DoD Common Access Card Authentication

Feature Description

UPDATED: 19 March 2021

Copyright Notices

Table of Contents

1 Introduction

A Common Access Card (CAC) is a smart card used for identification of active-duty military personnel, selected reserve, US Department of Defence (DoD) civilian employees and eligible contractor personnel. In addition to providing physical access to buildings and protected areas, it also allows access to DoD computer networks and systems satisfying two-factor authentication, digital security and data encryption. It leverages a Public Key Infrastructure (PKI) Security Certificate to verify a cardholder's identity prior to allowing access to protected resources.

The Edge Security Pack (ESP) feature of the Kemp LoadMaster supports integration with DoD environments leveraging CAC authentication and Active Directory application infrastructures. The LoadMaster acts on behalf of clients presenting X.509 certificates using CAC and becomes the authenticated Kerberos client for services.

CAC authentication can also be used to authenticate access to the LoadMaster WUI. For more information on this, please refer to the **Using CAC Authentication for LoadMaster WUI Access** section.

The request for and presentation of the client certificate happens during initial SSL session establishment. There are two core elements to the process of a user gaining access to an application with CAC:

- Authentication – occurs during SSL session establishment and entails:
- Verifying the certificate date
- Verifying revocation status using Online Certificate Status Protocol (OCSP)
- Verifying the full chain to the Certificate Authority (CA)
- Authorization – occurs after SSL session establishment and the matching of the certificate Subject Alternative Name (SAN) against the User Principal Name (UPN) of the appropriate principal in Active Directory.

1.1 Document Purpose

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

1.2 Intended Audience

This document is intended to be read by anyone interested in finding out how to configure the LoadMaster to use DoD CAC authentication.

1.3 Related Firmware Version

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

1.4 Prerequisites

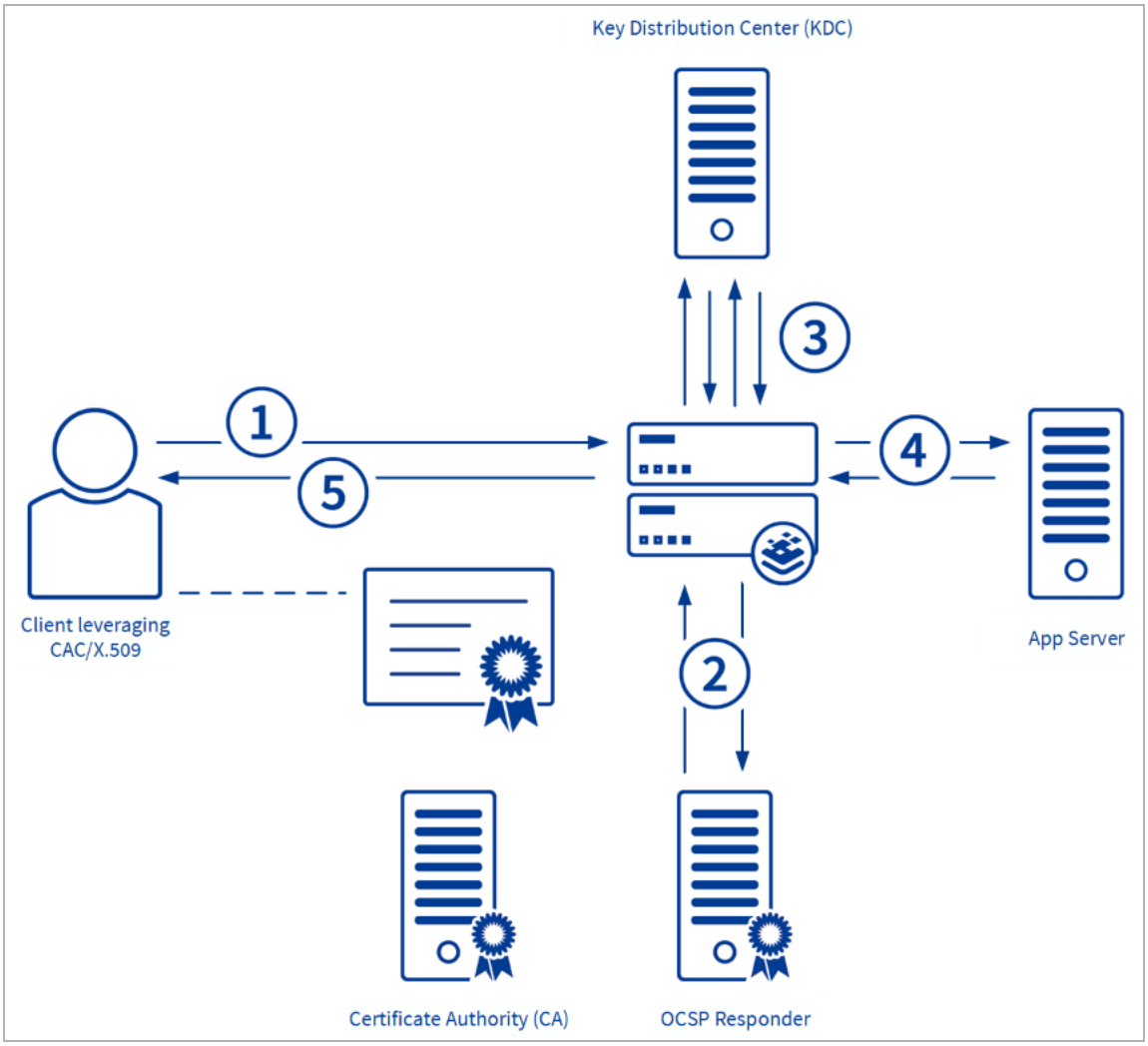
Before following the steps below to configure the LoadMaster, there are some prerequisites that need to be in place:

- The Active Directory settings must be configured correctly. If they are not configured correctly, constrained delegation will not work. For more information on what needs to be configured, please refer to the **Using CAC Authentication for LoadMaster WUI Access** section.
- A reverse DNS lookup zone needs to be set up which is able to resolve the IP address of the Real Server(s).

> There can be multiple entries for Real Servers in the DNS server. As a result of this, when the LoadMaster does a reverse lookup in order to get the FQDN, the result may not match the Service Principal Name (SPN). This may result in a mismatch between the SPN the LoadMaster generates and the one configured under the trusted user in the Active Directory. To mitigate this issue, it is possible to override the DNS server entries by adding hosts for local resolution in the LoadMaster (**System Configuration > Host & DNS Configuration**).

- The LDAP server needs to support LDAP over a secure transport, for example LDAPS or StartTLS.
- The appropriate certificates must have been issued for the LoadMaster.

2 DoD CAC Authentication



The above diagram illustrates the CAC/KCD logical authorization process:

1. A client attempts to access an ESP-protected service using CAC credentials.
2. The LoadMaster verifies that the credentials are still valid with a trusted OCSP responder.
3. After mapping the SAN which contains the client User Principal Name (UPN) in Active Directory, the LoadMaster obtains a service ticket for the user and obtains a service ticket for the application.

4. The LoadMaster forwards the user's service ticket to the desired service.

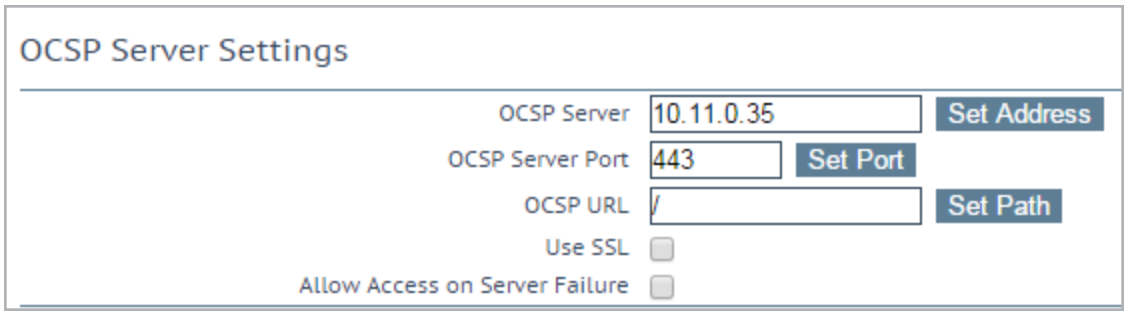
5. The LoadMaster passes the response to the client who gains access to the application/service.

2.1 Web User Interface (WUI) Options

There are a number of options in the LoadMaster WUI relating to DoD CAC authentication. These are described in the sections below.

2.1.1 OCSP Configuration

To get to the **OCSP Configuration** screen, in the main menu of the LoadMaster WUI, go to **Certificates & Security > OCSP Configuration**.



OCSP Server

The address of the OCSP server. This can either be in IP address or Fully Qualified Domain Name (FQDN) format.

OCSP Server Port

The port of the OCSP server.

OCSP URL

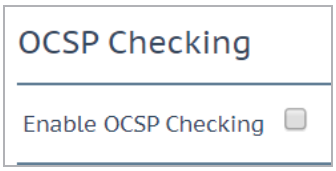
The URL to access on the OCSP server.

Use SSL

Select this to use SSL to connect to the OCSP server.

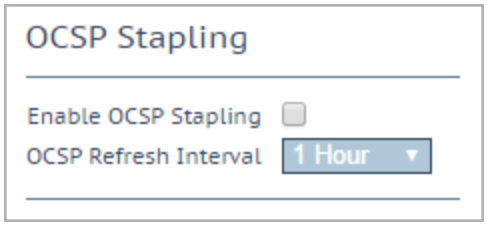
Allow Access on Server Failure

Treat an OCSP server connection failure or timeout as if the OCSP server had returned a valid response, that is, treat the client certificate as valid.



OCSP Checking

Select the **Enable OCSP Checking** check box to enable the LoadMaster to perform OCSP checks on certain outbound connections. This is disabled by default.



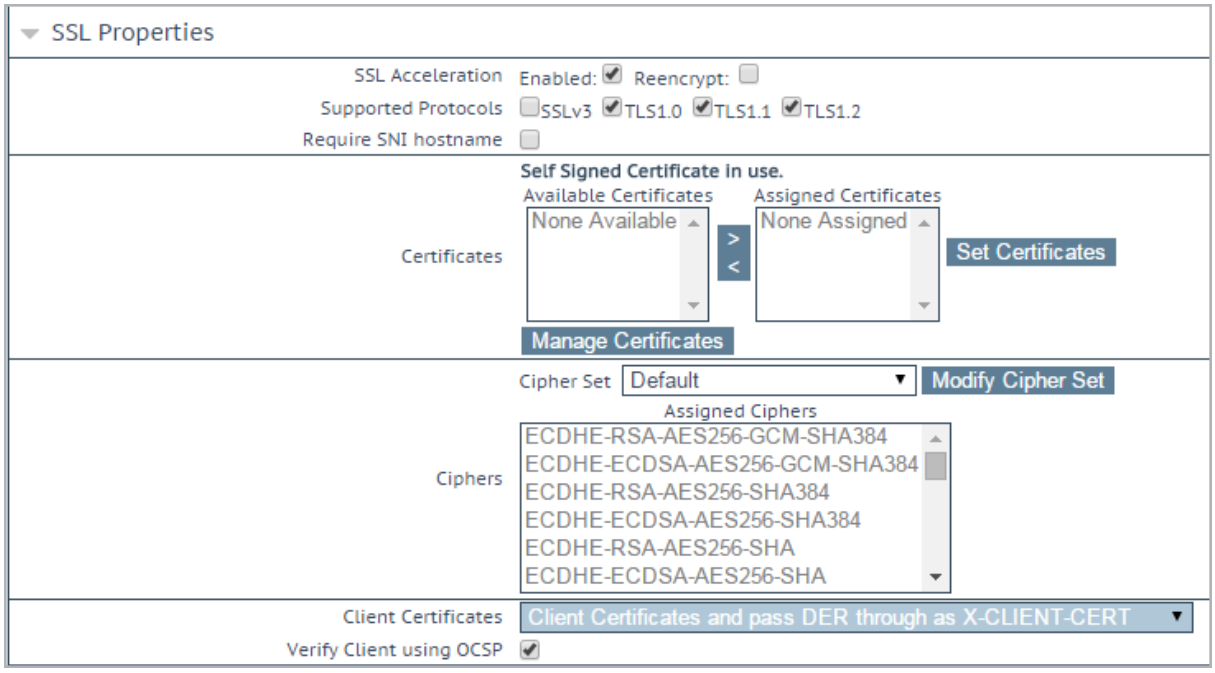
Enable OCSP Stapling

Select this check box to enable the LoadMaster to respond to OCSP stapling requests. If a client connects using SSL and asks for an OCSP response, this is returned. Only Virtual Service certificates are validated. The system holds a cache of OCSP responses that are sent back to the client. This cache is maintained by the OCSP daemon. When the OCSP daemon sends a request to the server, it uses the name specified in the certificate (in the **Authority Information Access** field). If it cannot resolve this name, then it uses the default OCSP server specified in the **OCSP Server** text box.

OCSP Refresh Interval

Specify how often the LoadMaster should refresh the OCSP stapling information. The OCSP daemon caches the entry for up to the amount of time specified here, after which it is refreshed. Valid values range from 1 hour (default) to 24 hours.

2.1.2 Verify Client using OCSP

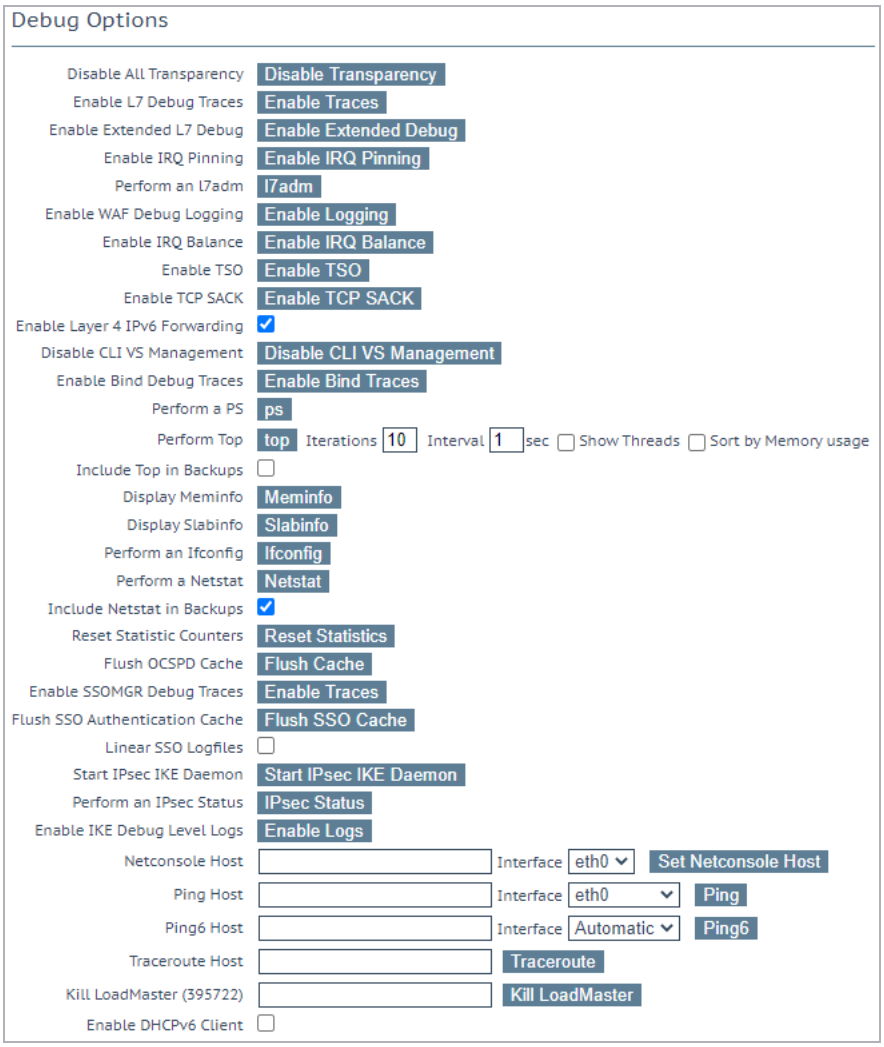


In the Virtual Service modify screen (**Virtual Services > View/Modify Services > Modify**) there is a check box in the **SSL Properties** section called **Verify Client using OCSP**. When this is enabled, the LoadMaster verifies that the client certificate is valid.

> If **Verify Client using OCSP** is enabled and the OCSP server settings have not been configured in the **OCSP Configuration** screen, the client cannot be verified and the connection will fail. There will not be a warning or error message on the WUI which indicates this so please ensure to check this if troubleshooting any problems.

2.1.3 Flush the OCSPD Cache

In the **Debug Options** screen (**System Configuration > Logging Options > System Log Files > Debug Options**) there is an option to flush the OCSPD cache. This option is intended to be used when troubleshooting or testing.



When using OCSP to verify client certificates, OCSPD caches the responses it gets from the OCSP server. The OCSPD log messages appear in the system messages log. This cache can be flushed by pressing the **Flush Cache** button. Flushing the OCSPD cache can be useful when testing, or when the Certificate Revocation List (CRL) has been updated.

2.2 Configure the LoadMaster

There are a number of areas that need to be configured for the LoadMaster to use DoD CAC authentication appropriately. Refer to the sections below for detailed configuration instructions.

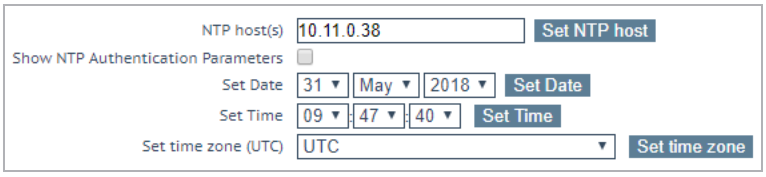
For information on what each of the WUI options mean, refer to the **Web User Interface (WUI) Options** section.

2.2.1 Connect to a Network Time Protocol (NTP) Host

If there is a time mismatch beyond a five-minute boundary between clients, intermediaries and servers, erroneous ticket invalidation will occur when KCD is in use. To avoid this problem, connect the LoadMaster to an NTP host server. The same host used by clients and servers in the infrastructure should be used by LoadMaster. An external NTP host server can be used if the LoadMaster can access it. However, if the LoadMaster is internal only – you will need to set up your own NTP server.

To configure the NTP settings on the LoadMaster, follow the steps below:

1. In the main menu, select **System Configuration > System Administration > Date/Time**.



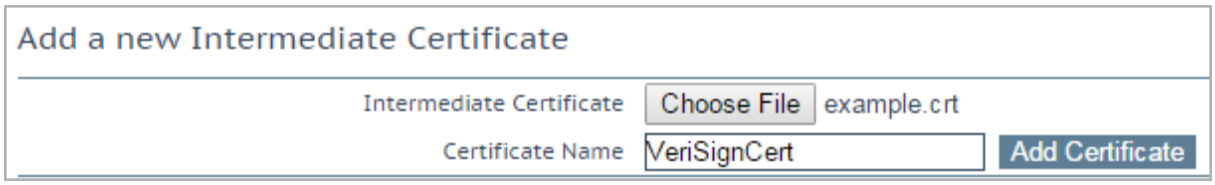
2. Enter the IP address of the **NTP host(s)** and click **Set NTP host**.
3. Select a time zone in the **Set time zone (UTC)** drop-down menu. Click **Set time zone**.

> The time zone needs to be manually set even when an NTP server is used.

2.2.2 Install the Root Certificate on the LoadMaster

First, the root certificate (which is needed for chaining certificates presented by clients) needs to be installed on the LoadMaster. To do this, follow the steps below in the LoadMaster WUI:

1. In the main menu, select **Certificates & Security > Intermediate Certs**.



2. Click **Choose File**.
3. Browse to and select the relevant certificate file.
4. Enter the **desired filename**.
5. Click **Add Certificate**.

6. Click **OK**.

2.2.3 Generate and Import a Client Certificate

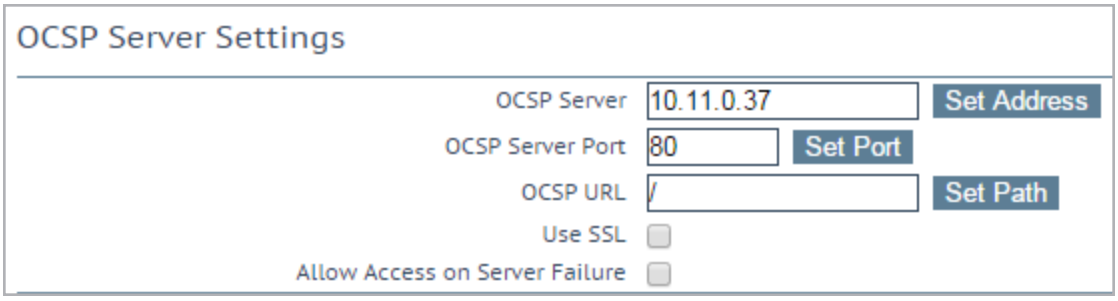
Generate a client certificate, for example with OpenSSL or Active Directory, which is signed by the root certificate. The client certificate must include a SubjectAltName (SAN) section with the email addresses of the clients. This is used to check if a particular user exists in the LDAP database. This client certificate must be imported in the clients' browser.

> Please import the certificate in the **Personal** tab of the browser certificate settings.

2.2.4 Configure the OCSP Options

To configure the OCSP options, follow the steps below in the LoadMaster WUI:

1. In the main menu, select **Certificates & Security > OCSP Configuration**.



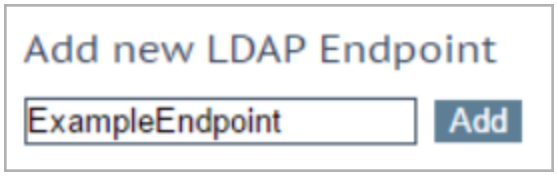
2. Enter the IP address or FQDN of the **OCSP Server** and click **Set Address**.
3. Enter the **OCSP Server Port** and click **Set Port**.
4. Enter the URL to access on the OCSP server in the **OCSP URL** text box and click **Set Path**.
5. Enable or disable the **Use SSL** option.
6. Enable or disable the **Allow Access on Server Failure** option.

> Kemp recommends leaving the **Use SSL** and **Allow Access on Server Failure** options disabled, but they can be enabled if needed.

2.2.5 Configure the LDAP Endpoint

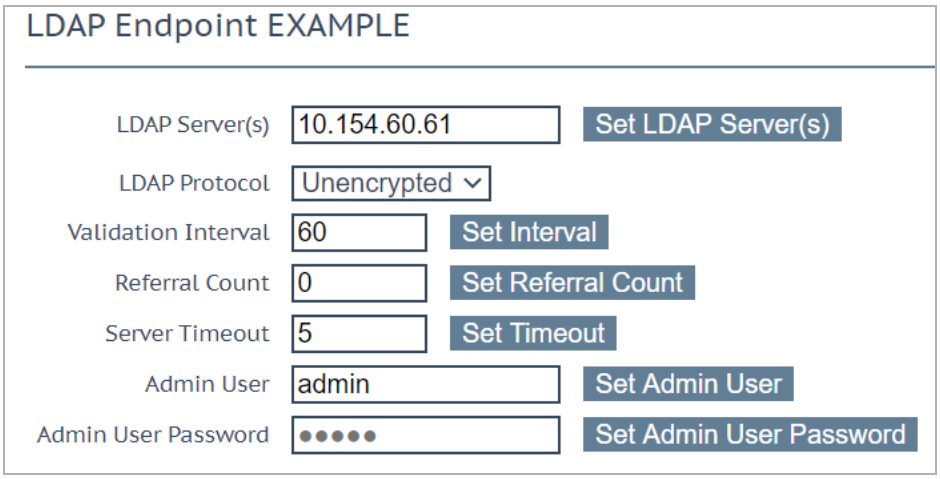
To add a new LDAP endpoint, follow the steps below:

1. Expand **Certificates & Security** and click **LDAP Configuration**.



2. Type a name for the endpoint and click **Add**.

> Spaces and special characters are not permitted in the LDAP endpoint name.



3. Type the IP address of the LDAP database or databases in the **LDAP Server(s)** text box and click **Set LDAP Server(s)**. Separate multiple entries by using a comma.

4. Select the relevant **LDAP Protocol** to communicate with the LDAP server.

> 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.

5. Type the **Validation Interval** and click **Set Interval**. This specifies how often the user is revalidated with the LDAP server.

6. Type the relevant username in the **Admin User** text box and click **Set Admin User**.

7. Type the password for the admin user and click **Set Admin User Password**. These admin credentials are used to check the LDAP server or servers.

2.2.6 Configure the SSO Domains

2.2.6.1 Configure the Inbound SSO Domain in the LoadMaster

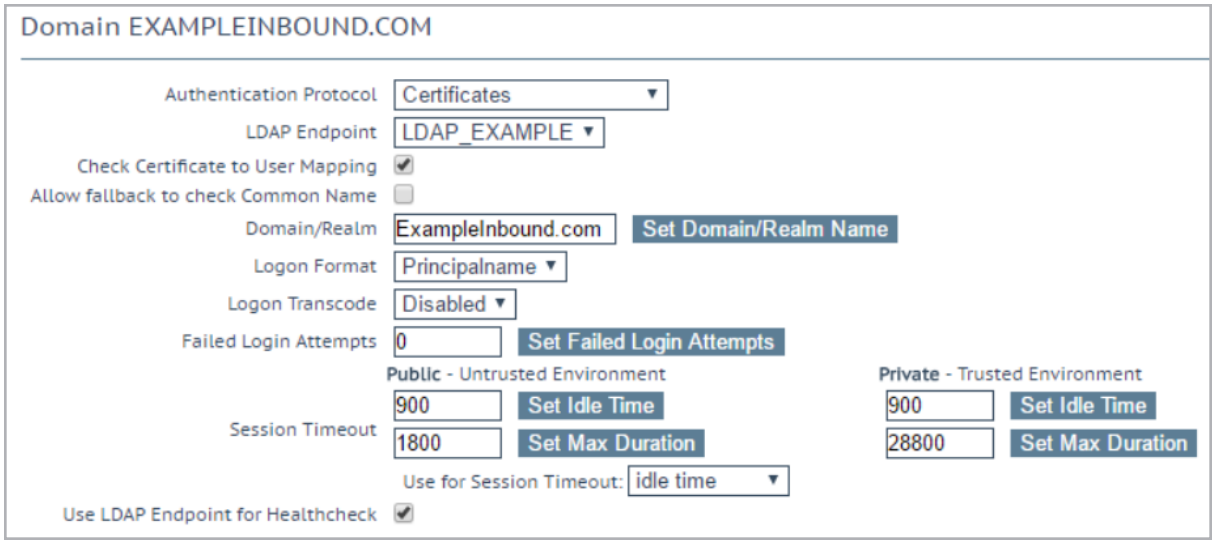
An inbound configuration SSO domain needs to be created in the LoadMaster. This should contain the IP address of the LDAP database as well as an administrator username and password. These login details are used to log in to the database and check if the user from the certificate does exist. If multiple domains are configured, sign-on can then be authenticated all at once. More information on this option can be found in the **ESP, Feature Description**.

To create and configure this SSO domain, follow the steps below:

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

2. In the **Client Side Single Sign On Configurations** section, enter the **Name** of the SSO domain.

3. Click **Add**.



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

5. Select the relevant **LDAP Endpoint** to use (as created in the **Configure the LDAP Endpoint** section).

6. Enable or disable the **Check Certificate to User Mapping** option.

> In LoadMaster firmware version 7.2.53, support for Personal Identity Verification (PIV) smart card authentication was added. As a result, the **Check Certificate to User Mapping** check box changed to a drop-down list called **Select Certificate to User Mapping** with a number of options. For further details, refer to the following article: PIV SSO Support.

7. Enable or disable the **Allow fallback to check Common Name** option.

> For more information regarding the **Check Certificate to User Mapping** option, refer to the **Check Certificate to User Mapping** section.

8. Enter the login domain to be used in the **Domain/Realm** text box.

> This is also used with the logon format to construct the normalized username, for example;
> **Principalname:** <username>@<domain>
> **Username:** <domain>\<username>
> If the **Domain/Realm** field is not set, the **Name** set when initially adding an SSO domain is used as the **Domain/Realm** name.

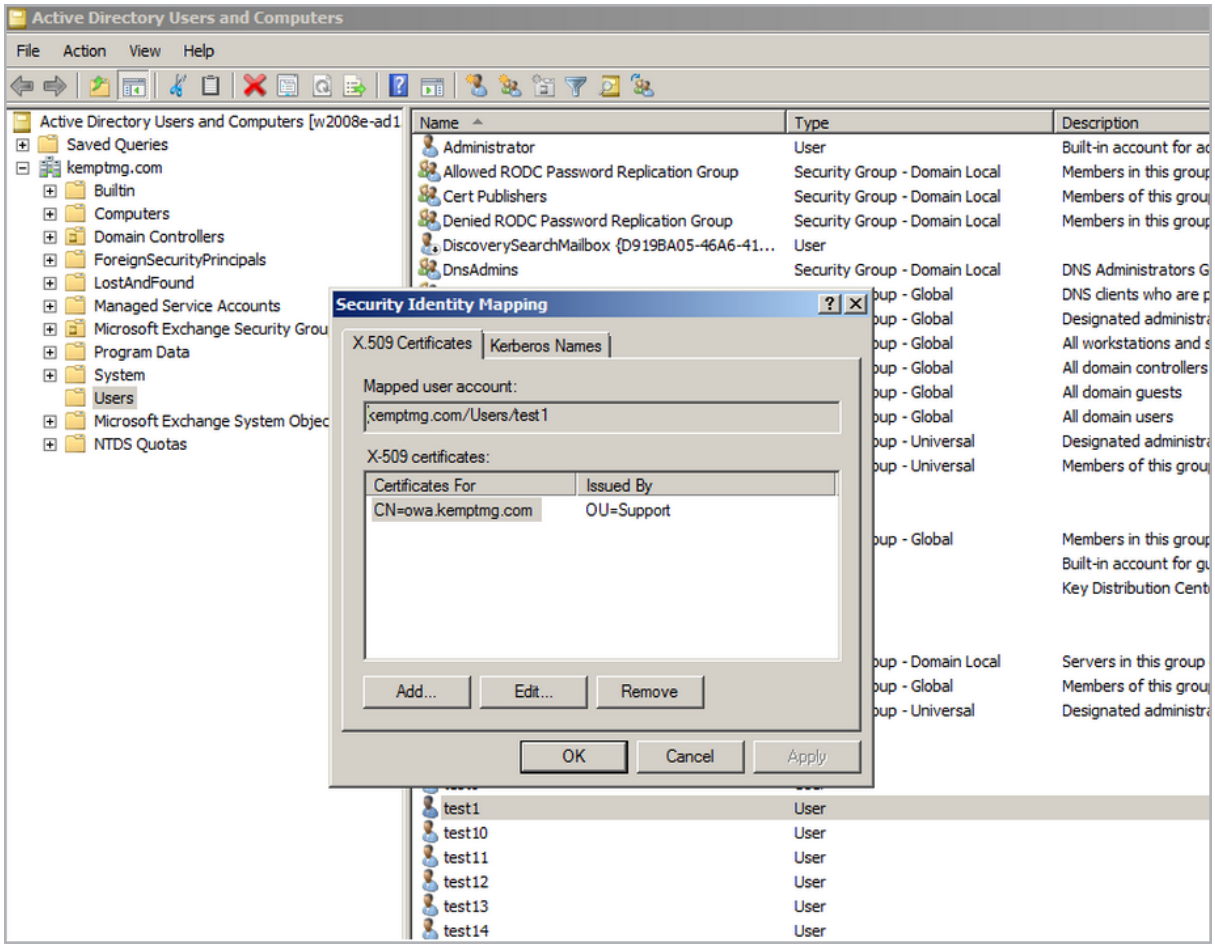
Check Certificate to User Mapping

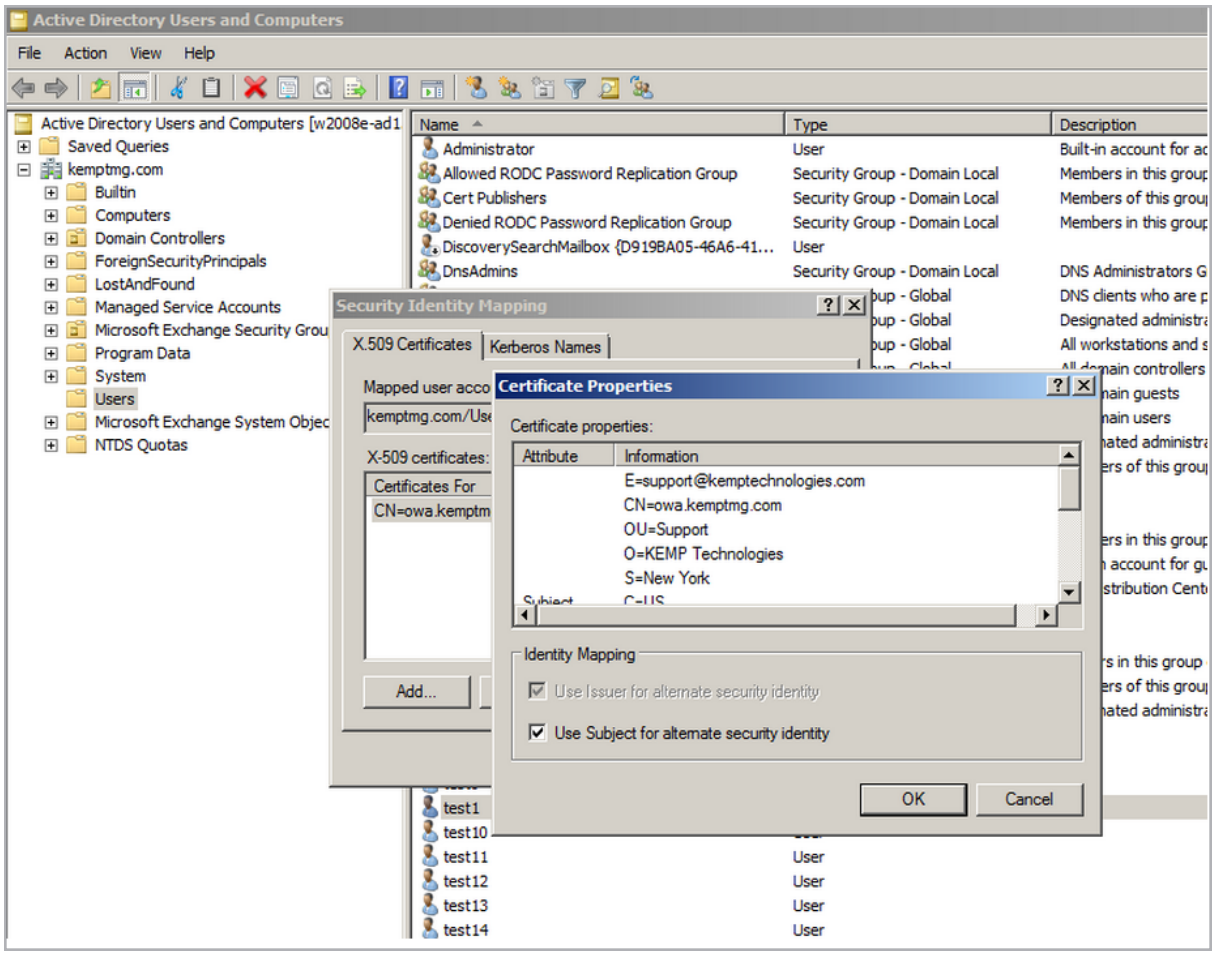
This section provides further information about the **Check Certificate to User Mapping** option. The **Check Certificate to User Mapping** option is only available when the **Authentication Protocol** is set to **Certificates**. When this option is enabled - in addition to checking the validity of the client certificate, the client certificate will also be checked against the altSecurityIdentities (ASI) attribute of the user on the Active Directory.

> In LoadMaster firmware version 7.2.53, support for Personal Identity Verification (PIV) smart card authentication was added. As a result, the **Check Certificate to User Mapping** check box changed to a drop-down list called **Select Certificate to User Mapping** with a number of options. For further details, refer to the following article: PIV Smart Card Support.

If the **Check Certificate to User Mapping** 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.

> The screenshots in this section were taken in Windows Server 2012 R2. They were correct at time of writing but they may change without our knowledge. Please consult the Microsoft documentation for the latest screenshots and steps.





The altSecurityAttribute can be set in the **Active Directory Users and Computers** (data.msc) console by using the **Name Mappings** task (see screenshots above). Both the **Issuer** and **Subject** are used for alternate security identity. Using the **Name Mappings** method will create an altSecurityIdentities entry on the form:

X509:<I>issuer data...<S>subject data...

There are other formats (created by other methods) but this is currently the only one supported by the LoadMaster.

> When changing the mapping in the Active Directory, the changes do not take effect immediately. To see the changes immediately, the LoadMaster SSO cache would need to be flushed or the user ticket would need to time out.

Flushing the SSO cache will flush all Single Sign-On (SSO) records, reset all authentication server statuses, reset the KCD domain (if relevant) and re-read the configuration. This has the effect of logging off all clients using Single Sign-On to connect to the LoadMaster.

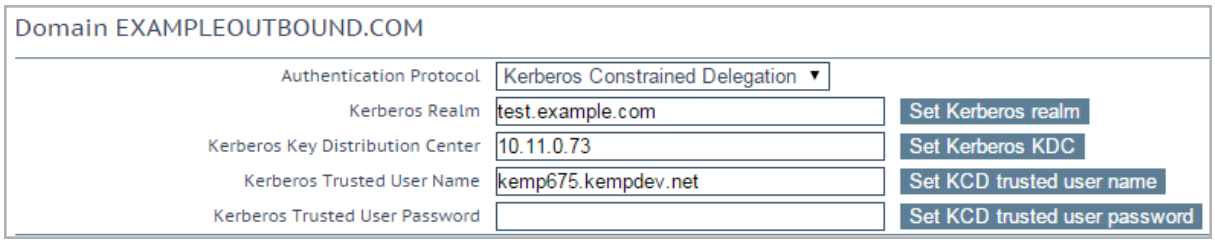
2.2.6.2 Configure the Outbound SSO Domain in the LoadMaster

> There are some guidelines to be aware of when creating a trusted user. For further details, refer to the **Create a LoadMaster Trusted User** section.

To configure the server (outbound) SSO domain, follow the steps below in the LoadMaster Web User Interface (WUI):

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

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



3. Select **Kerberos Constrained Delegation** as the **Authentication Protocol**.

4. Enter the **Kerberos Realm** address and click **Set Kerberos realm**. Click **OK**.

> The Kerberos realm should be a name (not an IP address), such as **kemptech.local**. If an IP address is specified, authentication will not work. This field only accepts one name. Double quotes are not allowed in this field.

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

> This field only accepts one **Key Distribution Center**.
> Double quotes are not allowed in this field.

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

> Refer to the **Create a LoadMaster Trusted User** section of this document for some key requirements relating to this trusted user account.

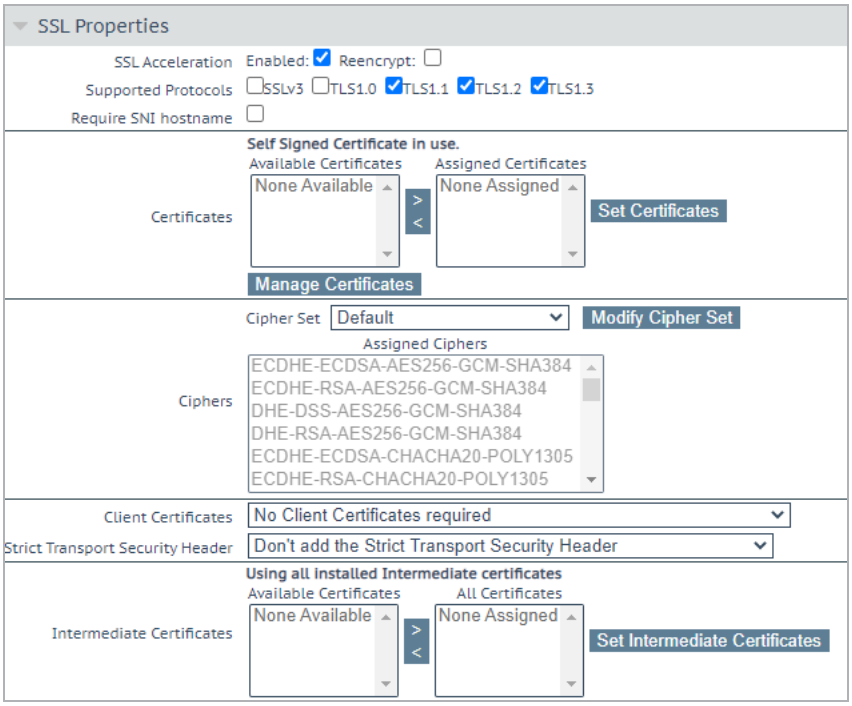
> Double and single quotes are not allowed in the **Kerberos Trusted User Name** field.

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

2.2.7 Configure the Virtual Service(s)

To configure the Virtual Service(s) to use DoD CAC authentication, follow the steps below:

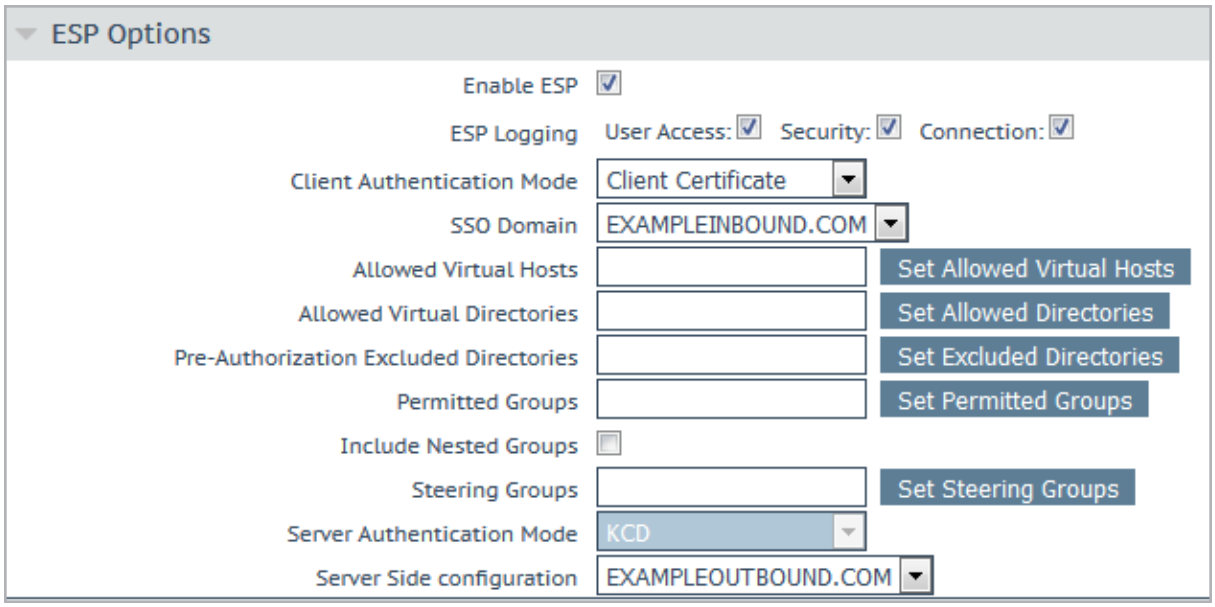
1. In the main menu, select **Virtual Services > View/Modify Services**.
2. Expand the **SSL Properties** section.



3. Select **Enabled**.

4. Click **OK**.

5. Expand the **ESP Options** section.



6. Select **Enable ESP**.

7. Select **Client Certificate** as the **Client Authentication** mode.

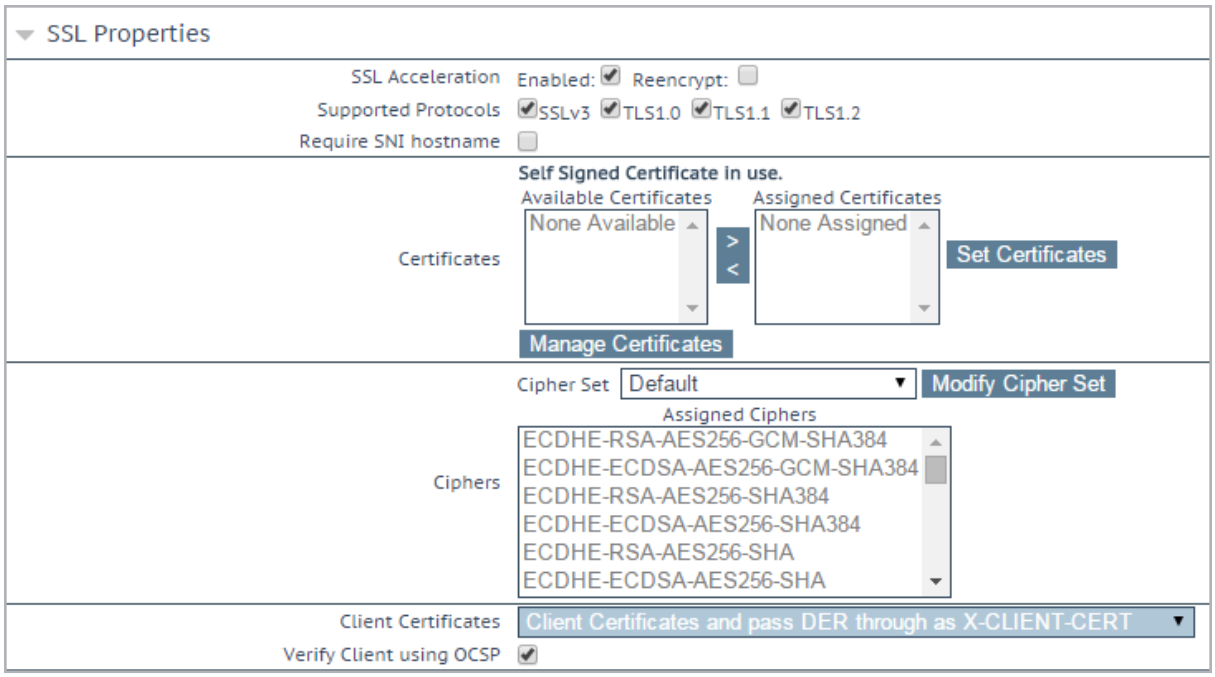
8. Select the inbound SSO domain which was configured in the **Configure the Inbound SSO Domain in the LoadMaster** section in the **SSO Domain** drop-down list.

> To allow the option to authenticate from multiple domains, alternative domains can be assigned at this point.

9. In the **Server Side configuration** drop-down list, select the outbound SSO domain which was created in the **Configure the Outbound SSO Domain in the LoadMaster** section.

10. Fill out any other details as needed. For more information on the general ESP options, refer to the **ESP, Feature Description**.

11. Expand the **SSL Properties** section.



12. Enable the **Verify Client using OCSP** option.

> If **Verify Client using OCSP** is enabled and the OCSP server settings have not been configured in the **OCSP Configuration** screen, the client cannot be verified and the connection will fail.

13. Fill out any other details as needed.

14. Add any Real Servers as needed.

> When using client certificates, you cannot have SubVSs when setting up an Exchange workload.

3 Using CAC Authentication for LoadMaster WUI Access

In addition to using CAC as the authentication protocol when using ESP, CAC authentication can also be used to authenticate user access to the LoadMaster administrative WUI. To configure this, follow the steps in the sections below.

3.1 Complete the CAC Infrastructure Configuration

Before enabling CAC authentication for LoadMaster WUI access, please ensure that the CAC infrastructure configuration has been completed. If it has not been completed, you may not be able to gain access to the LoadMaster WUI after enabling CAC authentication for WUI access. For further information on completing the CAC infrastructure configuration, refer to the other sections in this document and also the third party CAC documentation.

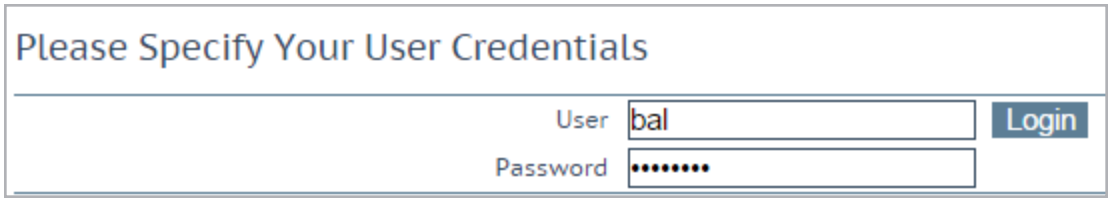
3.2 Upload the Certificate to be Validated to the LoadMaster

Ensure to upload the certificate to be validated to the **Intermediate Certs** section of the LoadMaster WUI. For step-by-step instructions, refer to the **Install the Root Certificate on the LoadMaster** section.

3.3 Enable Session Management

Session management needs to be enabled in the LoadMaster WUI in order to enable CAC authentication. To enable Session Management, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **System Configuration > Miscellaneous Options > WUI Settings**.
2. Tick the **Enable Session Management** check box.



3. Log in to the WUI.

4. If required, basic authentication can also be enabled.

For further information on WUI Session Management, refer to the **Web User Interface (WUI), Configuration Guide**.

3.4 Optionally Enable the OCSP Check

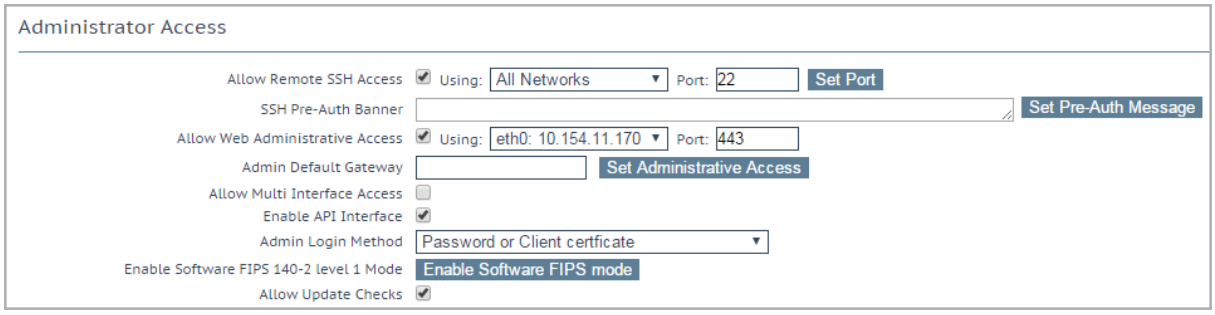
If desired, an OCSP check can also be enabled - but this is optional. For further information, refer to the OCSP sections in this document.

3.5 Enable CAC Authentication for LoadMaster WUI Access

Certificate authentication must be configured correctly before enabling WUI CAC support.

After session management has been enabled, CAC authentication can also be enabled for LoadMaster WUI access. To enable this, follow the steps below:

1. In the main menu of the LoadMaster WUI, go to **Certificates & Security > Remote Access**.



2. Select the relevant **Admin Login Method**.

The following login methods are available:

- **Password Only Access (default):** This option provides access using the username and password only – there is no access using client certificates.
- **Password or Client certificate:** The user can log in using either the username/password or using a valid client certificate. If a valid client certificate is in place, the username and password is not required.
  The client is asked for a certificate. If a client certificate is supplied, the LoadMaster will

check for a match. The LoadMaster checks if the certificate is a match with one of the local certificates, or checks if the Subject Alternative Name (SAN) or Common Name (CN) of the certificate is a match. The SAN is used in preference to the CN when performing a match. If there is a match, the user is allowed access to the LoadMaster. This works both using the API and user interface.
An invalid certificate will not allow access.
If no client certificate is supplied, the LoadMaster will expect that a username and password is supplied (for the API) or will ask the user to enter a password using the standard WUI login page.

- **Client certificate required:** Access is only allowed with the use of a client certificate. It is not possible to log in using the username and password. SSH access is not affected by this (only the **bal** user can log in using SSH).
- **Client certificate required (Verify via OCSP):** This is the same as the **Client certificate required** option, but the client certificate is verified using an OCSP service. The OCSP Server Settings must be configured in order for this to work. For further information on the OCSP Server Settings, refer to the **Configure the OCSP Options** section.

> In LoadMaster firmware version 7.2.53 and above, the OCSP server settings do not need to be configured in the LoadMaster if the certificate has an Authority Information Access (AIA) extension. For further details on the functionality introduced in 7.2.53, refer to the following article: PIV Smart Card Support.

Some points to note regarding the client certificate methods are below:

- The **bal** user does not have a client certificate. Therefore, it is not possible to log into the LoadMaster as **bal** using the **Client certificate required** methods. However, a non-**bal** user can be created and granted **All Permissions**. This will allow the same functionality as the **bal** user.
- There is no log out option for users that are logged in to the WUI using client certificates, as it is not possible to log out (if the user did log out the next access would automatically log them back in again). The session is terminated when the page is closed, or when the browser is restarted.

> In LoadMaster firmware version 7.2.53, support for PIV smart card authentication was added. As a result, a new **Select Certificate to User Mapping** drop-down list was added to the **Certificates & Security > Remote Access > WUI Authorization**

Options screen. For further details, refer to the following article: PIV Smart Card Support.

3.6 Logging in to the LoadMaster WUI with CAC Authentication

After enabling CAC WUI authentication, you are logged out of the LoadMaster WUI. Please close the web browser and open it again. Then, attempt to log in with a valid certificate.

The WUI authentication login is based on CAC X.509 certificates. Authentication systems vary depending on the type of system, such as Active Directory or another access control list.

When logging into the LoadMaster WUI with CAC and LDAP, the username needs to be fully qualified, that is, it needs to be the UserPrincipalname or <Domain>\<Username>.

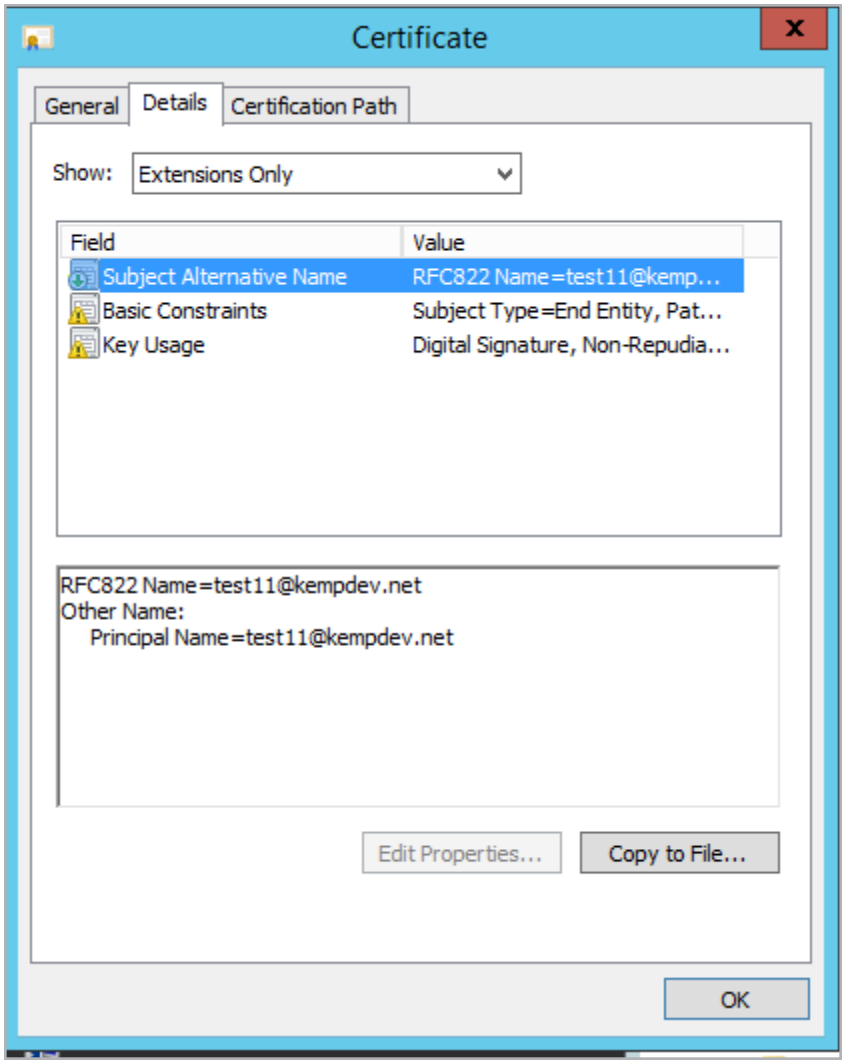
4 Appendix A: Configure the Active Directory Settings

There are certain Active Directory settings that need to be configured correctly for CAC authentication to work with the LoadMaster. Follow the steps below to configure these settings. If this account is not set up correctly, CAC authentication will not work.

The steps below are functionally equivalent for Windows Server 2008 and Windows Server 2012 R2. For more information, please refer to the Microsoft documentation.

> The screenshots in this section were taken in Windows Server 2012 R2. They were correct at time of writing but they may change without our knowledge. Please consult the Microsoft documentation for the latest screenshots and steps.

4.1 Add a Certificate to the Active Directory for TLS/LDAPS

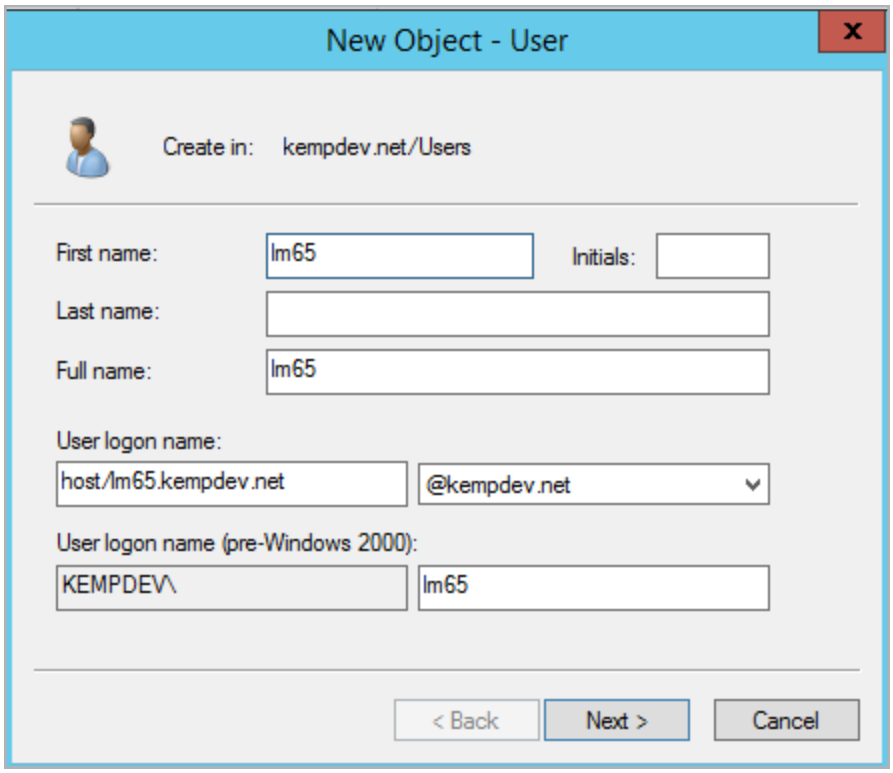


A certificate needs to be added to the Active Directory for Transport Layer Security (TLS)/Lightweight Directory Access Protocol over SSL (LDAPS).

4.2 Create a LoadMaster Trusted User

A LoadMaster trusted user must be created in the Windows domain (Active Directory). This trusted administrator user account is used to get tickets on behalf of users and services when a password is not provided. The Active Directory account for the trusted user is a user account, but it represents the LoadMaster.

Some guidelines regarding configuring the trusted user are listed below:



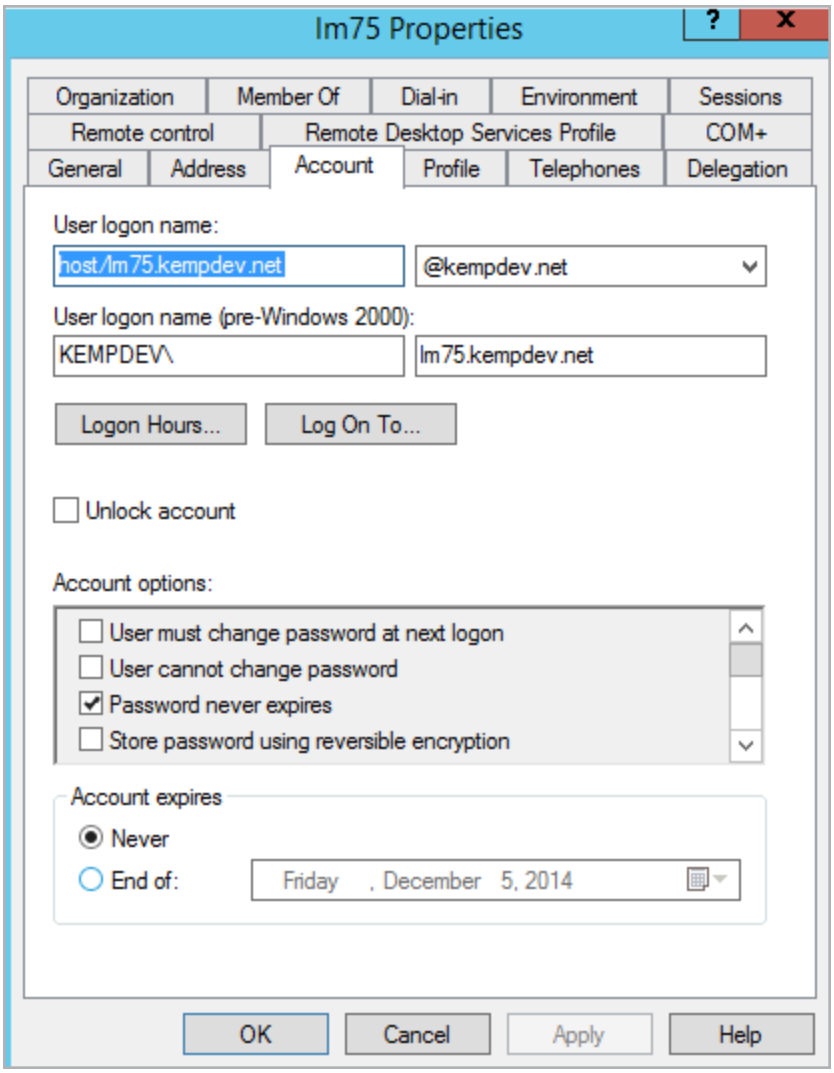
- The User Principal Name (UPN) (**User logon name**) must be like a Service Principal Name (SPN), for example **host/<FQDN>.UPNSuffix**, like the example in the screenshot above; **host/lm65.kempdev.net**

> The default UPN suffix must be used.

- The **pre-Windows 2000** user logon name has to be the name part of the FQDN that is part of the UPN above, for example **KempDEV**

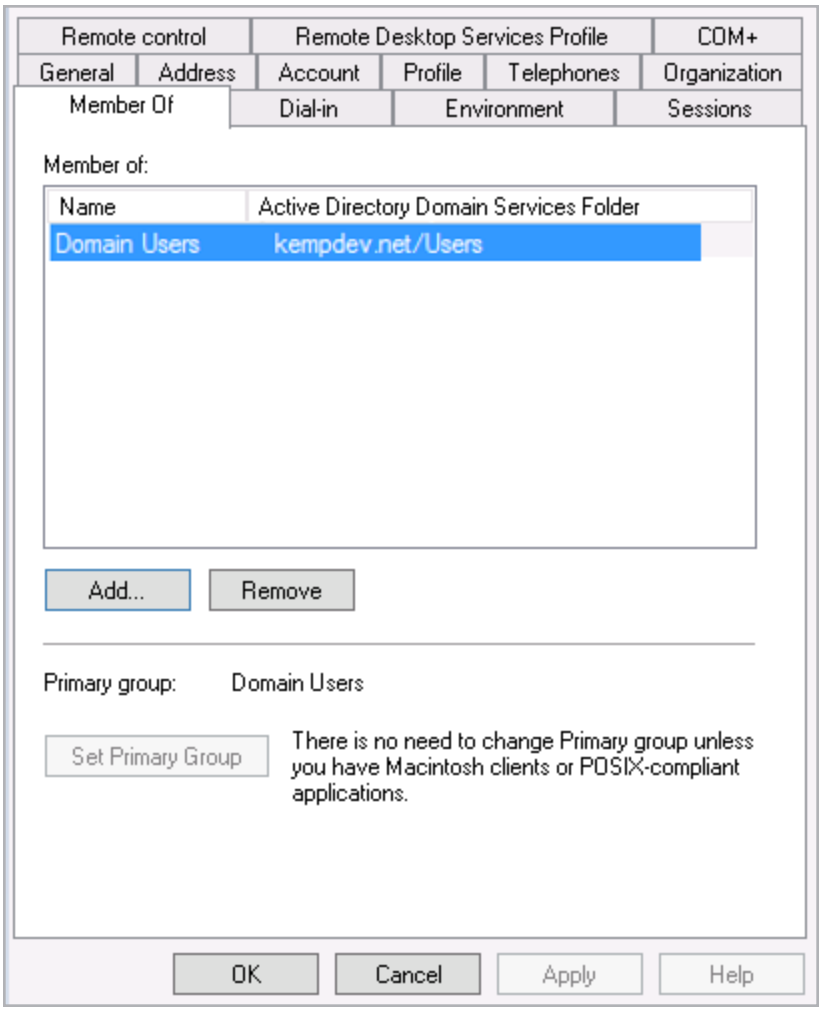
> A DNS entry representing the FQDN must be created, ideally with a PTR record for reverse lookup.

> In the LoadMaster, the **Kerberos Trusted User Name** is set to the FQDN name above, which should be the host name of the LoadMaster.



To open the user **Properties** screen, right-click the user and click **Properties**.

- The password should be set to never expire
- The user must have permissions to perform protocol transition. Refer to the **Configure Delegation for the User Entry** section for further information on this.



- The user must be a member of the relevant domain

In the example, the items are mapped as follows:

Item	Mapping	Additional Information
Username	lm75	
Domain	kemptech.net	
Kerberos Realm	kemptech.net	
Default UPN-suffix	kemptech.net	
LoadMaster FQDN	lm75.kemptech.net	DNS entry
FQDN name/LoadMaster	lm75	

Item	Mapping	Additional Information
hostname		
LoadMaster SPN	host/lm75.kemptech.net	
UPN of trusted user	host/lm75.kemptech.net	User logon name
Trusted user logon name	kempdev/lm75	User logon name (pre-Windows 2000)
Kerberos Trusted User Name	Lm75	

4.3 Associate an SPN with the User Entry

Execute the **ktpass.exe** file in the command prompt to associate a Service Principal Name (SPN) with the user entry, for example:

Example Syntax

ktpass.exe /princ host/<LoadMasterSPN>@<Domain> /ptype KRB5_NT_PRINCIPAL /mapuser <Domain>\<TrustedUserLogonName> /mapop set /setupn /crypto all

Example Command

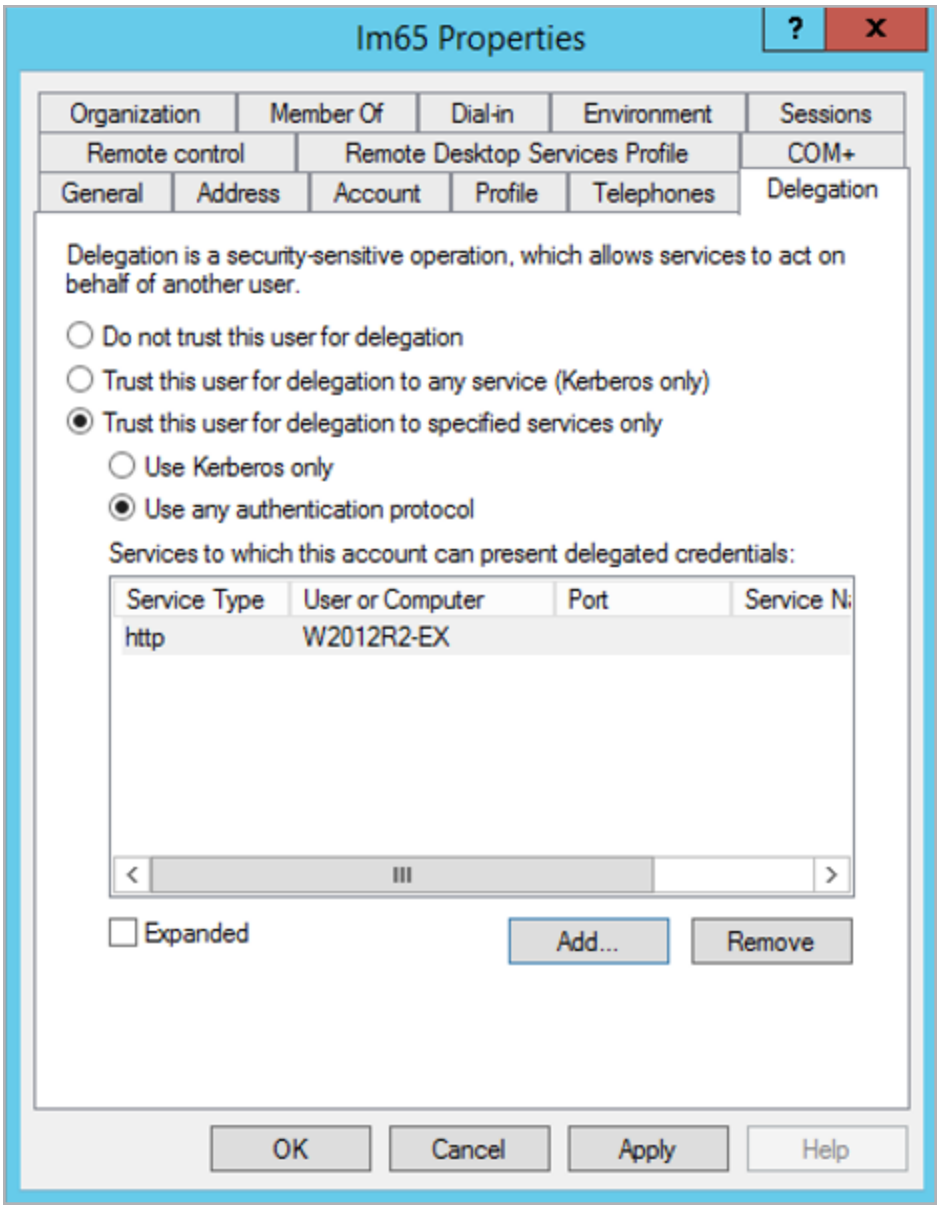
ktpass.exe /princ host/lm60.esptest.local@ESPTEST.local /ptype KRB5_NT_PRINCIPAL /mapuser ESPTEST\lm60.esptest.local /mapop set /setupn /crypto all

> The **ktpass.exe** file is a Microsoft command-line utility and is present on any Windows Server installation.

When this has been completed, the user properties window will have the **Delegation** tab.

4.4 Configure Delegation for the User Entry

Some guidelines relating to the delegation settings for the trusted user are provided below:



- The LoadMaster trusted user account must have delegation enabled (the ability to request a ticket on behalf of a user logging in) and be set to **Use any authentication protocol**

Delegation is not enabled by default when a user is created.

- In constrained delegation mode, the service(s) that need to be available must be selected. To do this, click the **Add** button.

Constrained delegation can be thought of as a white list type of security authenticating. Adding a service here is really adding it to the white list.

References

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

Kerberos Constrained Delegation, Feature Description

Web User Interface (WUI), Configuration Guide

ESP, Feature Description

Last Updated Date

This document was last updated on 19 March 2021.

