active Directory domain.

When you configure a server-side Kerberos Constrained Delegation (KCD) Single Sign On (SSO) domain, you specify details for the domain. As of LoadMaster firmware version 7.2.51, you can specify two Kerberos Key Distribution Centers (KDCs) separated by a space. This provides a backup in case the active KDC becomes unavailable. Prior to version 7.2.51, you could only specify one KDC.

The first KDC you enter becomes active until it fails. KDC availability is checked and if the KDC fails to respond successfully three times, or if it times out for five seconds, the active KDC is switched. There is no automatic fail-back functionality - the second KDC will be active until it becomes unavailable. To switch back to the first KDC if a failover has occurred and the first KDC becomes available again, clear the SSOMGR cache by going to **System Configuration > Logging Options > System Log Files > Flush SSO Cache**.

When two KDCs are specified, the active Kerberos KDC is shown underneath the **Kerberos Key Distribution Center** field.

Note: If you enter more than one KDC, the username and password must be the same for both KDCs.

Note: Double and single quotes are not allowed in the **Kerberos Key Distribution Center** field.

Kerberos Trusted User Name

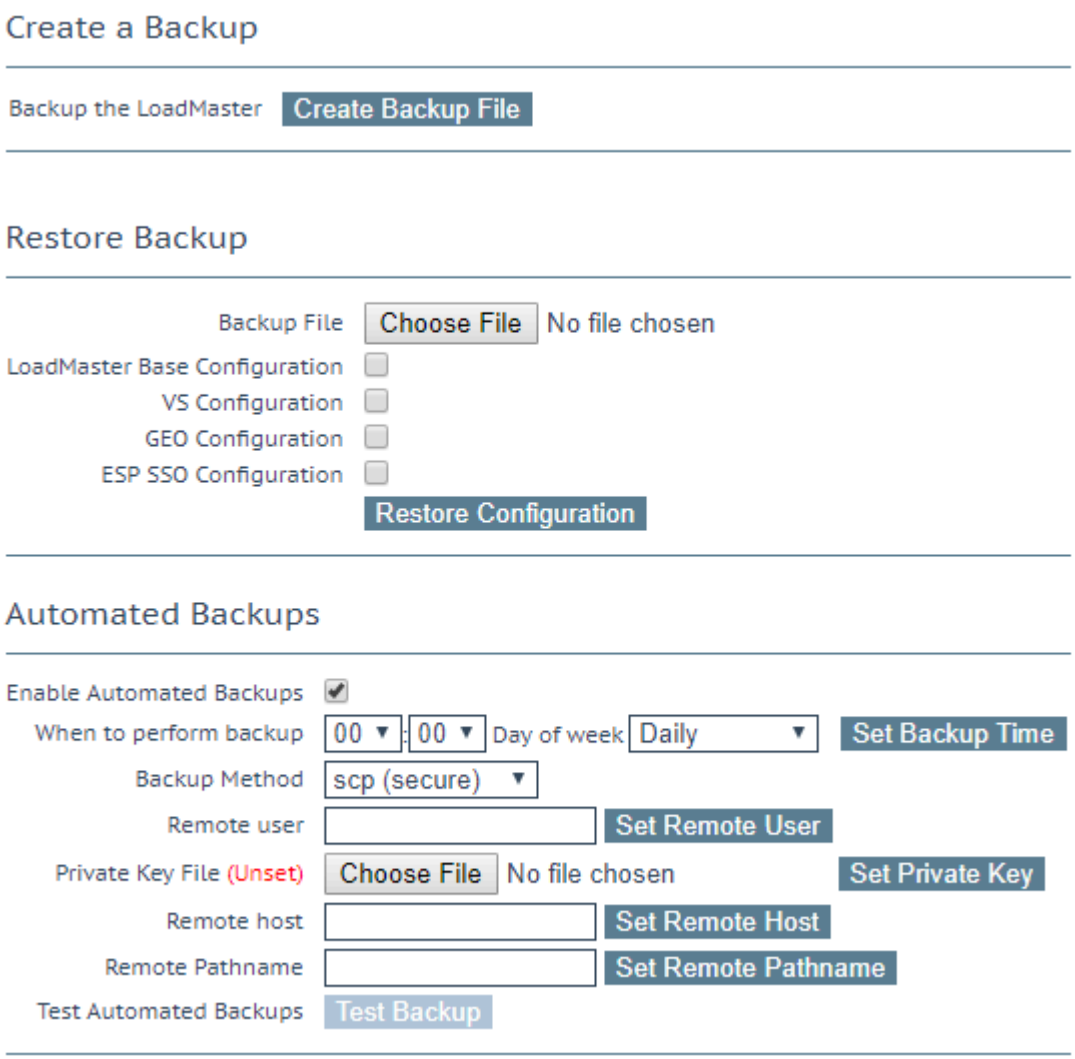
Before configuring the LoadMaster, a user must be created and trusted in the Windows domain (Active Directory). This user should also be set to use delegation. This trusted administrator user account is used to get tickets on behalf of users and services when a password is not provided. The user name of this trusted user should be entered in this text box.

Note: Double and single quotes are not allowed in this field.

Kerberos Trusted User Password

The password of the Kerberos trusted user.

Backup/Restore



Create Backup File

Generate a backup that contains the Virtual Service configuration, the local appliance information and statistics data. License information and SSL Certificate information is not contained in the backup.

For further details on what is not included in LoadMaster backups, refer to the following page: Important Notes.

For ease of identification, the Backup file name includes the LoadMaster's hostname.

By default, the LoadMaster includes a Netstat output in backups taken. When this is included, backups take longer to complete. You can stop the Netstat output from being included by disabling the **Include Netstat in Backups** option in the **Troubleshooting** screen (**System Configuration > Troubleshooting**).

Restore Backup

When performing a restore (from a remote machine), the user may select what information should be restored:

- **VS Configuration**
- **LoadMaster Base Configuration**
- **GEO Configuration**
- **ESP SSO Configuration** (This restores the SSO domains, LDAP endpoints and SSO custom image sets. This does not restore the Virtual Service settings - use the **VS Configuration** option to restore those.)
- A combination of the options

Note: It is not possible to restore a single machine configuration onto a HA machine or restore a HA configuration onto a single machine.

Note: It is not possible to restore a configuration with ESP-enabled Virtual Services onto a machine which is not enabled for ESP.

Note: A WAF configuration can only be restored onto a LoadMaster with a WAF license.

Note: If you restore a backup taken on LoadMaster version 7.2.58 or below (with Legacy Web Application Firewall (WAF) enabled on some Virtual Services) to a fresh install of 7.2.59 or above (where Legacy WAF is no longer available) - the LoadMaster will enable OWASP WAF on the affected Virtual Services with default WAF settings. If this happens, a message is displayed listing the Virtual Services and SubVSs that were affected. You should review these Virtual Services and make any modifications needed.

Automated Backups

If the **Enable Automated Backups** check box is selected, the system may be configured to perform automated backups on a daily or weekly basis.

For ease of identification, the Backup file name includes the LoadMaster's hostname.

If the automated backups are not being performed at the correct time, ensure the NTP settings are configured correctly. For further information, refer to the Date/Time section.

When to perform backup

Specify the time (24 hour clock) of backup. Also select whether to backup daily or on a specific day of the week. When ready, click the **Set Backup Time** button.

Note: In some situations, spurious error messages may be displayed in the system logs, such as:Dec 8 12:27:01 Kemp_1 /usr/sbin/cron[2065]: (system) RELOAD (/etc/crontab)Dec 8 12:27:01 Kemp_1 /usr/sbin/cron[2065]: (CRON) bad minute (/etc/crontab)

Note: These can be safely ignored and the automated backup will likely still complete successfully.

Backup Method

Select the file transfer method for automated backups:

- Ftp (insecure)
- scp (secure)
- sftp (secure)

If using scp or sftp, the **Private Key File** must be supplied.

Remote user

Set the username required to access remote host.

Private Key File

If using scp as the backup method, the **Private Key File** must be provided. This is the SSH private key generated using ssh-keygen on the remote scp server.

Remote password

The **Remote password** is used when the **Backup Method** is set to **Ftp (insecure)**. Set the password required to access remote host. This field accepts alphanumeric characters and most non-alphanumeric characters. Disallowed characters are as follows:

- Control characters
- ‘ (apostrophe)
- ` (grave)
- The delete character

Remote host

Set the IP address or hostname of the remote host to which you want the backup archives sent, optionally followed by a colon and the port number. If no port is specified, the default port for the selected protocol is used.

Remote Pathname

Set the location on the remote host to store the file.

Test Automated Backups

Clicking the **Test Backup** button performs a test to check if the automated backup configuration is working correctly. The results of the test can be viewed within the System Message File.

Debug Options

There are a couple of ESP-specific Debug Options in the WUI. These are described below.

To get to the **Debug Options** screen - in the LoadMaster WUI, go to **System Configuration > Logging Options > System Log Files > Debug Options**.

Contents

- Enable SSOMGR Debug Traces
- Flush SSO Authentication Cache
- SSO LDAP Server Timeout
- Linear SSO Log Files

Enable SSOMGR Debug Traces

Enabling this option will record any login attempts to the SSO domains configured on the LoadMaster. When this option is enabled, the SSOMGR traces are printed in the main syslog file.

Note: These are debug logs and should only be enabled when troubleshooting specific issues with Progress Kemp Support. This option should not be enabled all the time because it would degrade system performance and resource usage.

The syslogs are rotated on a per size/day manner. They are rotated every day at midnight or when the size reaches 10MB. Rotated files older than seven days are automatically removed.

To view, clear, and save these logs, go to **System Configuration > Logging Options > System Log Files** in the LoadMaster User Interface (UI).

ESP User Logs

Note: In LoadMaster firmware version 7.2.51, ESP user logs were expanded to be more useful and applicable to enterprise customers with extensive logging infrastructure. User Authentication, Authorization, and Accounting (AAA) information is included in the logs, including the time of request, username, domain, AAA server, AAA protocol type, AAA result, and error message.

To view, clear, and save the ESP user logs, go to **System Configuration > Logging Options > Extended Log Files** in the LoadMaster User Interface (UI).

Here is an example of these logs:

2021-09-08T07:34:22-04:00 lb100 ssomgr: vs=10.35.46.240:80 user=mgupta@kpauto.net domain=kempqaesp.net server=172.20.7.170 protocol=LDAP Unencrypted result=0:Success

...

2021-09-08T08:08:40-04:00 lb100 ssomgr: vs=10.35.46.240:80 user=mgupta@kpauto.net domain=KPAUTO.NET msg=Deleted expired user session, start time:1631102854 duration:66 seconds

You can generate these logs in Common Event Format (CEF) by enabling the **Use CEF Log Format** check box in **System Configuration > Miscellaneous Options > L7 Configuration**. Here is an example of these CEF logs:

2021-09-08T07:17:15-04:00 lb100 ssomgr: CEF:0|Kemp|LM|1.0|100|User AAA|0|vs=10.35.46.240:80 event=User AAA user=mgupta@kpauto.net domain=kempqaesp.net server=172.20.7.170 protocol=LDAP Unencrypted result=0:Success

...

2021-09-08T07:32:22-04:00 lb100 ssomgr: CEF:0|Kemp|LM|1.0|101|User session timeout|0|vs=10.35.46.240:80 event=User session timeout user=mgupta@kpauto.net domain=KPAUTO.NET msg=Deleted expired user session, start time:1631099835 duration:906 seconds

In LoadMaster firmware version 7.2.53, the ESP client session logging was further enhanced. The LoadMaster logs:

- The initially created ESP session

  CEF:0|Kemp|LM|1.0|8|Logged on|1|vs=10.35.46.157:443 event=Logged on srcip=10.35.2.45 user=mgupta@kempqaesp.net msg=logged on

- The time when the LoadMaster cleared the session from the cache. Note that if the entire cache is cleared, a single log message is recorded at the time of clearing, which notes that all existing sessions at that time were cleared form the cache.

  CEF:0|Kemp|LM|1.0|104|Flush SSO cache|1|event=Flush SSO cache msg=SSO cache being flushed user sessions:1 cookie sessions:0

- If an ESP session is deleted (when the user logs out from the application, when the session expires, or the user enters invalid credentials). The time of when the LoadMaster cleared the session is also logged.

  CEF:0|Kemp|LM|1.0|101|User session timeout|0|vs=10.35.46.242:443 event=User session timeout user=mohit@parent.net domain=MULLTIDOMAIN msg=Deleted expired user session, start time:1629182393 duration:69 seconds

  CEF:0|Kemp|LM|1.0|102|User session kill|0|vs=10.35.46.235:443 event=User session kill user=mohit@parent.net domain=MULLTIDOMAIN msg=Deleted user session, start time:1629378587 duration:8 seconds

  CEF:0|Kemp|LM|1.0|103|Kill all sessions|0|event=Kill all sessions domain=MULLTIDOMAIN msg=Deleted 1 user session(s) associated with domain

All logs related to ESP that are produced by the LoadMaster application running over Layer7 (including the connection, security, and user logs) support CEF. All other LoadMaster logs do not support CEF format – including logs produced by enabling the **Enable SSOMGR Debug Traces option** (which are printed in /var/log/messages).

Flush SSO Authentication Cache

Clicking the **Flush SSO Cache** button flushes the Single Sign-On cache on the LoadMaster. This has the effect of logging off all clients using Single Sign-On and forces the clients to re-connect to the LoadMaster.

SSO LDAP Server Timeout

You can configure the SSO LDAP server timeout value in seconds (default value is 5 seconds).

Linear SSO Log Files

By default, older log files are deleted to make room for newer log files, so that the filesystem does not become full. By default, the last 30 days of logs are stored. Selecting the **Linear SSO Log Files** check box prevents older files from being deleted.

Note: When using Linear SSO Logging, if the log files are not periodically removed and the file system becomes full, access to Virtual Services with ESP enabled is blocked, preventing unlogged access to the Virtual Service. Access to non-ESP enabled Virtual Services are unaffected by the Linear SSO Log File feature.

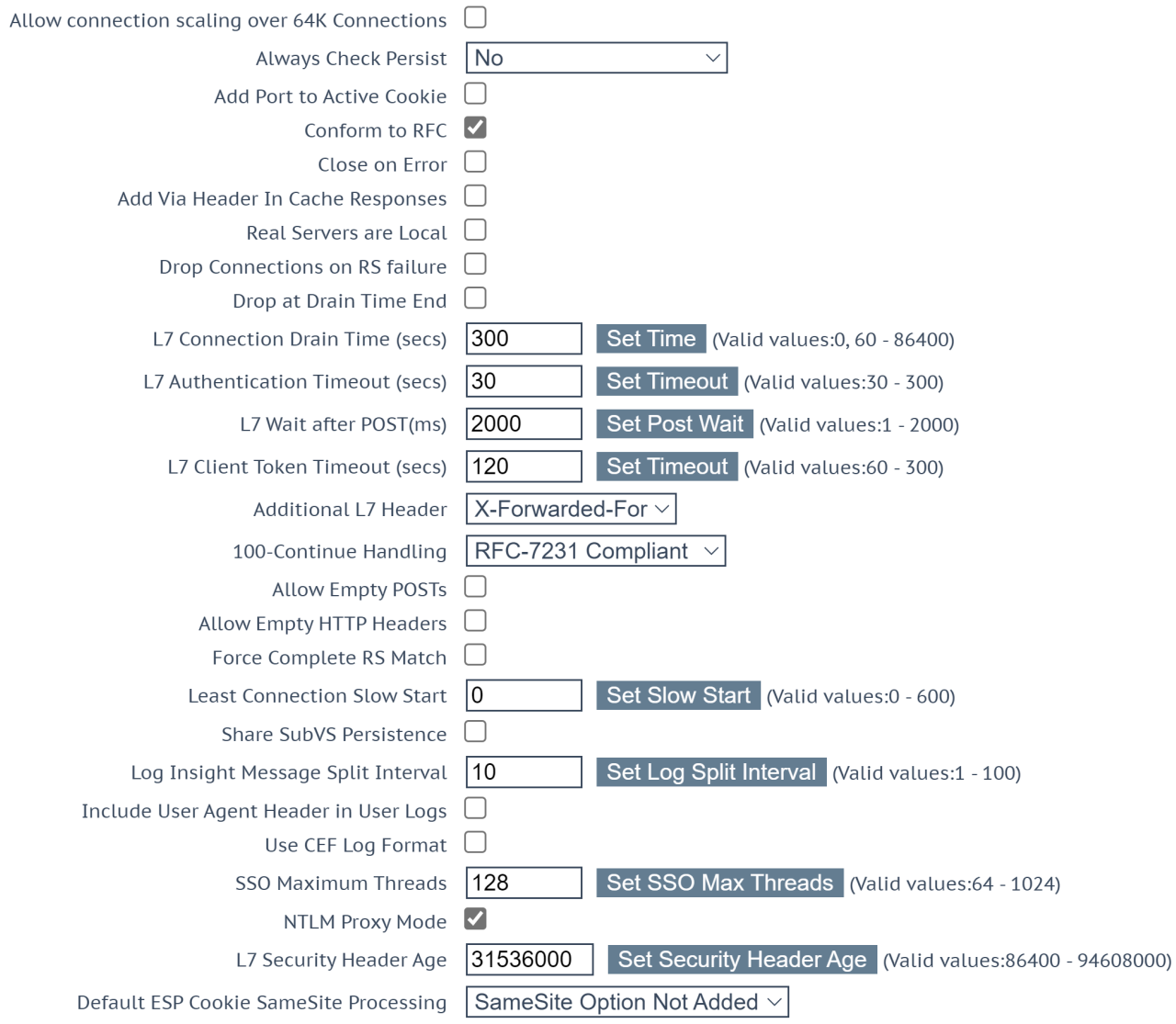
Miscellaneous Options

To get to the **Miscellaneous Options** section – in the LoadMaster WUI, go to **System Configuration > Miscellaneous Options**. In this section there are sub-sections for **L7 Configuration** and **Network Options**.

Contents

- L7 Configuration
- Network Options

L7 Configuration



L7 Authentication Timeout

When configuring ESP, users can set the **L7 Authentication Timeout (secs)** option.

This option supports the integration with third party, multi-factor, authentication solutions which may have secondary processes such as SMS or telephone verification. This setting determines how long (in seconds) the SSO form waits for authentication verification to complete before timing out.

L7 Client Token Timeout (secs)

The duration of time (in seconds) to wait for the client token while the process of authentication is ongoing (used for RSA SecurID and RADIUS authentication). The range of valid values is 60 to 300. The default value is 120.

Include User Agent Header in User Logs

When enabled, the User Agent header field gets added to the User Logs.

Use CEF Log Format

When enabled, the ESP logs are generated in Common Event Format (CEF). CEF log format is easily consumable for Security Information and Event Management (SIEM) tools, such as; Splunk, SolarWinds, LogRhythm, AlienVault, and so on.

SSO Maximum Threads

The maximum number of allowed threads for SSO authentication attempts. The range of valid values is 64 to 1024. The default value is 128.

NTLM Proxy Mode

In LoadMaster firmware version 7.2.48.4 Long Term Support (LTS) and 7.2.53, the **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, **NTLM Proxy Mode** is enabled by default.

When **NTLM Proxy Mode** is enabled, NTLM authorization works against the Real Servers. If **NTLM Proxy Mode** is disabled, the old insecure NTLM processing is performed.

Note: We highly recommend ensuring that **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**.

Default ESP Cookie SameSite Processing

This option allows you to set the default value of the SameSite option for cookies sent by the LoadMaster during ESP processing. The SameSite attribute tells browsers when and how to process cookies in first-party or third-party situations. SameSite is used by a variety of browsers to identify whether or not to allow a cookie to be accessed.

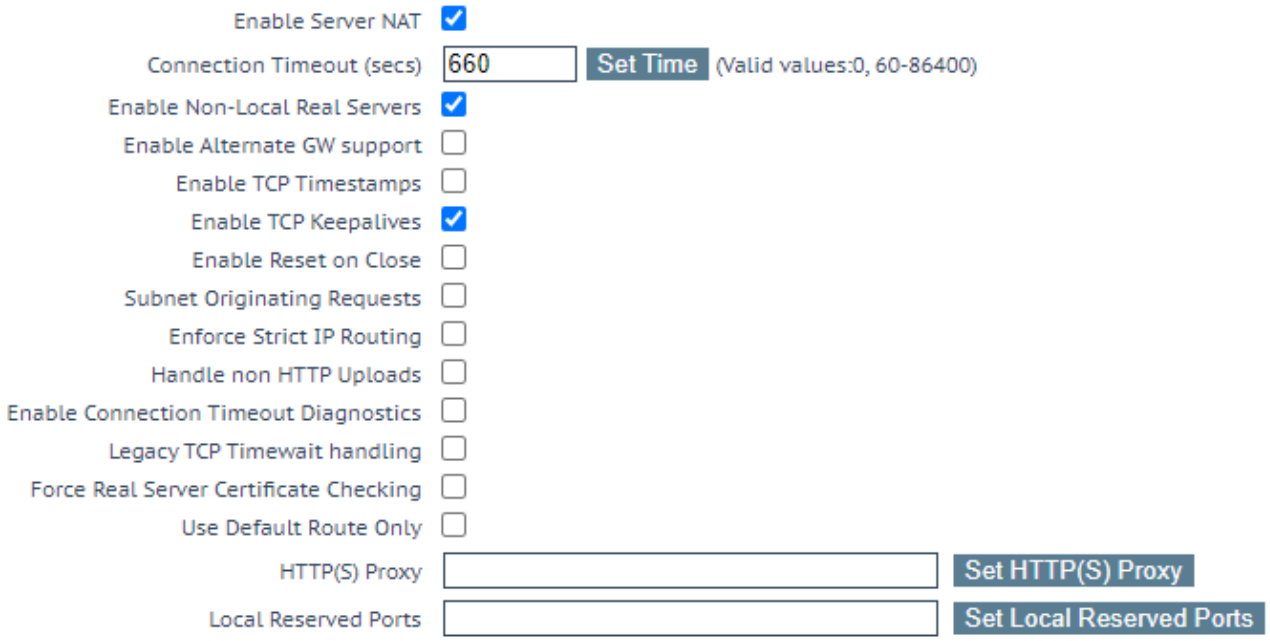
The following are the SameSite options:

- **SameSite option not added**
- **SameSite=None:** Signals that the cookie data can be shared with third parties/external sites (for advertising, embedded content, etc).
- **SameSite=LAX:** Signals that the cookie may be used as a first party cookie but may also be used when accessing the site from an external site via a link clicked by the user.
- **SameSite=Strict:** It is a subset of lax and only enables the cookie be used in first party context and excludes its use when accessing via an incoming link from an external site.

Network Options

When configuring ESP, to generate timeout logs, users can **Enable Connection Timeout Diagnostics** in

the **Network Options** screen in the WUI.



By default, connection timeout logs are not enabled. This is because they may cause too many unnecessary logs. If you wish to generate logs relating to connection timeouts, select the **Enable Connection Timeout Diagnostics** check box.

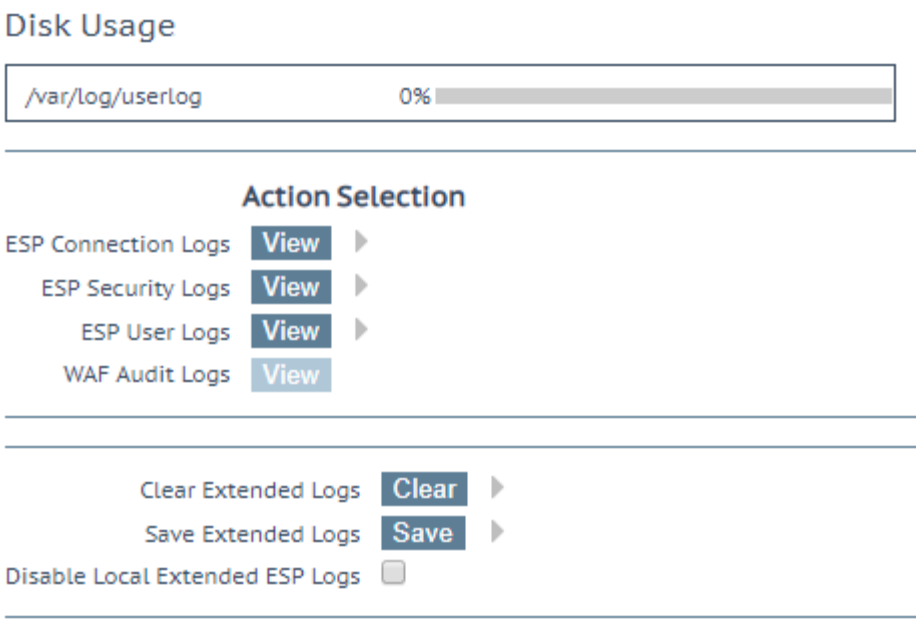
Logging Options

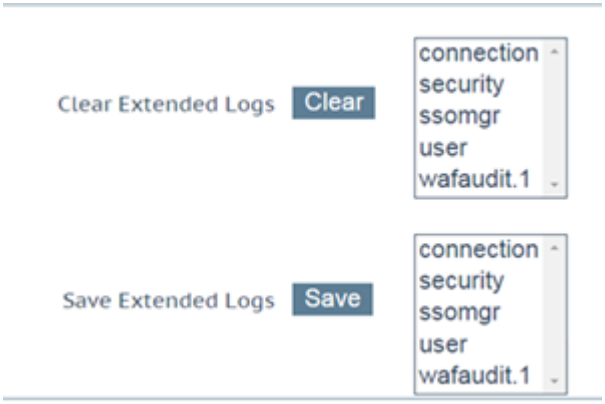
The **Extended Log Files** screen provides options for logs relating to the ESP feature.

The ESP and Web Application Firewall (WAF) audit logs are rotated every 30 days (older logs are removed). WAF remote logs are rotated every seven days.

Note: If debug logging is enabled, it is possible that sensitive information may appear in the logs. If you are concerned by this, clear all the logs immediately after disabling debug logging.

To get to the **Extended Log Files** screen – in the LoadMaster WUI, go to **System Configuration > Logging Options > Extended Log Files**.





Disk Usage - This section provides an indication of the percentage used/free of the log partition. Color-coding is used to highlight different usage levels:

- 0% to 50%: green
- 50% to 90%: orange
- 90% to 100%: red

There are multiple log files relating to ESP stored on the LoadMaster. These are listed below the **Disk Usage** section. These logs are persistent across LoadMaster reboots.

You can select one of the **View** or **Save Action** buttons with the default filter options to apply the action to the various log files (Connection Logs, Security Logs, and so on). For the **Clear** button, you must first select which logs to clear using the **Selection** controls.

To access the **Selection Controls**, click one of the right caret icons ▸ at the right of the buttons. For example, clicking on the icon to the right of the **Clear** and **Save** buttons, displays these controls.



You can filter the logs to clear or save by selecting a subset of log files from the multiple pick list on the right.

- **ESP Connection Logs:** logs recording each connection
- **ESP Security Logs:** logs recording all security alerts
- **ESP User Logs:** logs recording all user logins. If the user is known, the URL which is being accessed by the user is recorded in the user log.

In LoadMaster firmware version 7.2.51, ESP user logs were expanded to be more useful and applicable to enterprise customers with extensive logging infrastructure. User Authentication, Authorization, and Accounting (AAA) information is included in the logs, including the time of request, username, domain, AAA server, AAA protocol type, AAA result, and error message. For further details, refer to the section Enable SSOMGR Debug Traces.

In LoadMaster firmware version 7.2.53, the ESP client session logging was further enhanced. The LoadMaster logs:

- The time when the LoadMaster cleared the session from the cache. Note that if the entire cache is cleared, a single log message is recorded at the time of clearing, which notes that all existing sessions at that time were cleared form the cache.

- If an ESP session is deleted (when the user logs out from the application, when the session expires, or the user enters invalid credentials). The time of when the LoadMaster cleared the session is also logged.

To view the logs, select the relevant options and click **View**. For more information, refer the **Extended Log Files** section of the Web User Interface document.

It is possible to view logs for as far back as they have been stored. By default, logs are stored for the last 30 days. One or more archived log files can be viewed by selecting the relevant file(s) from the list of file names and clicking **View**. The logs can be filtered by entering a word(s) or regular expression in the filter field and clicking **View**.

Clear Extended Logs

Extended logs can be deleted by first selecting the logs to remove and then clicking **Clear**. An error is returned if you don't select the logs to remove first.

Save Extended Logs

Click the arrow to expand the options. Select a file type (for example, **connection**). Click **Save** . This saves a file to your machine.

Specific log files can be saved by filtering one or more individual log files in the log file list or selecting a specific log type (for example connection, security or user) in the log file list and clicking **Save**.

Note: For further information on the ESP logs, refer to the **ESP Logs Technical Note** on the Documentation Page.

Disable Local Extended ESP Logs

If **Disable Local Extended ESP Logs** is disabled (the default option), messages are written to the extended ESP logs expediently and are not sent to any remote syslog servers that are defined.

If **Disable Local Extended ESP Logs** is enabled, no messages are written to the extended ESP logs and messages are only sent to the remote logger (if one is defined). If a remote logger is not defined, no logs are recorded.

You can no longer configure the system to both populate the local extended ESP logs and send the same messages to remote syslog servers, as it was in previous releases.

4

Setting up a Virtual Service with ESP

This section details the various steps required to configure ESP on a Virtual Service.

Note: In order to enable ESP functionality on an encrypted service, an SSL certificate must be imported to the LoadMaster. The certificate must contain a private key. This document assumes that the certificate has already been imported correctly.

Note: For further details on how to configure SSL Certificates, please reference the SSL Accelerated Services, Feature Description document.

Contents

- Create a Single Sign-On (SSO) Domain
- Create a Virtual Service
- Configure a Simple Mail Transfer Protocol (SMTP) ESP Service

Create a Single Sign-On (SSO) Domain

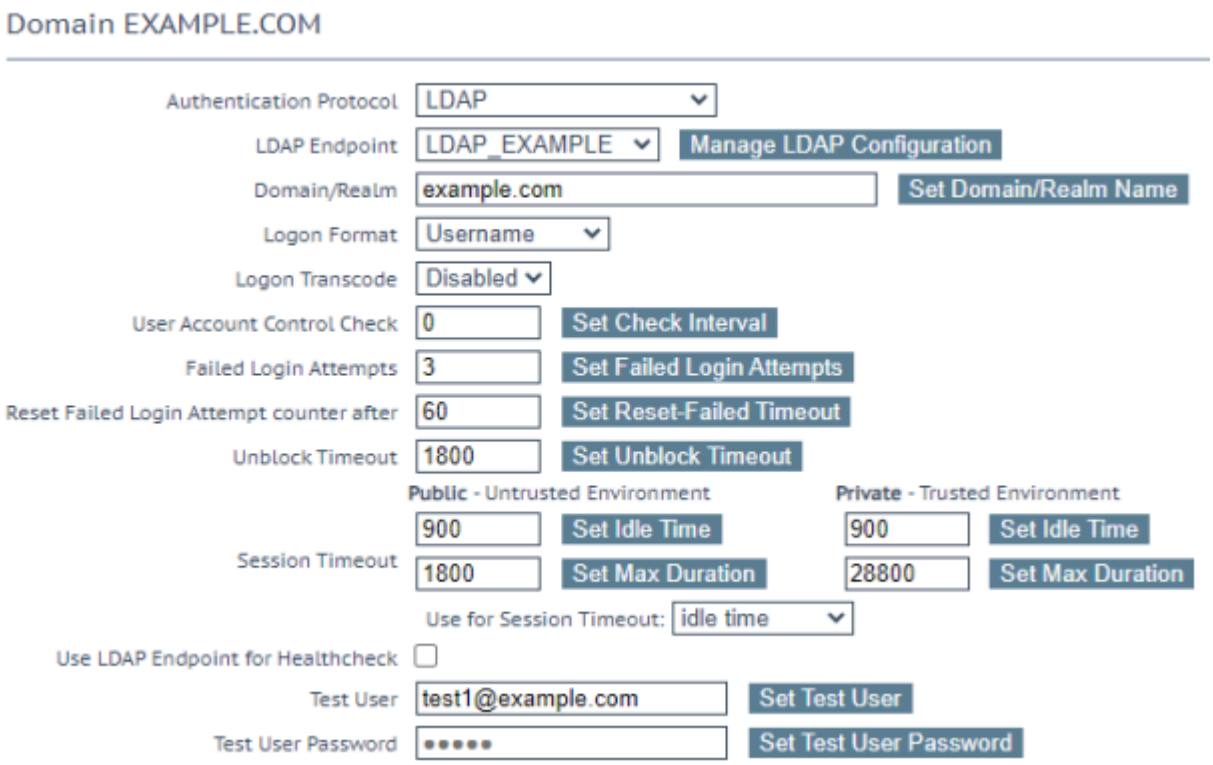
Note: The maximum number of SSO domains that are allowed is 128.

Follow the steps below to create an SSO domain:

1. Log in to the LoadMaster.
2. Select **Virtual Services** in the main menu and select **Manage SSO Domains**.



3. Enter the name of the domain and click **Add**.



4. Select **LDAP** as the **Authentication Protocol**.

Note: The other configuration types and authentication protocols - **LDAP**, **RADIUS**, **RSA-SecurID**, **Certificates**, **RADIUS and LDAP**, and **RSA-SecurID and LDAP** - can be selected if the Active Directory environment is configured for it.

Note: For more information on the **RSA-SecurID**, **Kerberos Constrained Delegation** or **Certificates** options, including steps on how to configure them, refer to the relevant documents: - RSA Two Factor Authentication, Feature Description - Kerberos Constrained Delegation, Feature Description

---

5. Select the relevant LDAP endpoint in the **LDAP Endpoint** drop-down list. For further information on LDAP endpoints, refer to the LDAP Configuration section.
6. In the **Domain/Realm** field, enter the login domain to be used.

Note: This is also used with the logon format to construct the normalized username, for example; - **Principalname:** <username>@<domain> - **Username:** <domain>\<username>

Note: If the **Domain/Realm** field is not set, the **Domain** name set when initially adding an SSO domain

---

is used as the **Domain/Realm** name.

7. Select the relevant **Logon format**. The login format comprises of two options, as outlined below:
   1. **principalname:** Selecting this as the Logon format means that the client does not need to enter the domain when logging in, for example **username@domain**. The SSO domain entered in the corresponding text box is used as the domain in this case.

      Note: When using **RADIUS** as the **Authentication protocol** the value in this SSO domain field must exactly match for the login to work. It is case sensitive.

   2. **username:** Selecting this as the logon format means that the client needs to enter the domain and username, for example **domain\username**.
8. Specify the number of **Failed Login Attempts** that a user can have before their account is locked out. Click **Set Failed Login Attempts**.

   Note: When a user is locked out, all existing logins for that user are terminated, along with future logins. Users can be unblocked in the **Currently Blocked Users** section of the **Manage Domain** screen.

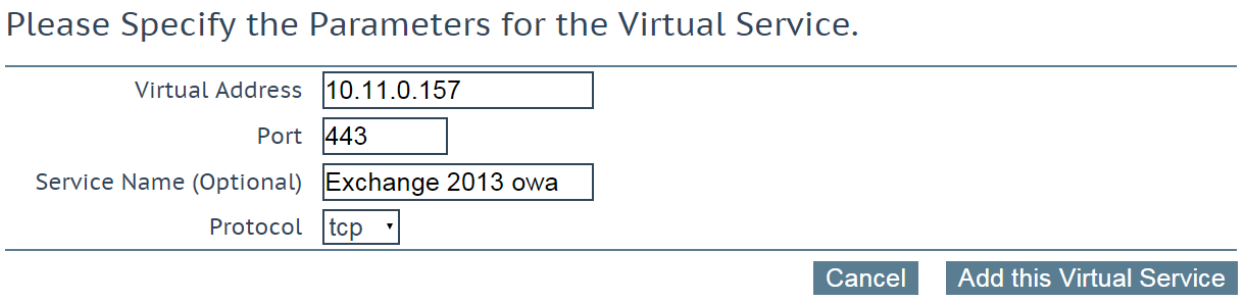
9. Enter the amount of time (in seconds) that you would like to **Reset Failed Login Attempt Counter after**. Click **Set Reset-Failed Timeout**.
10. Enter the amount of time (in seconds) after which a blocked user account is unblocked in the **Unblock Timeout** text box. Click **Set Unblock Timeout**.
11. Enter the relevant value(s) in the **public** and **private idle time** and **max duration** text box(es) and click the relevant button(s) as appropriate. The timeout value that is applied depends on whether the user selects public or private on the login screen.
12. Select the relevant option for **use value** (either **max duration** or **idle time**).
13. Select whether or not to use the LDAP endpoint for the health check.
14. If you have decided not to use the LDAP endpoint for the health check, in the **Test User** and **Test User Password** fields, enter credentials of a user account for the SSO Domain. The LoadMaster will use this information in a health check of the Authentication Server. This health check is performed every 20 seconds. This 20 second health check is hard coded and cannot be modified.
15. Click **OK**.

Note: It is also possible to **unlock** blocked users from the Manage Domain screen. To do this, simply click the **unlock** button for the relevant blocked user.

Create a Virtual Service

Follow the steps below to create a Virtual Service with ESP. In this example we will configure an **owa** for Exchange 2013 service.

1. In the menu on the left, click **Virtual Services** and select **Add New**.



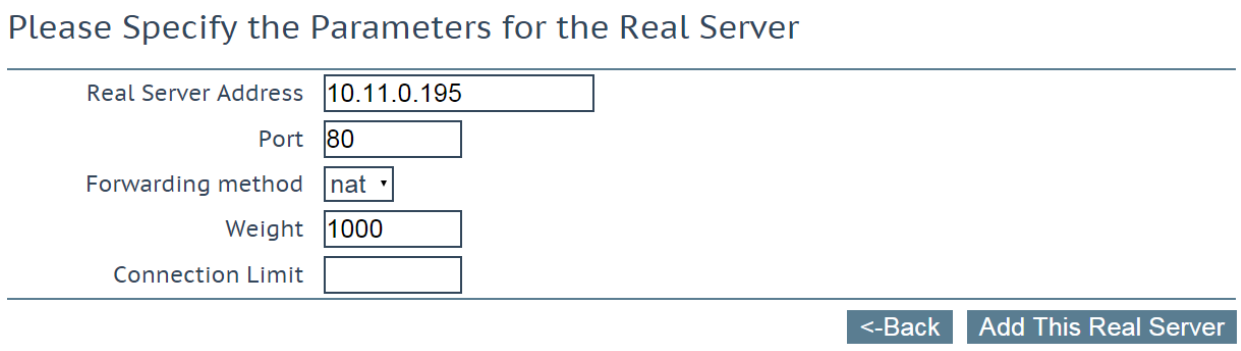
2. Enter the Virtual Address, for example **10.11.0.157**.

Note: This is the Virtual IP address of the Virtual Service. It must be unique and not in use by any other device on the network.

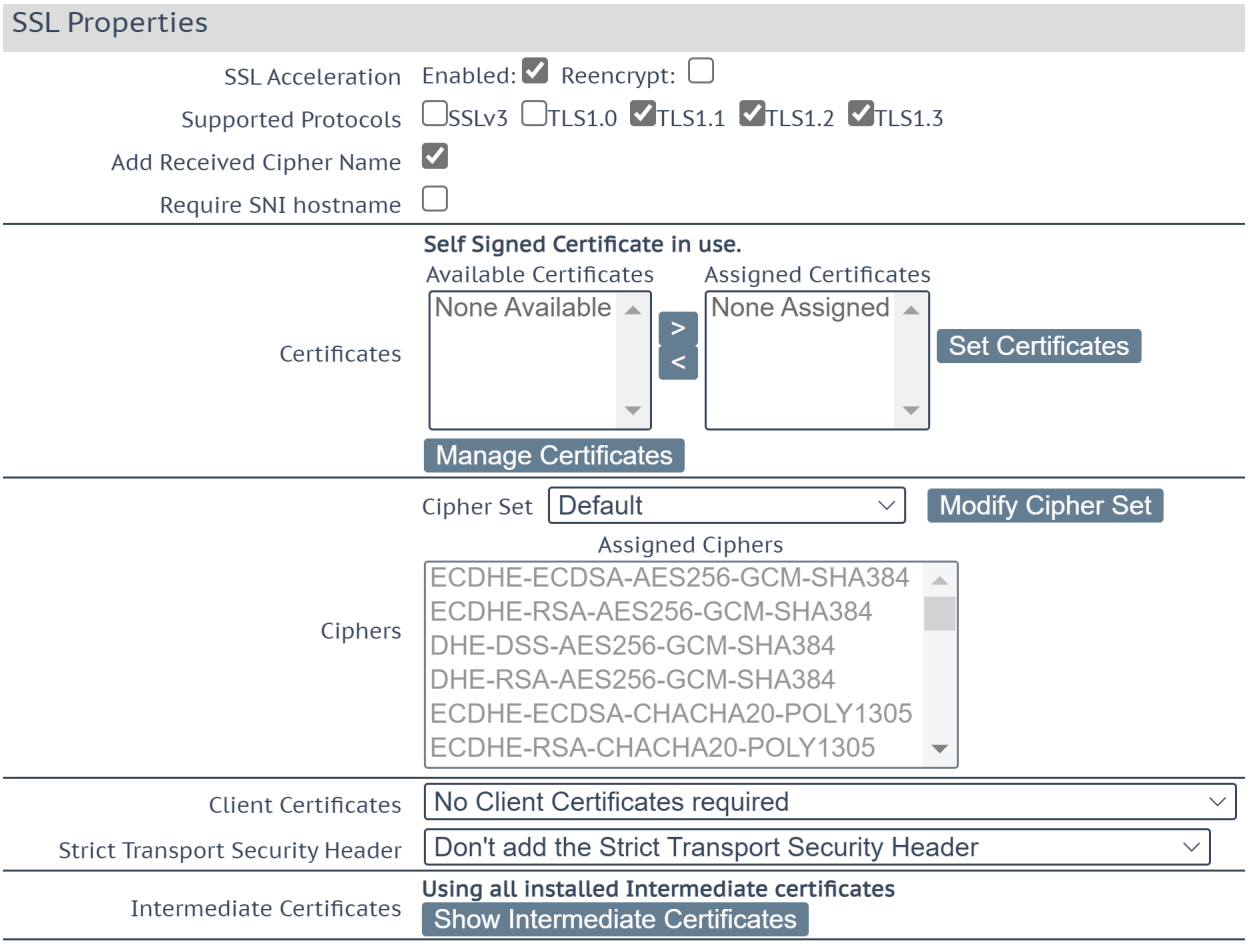
3. Enter **443** as the **Port** number as all workloads are accessing Exchange 2013 using HTTPS.

Note: Creating Virtual Services for other protocols is outside the scope of this document.

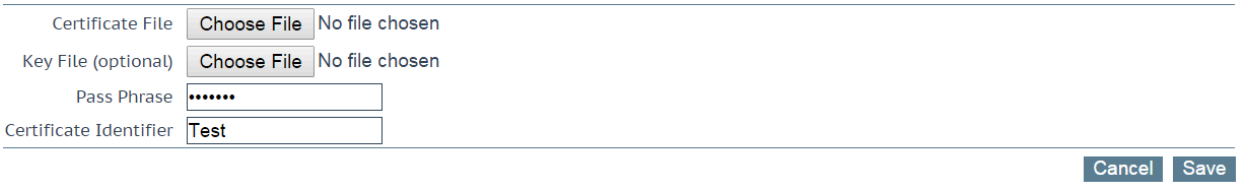
4. Enter the desired Service Name, for example **Exchange 2013 owa**.
5. Ensure that **tcp** is selected as the Protocol.
6. Click the **Add this Virtual Service** button.
7. Expand the **Real Servers** section.
8. Enter **/OWA/healthcheck.htm** as the **URL**.
9. Click the **Set URL** button.
10. Select **GET** from the **HTTP Method** drop-down list.
11. Click the **Add New** button.



12. Enter the relevant **Real Server Address**.
13. Enter **80** as the port.
14. Click **Add This Real Server**.
15. Expand the **SSL Properties** section.

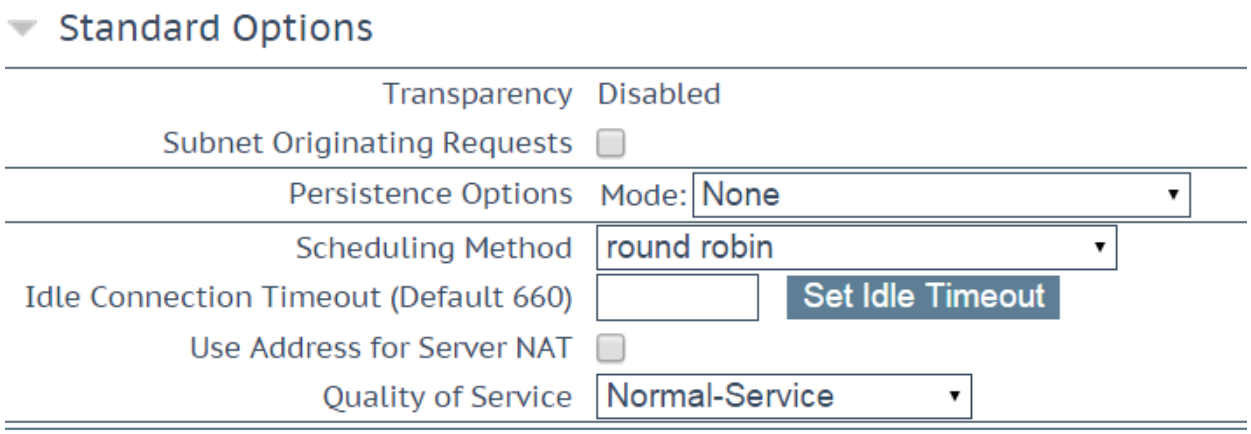


16. Select the **Enabled** checkbox.
17. Select the **Reencrypt** checkbox.
18. Click the **Manage Certificates** button.
19. Click **Import Certificate**.

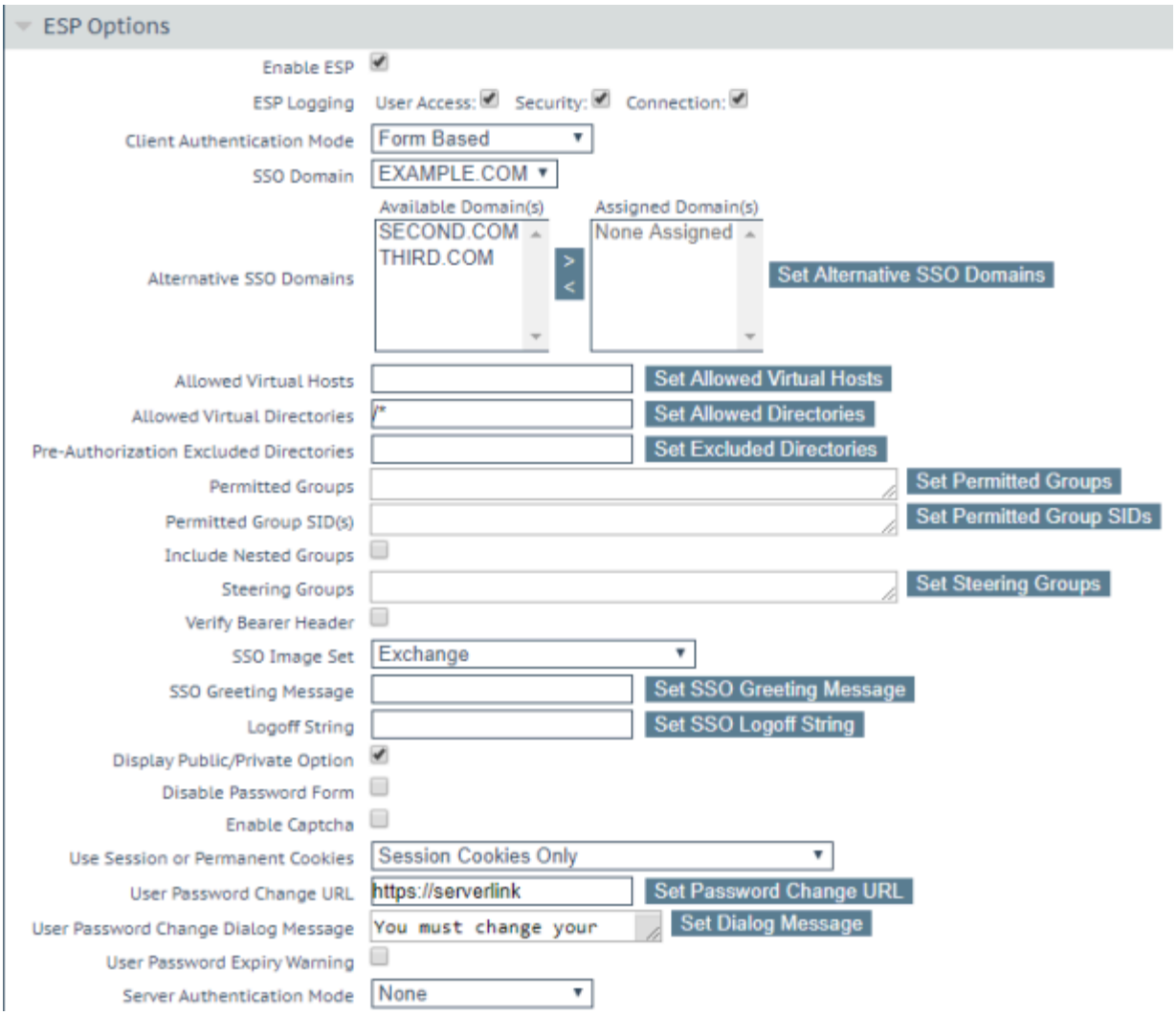


20. Click the first **Choose File** button.
21. Browse to and select the relevant certificate.
22. Click the second **Choose File** button.
23. If needed, browse to and select the relevant **Key File**.
24. Enter the **Pass Phrase**.
25. Enter a name for the certificate in the **Certificate Identifier** text box.
26. Click **Save**.
27. Click **OK**.

28. Select **View/Modify Services** in the main menu.
29. Click **Modify** on the relevant Virtual Service.
30. Expand the **Standard Options** section.



31. Ensure that **None** is selected as the **Persistence Options Mode**.
32. Ensure that **round robin** is selected as the **Scheduling Method**.
33. Expand the **ESP Options** section.



34. Select the **Enable ESP** check box.
35. Select the relevant option in the **Client Authentication Mode** drop-down list.
36. Select the relevant Domain that was created within the **SSO Domain** drop-down list.
37. Enter the relevant hosts in the **Allowed Virtual Hosts** text box, for example **mail.example.com**.

Note: More than one host can be provided by using a space-separated list. Wildcards can also be used, for example ***progressdemo.com**.

Note: The Allowed Virtual Hosts text box should contain host names, not IP addresses.

---

38. Enter any directories that can be accessed by the Virtual Services, for example **/owa*** in the **Allowed Virtual Directories** text box.
39. Click **Set Allowed Directories**.

Note: If a Virtual Service needs to allow more than one virtual directory, use a space-separated list. Optionally, a wildcard character can be used, for example **/*** to allow all virtual directories.

---

40. Enter all the virtual directories that will not be pre-authorized by this Virtual Service, for example, **/owa/guid*** in the **Pre-Authorization Excluded Directories** field.

41. Click **Set Excluded Directories**.

Note:

The Globally Unique Identifier (GUID) is unique to each organization. To find the correct GUID, run the following command on the Exchange Server:

Get-Mailbox -Arbitration | where {$_.PersistedCapabilities -like "OrganizationCapabilityClientExtensions"} | fl exchangeGUID, primarysmtpaddress

42. Enter any groups that are allowed to access this Virtual Service in the **Permitted Groups** text box.

Note: Multiple groups can be entered but the group names must be separated by a semi-colon.

Note: The following characters are not allowed in permitted group names: **/ : + ***

43. Click **Set Permitted Groups**.
44. Enable or disable the **Include Nested Groups** option.

Note: There is a theoretical limit of approximately six nested groups.

Note: This field relates to the **Permitted Groups** setting. Enable this option to include nested groups in the authentication attempt. If this option is disabled, only users in the top-level group are granted access. If this option is enabled, users in both the top-level and first sub-level group are granted access.

45. Select an **SSO Image Set**, if required.

Note: Custom SSO image sets can be created and uploaded to the LoadMaster. For more information, refer to the Custom Authentication Form, Technical Note.

46. Enter a message in the **SSO Greeting Message** field, if required.

Note: The SSO Greeting Message can have up to 255 characters. The field accepts HTML code, so the users can insert their own an image can be entered if desired. The grave accent character (` ) is not supported. If this character is entered in the SSO Greeting Message, the character will not display in the output, for example **a`b`c** becomes **abc**.

47. Enter **/owa/logoff.owa** in the **Logoff String** text box.

Note: In a customized environment, if the OWA logoff string has been changed, the modified logoff string must be entered here.

48. If required, select the **Display Public/Private Option** which will show a public/private option on the login screen. When this option is enabled, the timeout value is determined based on which option the user selects. The timeout values are set in the manage SSO domain screen. For more information on the timeout fields, refer to the Create a Single Sign-On (SSO) Domain section. When the user selects **Private** their username is stored for that session.
49. If needed, enable the **Disable Password Form** check box. This may be needed when password validation is not required, for example if using RSA SecurID authentication in a singular fashion.
50. Select the relevant option in the **Use Session or Permanent Cookies** field.

Note: Permanent cookies should only be used when using single sign on with SharePoint or similar services.

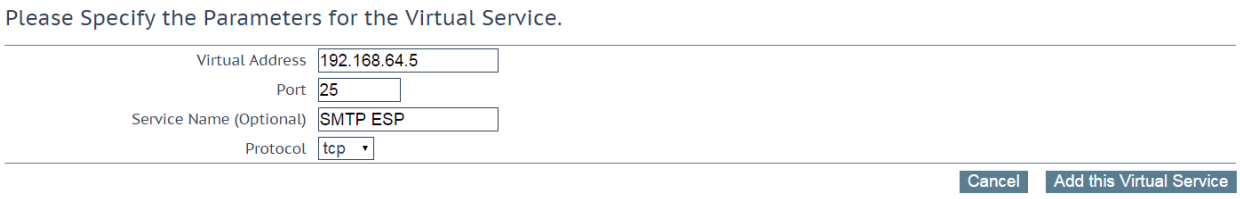
51. Specify the **User Password Change URL** and **User Password Change Dialog Message**, if needed.
52. Select **Basic Authentication** in the **Server Authentication Mode** drop-down menu.

You can check the status of the Virtual Service by selecting **Virtual Services > View/Modify Services** in the main menu. An **Up** status indicates that the latest health check passed successfully.

Configure a Simple Mail Transfer Protocol (SMTP) ESP Service

In an SMTP Virtual Service (with **25** as the Port), the ESP feature is available when the **Enable ESP** check box is selected, but there is a reduced set of options. To configure an SMTP ESP Service, follow the steps below:

1. In the menu on the left, click **Virtual Services** and select **View/Modify Services**.
2. Click the **Add New** button.



3. Enter the Virtual IP Address for the Virtual Service in the **Virtual Address** text box.

Note: This is the Virtual IP address of the Virtual Service. It must be unique and not in use by any other device on the network.

4. Enter **25** in the **Port** text box.
5. Enter a recognizable **Service Name**, for example **SMTP ESP**.
6. Click the **Add this Virtual Service** button.
7. Expand the **ESP Options** section.



8. Select **Enable ESP**.
9. Ensure the **Connection Logging** check box is selected.
10. Specify the domains permitted by this virtual service in the **Permitted Domains** field. For example, if the Virtual Service should receive SMTP traffic from john@progress.com, then **progress.com** must be specified in this field.
11. Click the **Set Permitted Domains** button.
12. Add any Real Servers, as needed, in the **Real Servers** section.

To check the status of the Virtual Service, select **Virtual Services > View/Modify Virtual Services**.

5

Client Certificate Authentication with No Server Side Authentication

In LoadMaster firmware version 7.2.53, support was added for **Client Certificate** client authentication with no server side authentication. This is useful in cases where ESP is simply needed for pre-authentication (which is possible using the certificate) and where other credentials are then passed on in the Real Sever (username/password/multi-factor authentication, and so on). To configure this, follow the steps below in the LoadMaster WUI:

1. Go to **Virtual Services > View/Modify Services**.
2. Click **Modify** on the relevant Virtual Service.
3. Expand the **SSL Properties** section and ensure that **SSL Acceleration** is **Enabled**.
4. Expand the **ESP Options** section and ensure that ESP is enabled.
5. Set the **Client Authentication Mode** to **Client Certificate** and the **Server Authentication Mode** to **None**.
6. Configure any other setting as needed.

6

RADIUS Two Factor and LDAP Authentication

As of LoadMaster firmware version 7.2.52, RADIUS two-factor and LDAP authentication is supported. To configure this, follow the steps below in the LoadMaster WUI:

1. Select **RADIUS and LDAP** as the **Authentication Protocol** when adding or modifying a client-side Single Sign On (SSO) domain in **Virtual Services > Manage SSO**. If the RADIUS server is configured to use two-factor authentication, the LoadMaster will detect this automatically and perform RADIUS two-factor authentication.
2. Set the LDAP Endpoint and RADIUS Server(s) for this SSO domain.

   Note: The LoadMaster uses the credentials specified for the LDAP Endpoint configuration to contact the RADIUS and LDAP servers and verify client SSO credentials. So, these administrative credentials must be configured on all the RADIUS and LDAP servers in the domain.

3. Select **Exchange** or **Blank** as the **SSO Image Set** in the **ESP Options** section of the Virtual Service **Modify** screen.
4. Set the other parameters as appropriate for your configuration.

7

PIV Smart Card Support

In LoadMaster firmware version 7.2.53, support was added for Personal Identity Verification (PIV) smart card authentication. PIV guidance is to match certificate fields to "altsecurityidentities" in the Active Directory (AD). Support has been added for both SSO and WUI authentication.

Select Certificate to User Mapping

The **Select Certificate to User Mapping** field appears in the **Virtual Services > Manage SSO > Modify** screen if the **Authentication Protocol** is set to **Certificates**.

The **Select Certificate to User Mapping** field appears in the **Certificates & Security > Remote Access > WUI Authorization Options** screen if the following settings are configured:

- **Session Management** must be enabled (**Certificates & Security > Admin WUI Access**) to see the **WUI Authorization Options** button.
- The **Admin Login Method** in **Certificates & Security > Remote Access** must be set to a **Client certificate** method.
- The **Pre-Auth Click Through Banner** must be set in **Certificates & Security > Admin WUI Access** before you can select a **Client certificate** method as the **Admin Login Method** in **Certificates & Security > Remote Access**.

The **Select Certificate to User Mapping** field has the following values:

- User Principal Name (default value)
- Subject

- Issuer and Subject
- Issuer and Serial Number

Some configuration caveats are below:

- After a certificate is revoked, the certificate fails authentication. However, sometimes it remains in the cache so to make it fail instantly ensure to use the **Flush OCSPD Cache** option in **System Configuration > System Administration > Logging Options > Debug Options**.
- If the LDAP query returns more than one match, the login fails.
- If the Authority Information Access (AIA) is present in the certificate, the LoadMaster attempts to connect with the provided AIA. If this does not work, it tries to connect with the local server.
- If the LoadMaster cannot get the status of the server configured in the certificate AIA, the LoadMaster does not fail back to the local server.
- If the certificate cannot be validated because the server is unavailable, there is an option in **Certificates & Security > OCSP Configuration** called **Allow Access on Server Failure** where you can decide if you want to pass the authentication or not. Enabling this check box treats an OCSP server connection failure or timeout as if the OCSP server has returned a valid response. That is, the client certificate is treated as valid.

8

Troubleshooting

When users connect to a Virtual Service using both ActiveSync and OWA from the same client IP address and using the same username, it will cause the OWA session to log out. This can be prevented by separating and distinguishing these two logins.

To do this, create two separate SSO domains - one for OWA and one for ActiveSync. Both SSO domains can have the same details except for the **Logon Format** - this needs to be set to **Principalname** in one SSO domain and **Username** in the other.

This should result in the two connections being separated and using different logon formats, that is, user@domain.com and domain\user, and therefore ActiveSync will not cause OWA to log out when using the same IP address.

9

Support for Additional Security Headers Added

Customers have reported that Single Sign On (SSO) configurations are failing security scans that require one or more of the following headers to be set on publicly available SSO pages:

- X-Frame-Options
- X-XSS-Protection
- X-Content-Type-Options
- HSTS Strict-Transport-Security

While it was possible in previous releases (before version 7.2.40) to set these headers manually on the Virtual Service, they were not being set on associated SSO login pages. In firmware version 7.2.40, the LoadMaster automatically sets these headers on all SSO pages and also on all WUI pages served by LoadMaster. As of version 7.2.41, all headers except Strict-Transport-Security (STS) are sent. STS headers are only sent if they are enabled in the Virtual Service (**Strict Transport Security Header** drop-down list in the **SSL Properties** section).

10

References

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

Web User Interface (WUI), Configuration Guide

Kerberos Constrained Delegation, Feature Description

RSA Two Factor Authentication, Feature Description

Custom Authentication Form, Technical Note

SSL Accelerated Services, Feature Description

ESP Technical Deep Dive

11

Appendix A - Expected Normalization Results (for LDAP Only) from Example Configurations

Login Format Setting	Realm	Input Username	Normalized User	Used for BIND	Result
Not Specified	example	test01	test01@EXAMPLE.COM	test01@EXAMPLE.COM	Success
Not Specified	example	test01@example.com	test01@example.com	test01@example.com	Success
Not Specified	example	test01@example	test01@example	test01@example	Success
Not Specified	example	example\test01	example\test01	example\test01	Success
Not Specified	example	example.com\test01	example.com\test01	example.com\test01	Fail

Login Format Setting	Realm	Input Username	Normalized User	Used for BIND	Result
Principal Name	example	test01	test01@example	test01@example	Success
Principal Name	example	test01@example.com	test01@example.com	test01@example.com	Success
Principal Name	example	test01@example	test01@example	test01@example	Success
Principal Name	example	example\test01	example\test01	test01@example	Success
Principal Name	example	example.com\test01	test01@example.com	test01@example	Success
Username	example	test01	example\test01	example\test01	Success
Username	example	test01@example.com	example\test01	example\test02	Success
Username	example	test01@example	example\test01	example\test01	Success
Username	example	example\test01	example\test01	example\test01	Success
Username	example	example.com\test01	example\test01	example\test01	Success
Not Specified	None	test01	test01@EXAMPLE.COM	test01@EXAMPLE.COM	Success
Not Specified	None	test01@example.com	test01@example.com	test01@example.com	Success
Not Specified	None	test01@example	test01@example	test01@example	Success
Not Specified	None	example\test01	example\test01	example\test01	Success

Login Format Setting	Realm	Input Username	Normalized User	Used for BIND	Result
Not Specified	None	example.com\test01	example.com\test01	example.com\test01	Fail
Principal Name	None	test01	test01@EXAMPLE.COM	test01@EXAMPLE.COM	Success
Principal Name	None	test01@example.com	test01@example.com	test01@example.com	Success
Principal Name	None	test01@example	test01@example	test01@example	Success
Principal Name	None	example\test01	example\test01	example\test01	Success
Principal Name	None	example.com\test01	test01@EXAMPLE.COM	test01@EXAMPLE.COM	Success
Username	None	test01	EXAMPLE.COM\test01	EXAMPLE.COM\test01	Fail
Username	None	test01@example.com	EXAMPLE.COM\test01	EXAMPLE.COM\test01	Fail
Username	None	test01@example	test01@example	test01@example	Success
Username	None	example\test01	example\test01	example\test01	Success
Username	None	example.com\test01	EXAMPLE.COM\test01	EXAMPLE.COM\test01	Fail
Username Only	None	test01	test01	N/A	Pass
Username Only	None	test01@example.com	test01	N/A	Pass
Username Only	None	test01@example	test01	N/A	Pass

Login Format Setting	Realm	Input Username	Normalized User	Used for BIND	Result
Username Only	None	example\test01	test01	N/A	Pass
Username Only	None	example.com\test01	test01	N/A	Pass