



PowerShell

Interface Description

VERSION: 17.0

UPDATED: June 2017

Copyright Notices

Copyright © 2002-2017 KEMP Technologies, Inc. All rights reserved. KEMP Technologies and the KEMP Technologies logo are registered trademarks of KEMP Technologies, Inc.

KEMP Technologies, Inc. reserves all ownership rights for the LoadMaster and KEMP 360 product line including software and documentation.

Used, under license, U.S. Patent Nos. 6,473,802, 6,374,300, 8,392,563, 8,103,770, 7,831,712, 7,606,912, 7,346,695, 7,287,084 and 6,970,933

Table of Contents

1 Introduction	5
1.1 Document Purpose	5
1.2 Intended Audience	5
1.3 Prerequisites	5
2 Windows PowerShell	6
2.1 Installing the KEMP PowerShell Module	6
2.2 Importing the Certificate	7
2.3 Using the Get-Help Command	8
2.4 Authenticating to the LoadMaster	8
2.4.1 Configure Certificate-Based Authentication	9
2.4.1.1 Enable Session Management	9
2.4.1.2 Create a User (If Needed)	9
2.4.1.3 Enable Client Certificate Authentication on the LoadMaster	10
2.4.1.4 Generate and Download the Client Certificate	11
2.4.1.5 Create the PFX File	13
2.4.1.6 Import the PFX File into the Microsoft Management Console (if using Windows)	13
2.4.1.7 Specify the Certificate Details in the API	22
2.5 Object Structure	23
2.5.1 Errors	24
2.6 Initially Configure a LoadMaster Using PowerShell API Commands	25
2.6.1 Licensing Cloud LoadMasters	26
2.6.2 Initial Configuration Commands List	26
2.6.3 Accept the EULAs	27
2.6.4 Retrieve the Available Licenses (optional)	28
2.6.4.1 Example without Specifying an Order ID	29

2.6.4.2 Example with a Valid Order ID	30
2.6.4.3 Example with an Invalid (Undefined) KEMP ID	31
2.6.4.4 Retrieve License Types when using Activation Server Functionality	31
2.6.5 License the LoadMaster	31
2.6.5.1 Online Licensing Example	32
2.6.5.2 Offline Licensing Example	32
2.6.6 Set the Initial Password for the LoadMaster	33
2.6.7 Retrieve the License Details (optional)	33
2.6.8 Update a LoadMaster License	33
2.7 Code Snippet Examples	34
2.7.1 Online Licensing	34
2.7.2 Initialize the LoadMaster Connection Parameters	35
2.7.3 Enable the API	35
2.8 Known Issues with Beta PowerShell Wrapper	36
References	37
Document History	38

1 Introduction

KEMP Technologies products optimize web and application infrastructure as defined by high-availability, high-performance, flexible scalability, security and ease of management. They minimize the total cost-of-ownership for web infrastructure, while enabling flexible and comprehensive deployment options.

1.1 Document Purpose

This document provides some information on how to import the KEMP PowerShell module, how to enable the API interface on the LoadMaster and how to use the **Get-Help** command to retrieve help text relating to the various commands and parameters that can be used.

1.2 Intended Audience

This document is intended to help anyone who wishes to configure or interface to the KEMP LoadMaster using Windows PowerShell commands.

1.3 Prerequisites

For the PowerShell API to work with the LoadMaster, the following prerequisites must be met:

- Either TLS1.1 or TLS1.2 must be enabled in the LoadMaster WUI Settings. These are enabled by default. SSLv3 and TLS1.0 are unsupported with the PowerShell API. To set the **Supported TLS Protocols**, go to **Certificates & Security > Admin WUI Access** and select the check boxes provided.
- The API interface must be enabled on the LoadMaster. To enable it – go to **Certificates & Security > Remote Access** and tick the **Enable API Interface** check box.
- PowerShell version 5 or above is recommended.

2 Windows PowerShell

Companies are focusing on the internal changes necessary to enable their organization to scale efficiently in line with growth. Working more quickly and efficiently means managing and protecting a greater number of devices, applications, systems and identities. IT departments are using automation frameworks to meet that challenge.

PowerShell is an automation platform and scripting language for Windows and Windows Server. KEMP have had a PowerShell module since 2013. It simplifies the management of systems and is key to enabling IT departments to adopt automation in dynamic environments. In PowerShell, administrative tasks are generally performed by cmdlets, which are specialized .NET classes implementing particular operations. KEMP's PowerShell cmdlet improvements in our 7.2.39 release, are an enhancement for companies on an automation path, especially for automating your KEMP LoadMaster family of products.

2.1 Installing the KEMP PowerShell Module

Download the KEMP PowerShell module from the KEMP Documentation page, <https://kemptechnologies.com/loadmaster-documentation/>. Unzip the files.

The module contains the following files within the `Kemp.LoadBalancer.Powershell` folder:

- `Kemp.LoadBalancer.Powershell.psd1`
- `Kemp.LoadBalancer.Powershell.psm1`
- `deprecated.psm1`
- `Kemp.LoadBalancer.Powershell-Help.xml`

Before installing the KEMP PowerShell module, please ensure that you have Microsoft PowerShell version 3.0 installed.

Copy the **`Kemp.LoadBalancer.Powershell`** folder to the relevant folder.

Install the module in a folder that is available in `PSModulePath` (`$Env:PSModulePath`).

If `PSModulePath` does not contain the module folder value, add the module path to the in `PSModulePath` environment variable. The module path can be for the current user only or for all users. Recommended values are:

- `$home\Documents\WindowsPowerShell\Modules` for the current User
- `$Env:ProgramFiles\WindowsPowerShell\Modules` for All Users

For example, install the KEMP PowerShell module for the current user only:

```
# Save the current value of PSModulePath
$mpath = [Environment]::GetEnvironmentVariable("PSModulePath")
# Add the new path to the $mpath variable
```

```
$ mpath +=
";$home\Documents\WindowsPowerShell\Modules\Kemp.LoadBalancer.PowerShell"
# Add the paths in $currValue to the PSModulePath value.
[Environment]::SetEnvironmentVariable("PSModulePath", $currValue)
```

Import the module to start using it:

```
Import-Module Kemp.LoadBalancer.PowerShell
Get-Module Kemp.LoadBalancer.PowerShell
```

ModuleType	Version	Name	ExportedCommands
Script	7.2.39.0	Kemp.LoadBalancer.PowerShell	{Add-BondedInterface, A...

For the PowerShell commands to work, the API interface must be enabled on the LoadMaster. To enable it using the Web User Interface (WUI), go to **Certificates & Security > Remote Access** and select **Enable API Interface**.

You can test the connection to the load balancer by using the **Test-LmServerConnection** command, for example:

```
Test-LmServerConnection -ComputerName 10.11.0.60 -Port 443 -Verbose
```

To retrieve a list of available commands, run the following command:

```
Get-Command -Module Kemp.LoadBalancer.PowerShell
```

To retrieve the build number of the PowerShell module, run the following command:

```
(Get-Module Kemp.LoadBalancer.PowerShell).ReleaseNotes
```

This command only works on PowerShell version 5 and above.

2.2 Importing the Certificate

As of LoadMaster version 7.2.36 the PowerShell module is signed. Depending on your execution policy, you may need to import the KEMP PowerShell certificate to allow execution. When you download the module from the KEMP website to obtain the following files:

- Kemp.LoadBalancer.PowerShell-Help.xml
- Kemp.LoadBalancer.PowerShell.psd1
- Kemp.LoadBalancer.PowerShell.psm1
- kemp-cert.cer
- symantec-ca.cer
- symantec-int.cer

Perform the following steps:

1. Double-click the `symantec-ca.cer` file and install it in Trusted Root Certification Authorities.
2. Double the `symantec-int.cer` file and install it in Trusted Root Certification Authorities.
3. Confirm the installation by clicking **OK** when requested.
4. Double click the **kemp-cert.cer** and install it in **Trusted Publishers**.
5. Set the execution policy to **AllSigned**. For example, `Set-ExecutionPolicy -ExecutionPolicy AllSigned -Scope CurrentUser`.

Alternatively, you could adjust your execution policy to one that is less restrictive.

2.3 Using the Get-Help Command

To retrieve help text for a particular command, run the **Get-Help** command, followed by a command name, for example:

Get-Help Set-VirtualService

Different parameters can be specified to retrieve more detailed help text:

- **-Detailed**: Provides further detailed help, including a list of parameters and their descriptions.
- **-Examples**: Provides an example command and example output.
- **-Full**: Provides all of the help text for the specified command.

For example:

Get-Help Set-VirtualService -Full

2.4 Authenticating to the LoadMaster

To run PowerShell API commands, you need to establish authentication with the LoadMaster. There are two ways to establish authentication:

- Using credentials; a LoadMaster username (**Credential**) and password
- Using certificate-based authentication

Whichever option you use, you can either specify the parameters when running individual commands, or using the **Initialize-LmConnectionParameters** command.

You can also globally set the KEMP LoadMaster IP address that you are directing the commands to by using the **Initialize-Lm** command, for example:

Initialize-Lm -Address 10.11.0.60 -LBPort 443 -Credential bal -Verbose

You can either enter a username for the load balancer or provide a `PSCredential` object. When you enter a username, a prompt appears asking for the password. You can override the globally-provided `LoadBalancer` address and `User Name` on each individual command by using the **LoadBalancer** or **Credential** parameter within the command.

Similarly, you can specify the details to use certificate-based authentication using the **Initialize-LmConnectionParameters** command. For further information on the various steps involved to configure certificate-based authentication, refer to the below section.

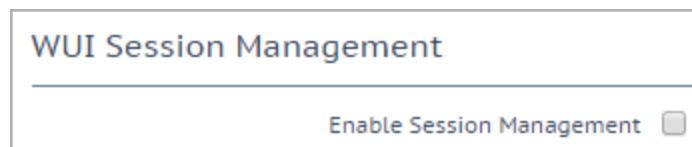
2.4.1 Configure Certificate-Based Authentication

Follow the steps in the sections below to configure certificate-based authentication.

2.4.1.1 Enable Session Management

You must enable **Session Management** before you can enable client certificate authentication. To enable Session Management, follow the steps below:

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



2. Select the **Enable Session Management** check box.

Once this check box is selected, the user is required to log in to continue using the LoadMaster.

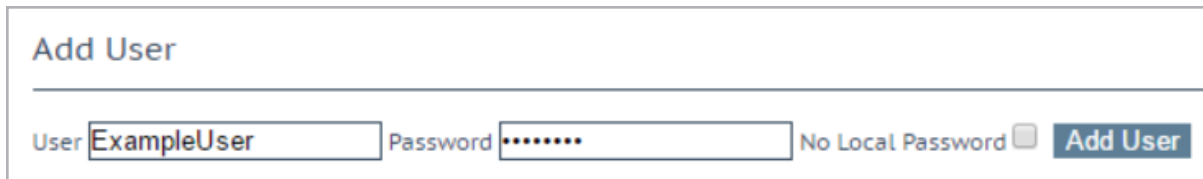
3. Configure any other settings as needed.

The default state for the Require Basic Authentication check box is disabled. When this option is disabled, both certificate and credential-based remote access are available. If the check box is enabled, only credentials are valid for remote access.

2.4.1.2 Create a User (If Needed)

It is not possible to use certificate-based authentication with the **bal** user. However, you can create a non-**bal** user and grant it **All Permissions**, or whatever permissions you want. If you do not already have another user created, you can add one by following these steps:

1. In the main menu of the LoadMaster WUI, expand **System Configuration > System Administration** and click **User Management**.



2. At the bottom of the screen, enter a username in the **User** text box.
3. At this point, you can either set a **Password** for the new user, or select the **No Local Password** check box.

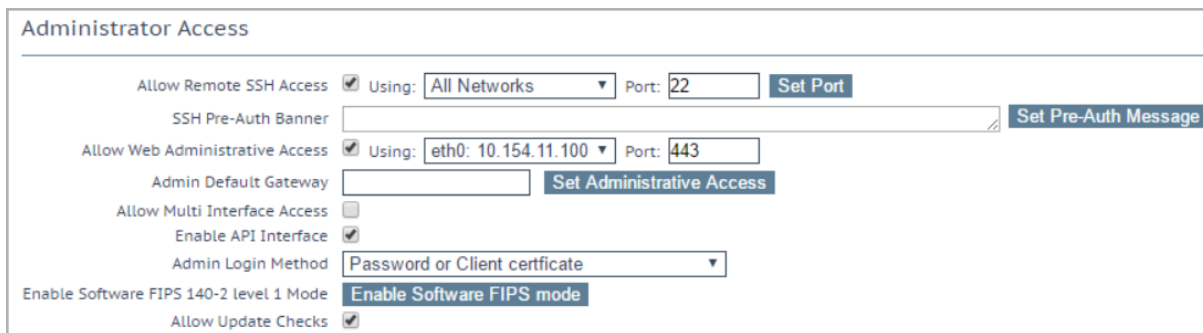
For further information on the **No Local Password** option, and on certificate authentication in general, refer to the **User Management, Feature Description**.

4. Click Add User.

2.4.1.3 Enable Client Certificate Authentication on the LoadMaster

A number of different login methods are available to enable. For steps on how to set the **Admin Login Method**, along with a description of each of the available methods, refer to the steps below:

5. In the main menu of the LoadMaster WUI, expand **Certificates & Security** and click **Remote Access**.



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

Using local certificates will only work with API authentication. Because of this, it might be best to select the **Password or Client certificate** option. This will allow API access using the client certificate and WUI access using the username/password.

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 either using 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 LoadMaster asks the client for a certificate. If a client certificate is available, the LoadMaster checks 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 granted 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 using 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. You must configure the OCSP Server Settings for this to work. For further information on the OCSP Server Settings, refer to the **DoD Common Access Card Authentication, Feature Description**.

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 terminates when the page is closed, or when the browser is restarted.

2.4.1.4 Generate and Download the Client Certificate

To generate a local certificate, follow the steps below:

Users with **User Administration** permissions are able to manage local certificates for themselves and other users.

1. In the main menu of the LoadMaster WUI, navigate to **System Configuration > System Administration > User Management**.

Local Users

User	Permissions	Operation
ExampleUser	All Permissions	<button>Modify</button> <button>Delete</button>

2. Click **Modify** on the relevant user.

Local Certificate

Download Certificate

Generate Certificate

Delete Certificate

Download

Generate

Delete

Passphrase

3. Enter a **Passphrase** and click **Generate**.

Entering a passphrase is optional. If a passphrase is entered it gets used to encrypt the private key.

10.154.11.170 says:

New Certificate generated

☐ Prevent this page from creating additional dialogs.

OK

4. Click **OK** to the pop-up message that appears.

Local Certificate

Download Certificate

Regenerate Certificate

Delete Certificate

Download

Regenerate

Delete

Passphrase

5. Click **Download**.

You can also regenerate from this screen.

2.4.1.5 Create the PFX File

When you generate a certificate, as described in the section above, the LoadMaster creates a .pem file. For certificate-based authentication to work with PowerShell, a .pfx file is required.

You can convert the .pem file to .pfx any way you like. For the purposes of this document, we have provided steps on how to do it using OpenSSL. If you are using Windows, you may need to install OpenSSL to run these steps.

To create a .pfx file using, follow the steps below:

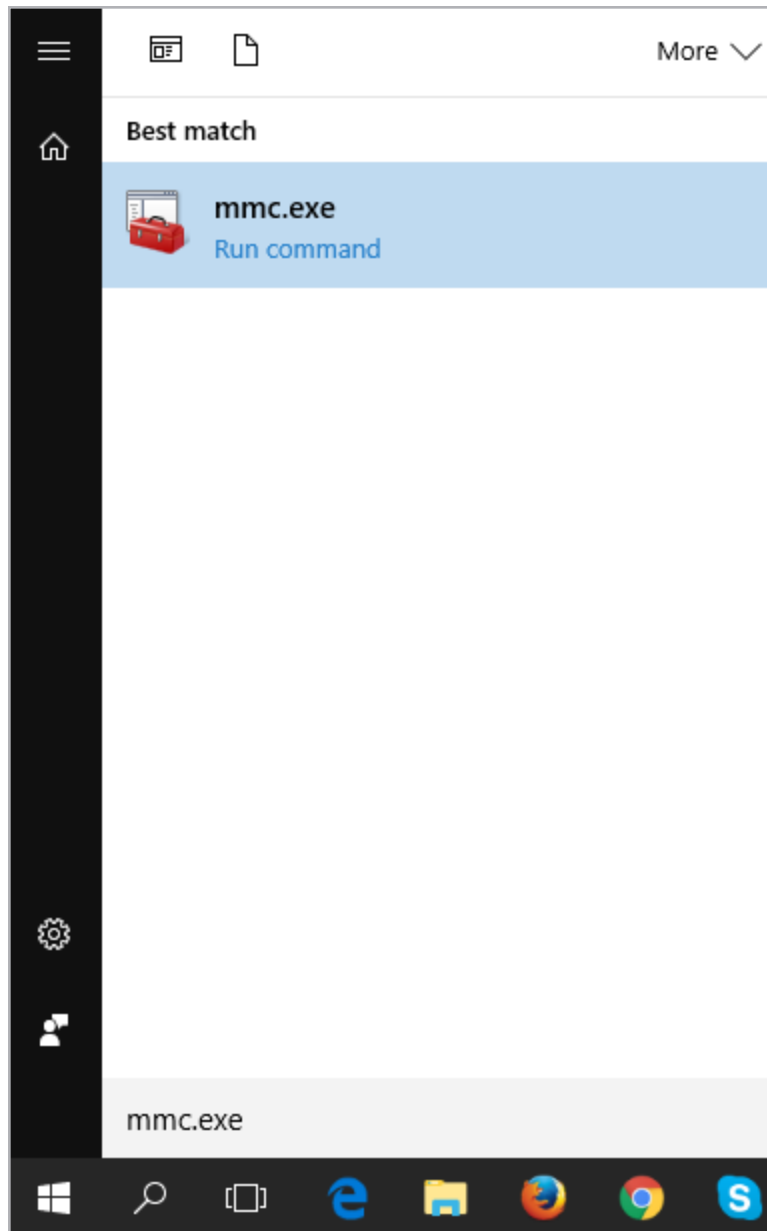
1. Open the .pem certificate.
2. Copy from the start of the **-----BEGIN CERTIFICATE-----** section to the end of the **-----END CERTIFICATE-----** section.
3. Paste this text into a new file.
4. Save the file as **<CerFileName>.cer**.
5. Go to the .pem certificate file again.
6. Copy from the start of the **-----BEGIN RSA PRIVATE KEY-----** section to the end of the **-----END RSA PRIVATE KEY-----** section.
7. Paste this text into a new file.
8. Save the file as **<KeyFileName>.key**.
9. Use the **openssl** command to create the .pfx file:

```
openssl pkcs12 -export -out <NewFileName>.pfx -inkey <KeyFilename>.key -in  
<CerFileName>.cer
```

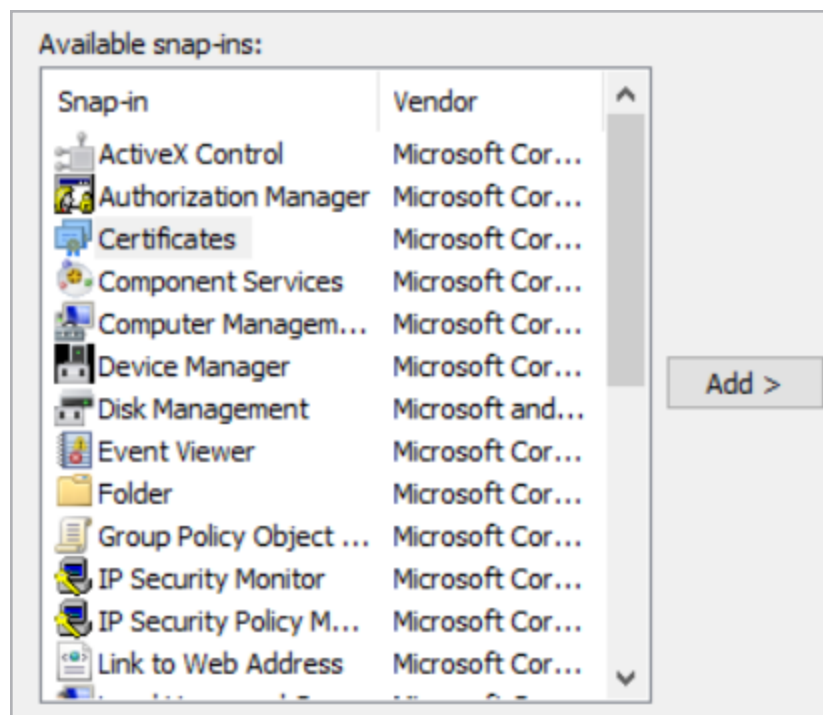
10. Import the certificate to the web browser.

2.4.1.6 Import the PFX File into the Microsoft Management Console (if using Windows)

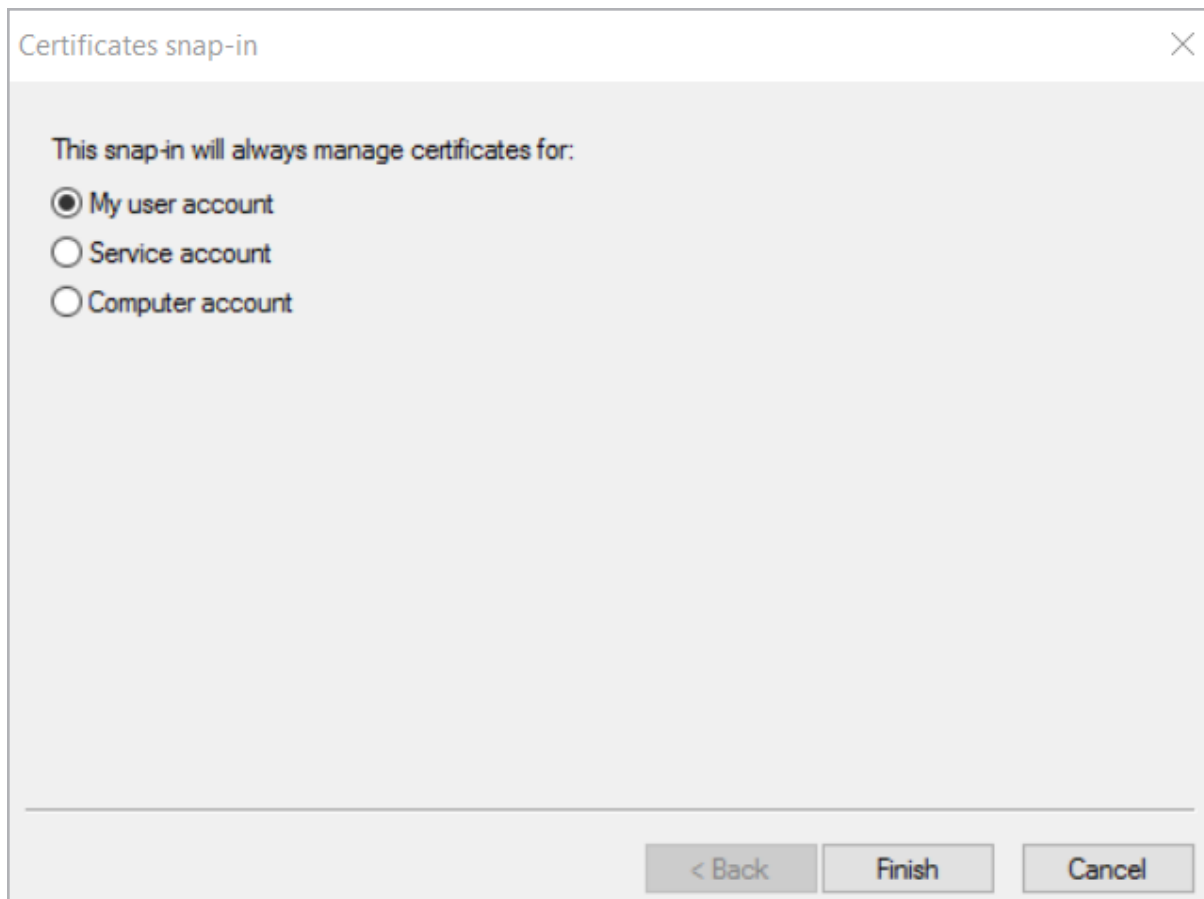
If you are using Windows, follow the steps below to import the .pfx file into the Microsoft Management Console:



11. Click **Start** and type **mmc.exe**.
12. Click **mmc.exe** to open the Microsoft Management Console.
13. Click **File** and select **Add/Remove Snap-in**.

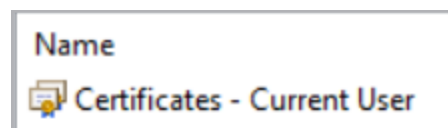


14. Select **Certificates** on the left and click **Add**.

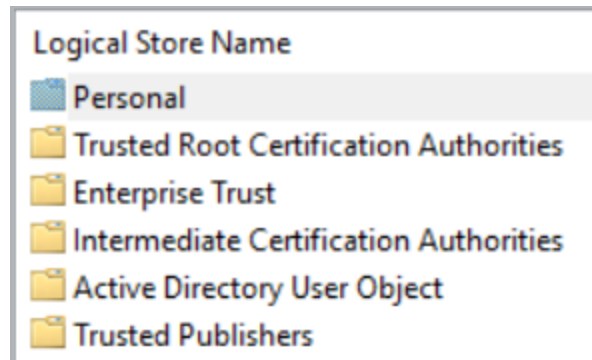


15. Ensure that **My user account** is selected and click **Finish**.

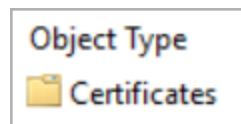
16. Click **OK**.



17. Double-click **Certificates – Current User**.

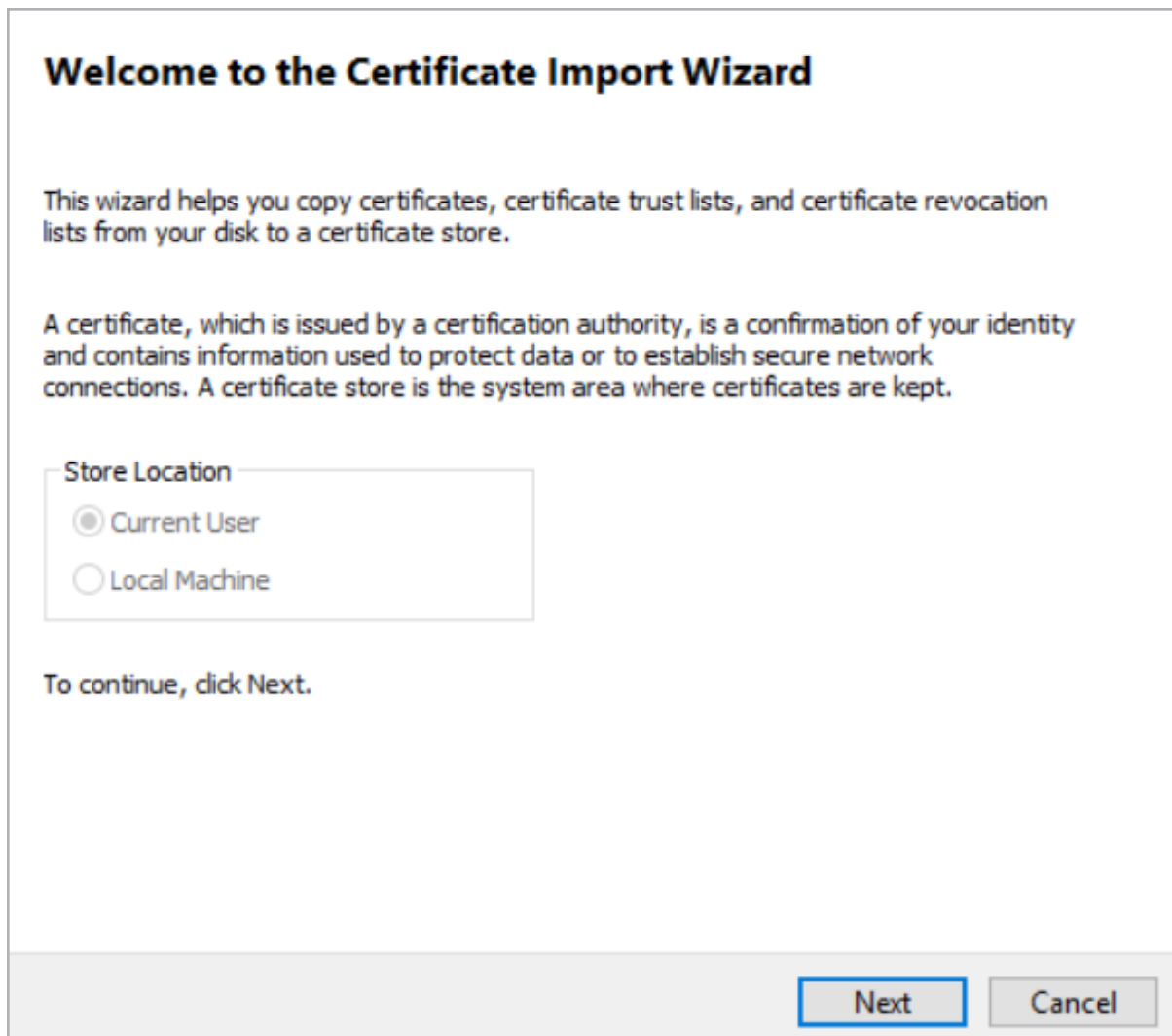


18. Double-click **Personal**.



19. Double-click **Certificates**.

20. Right-click on any white space in the middle panel, select **All Tasks** and click **Import**.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

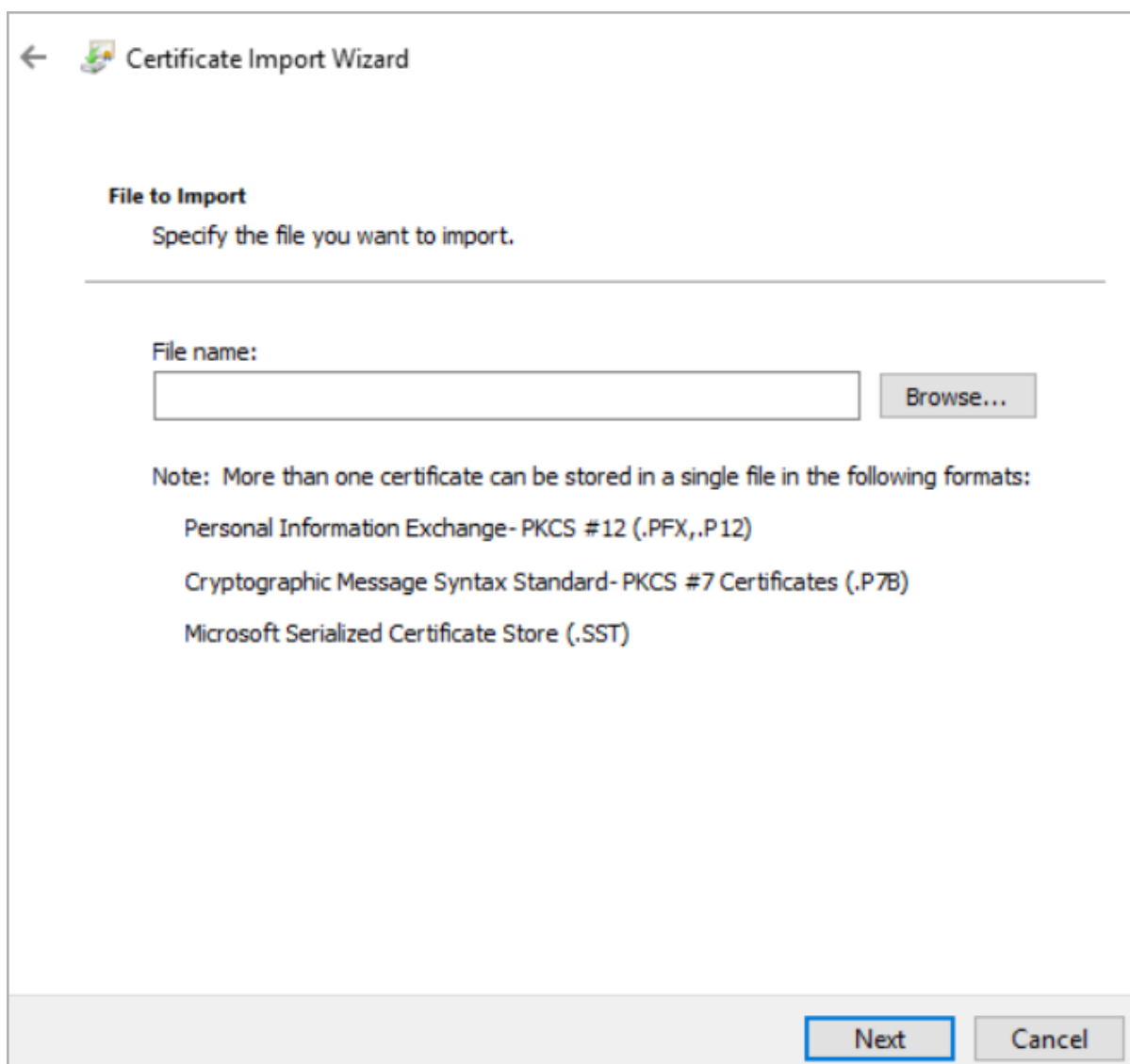
☒ Current User

☐ Local Machine

To continue, click Next.

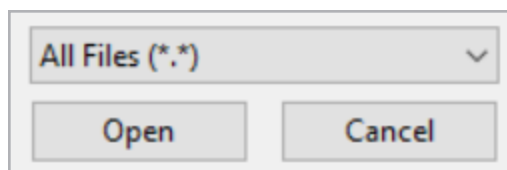
Next **Cancel**

21. Click **Next**.



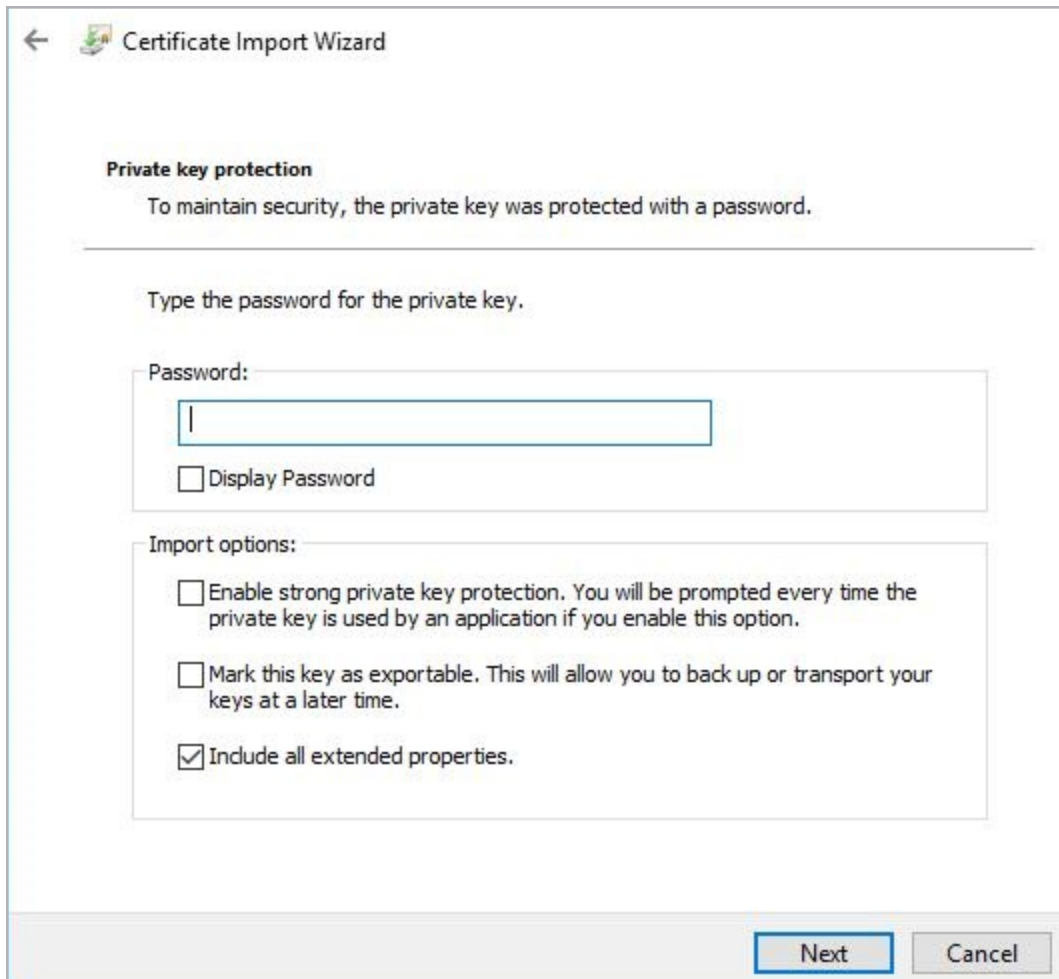
22. Click **Browse**.

23. Browse to the location of the .pfx file to be imported.



24. Select **All Files** in the drop-down menu in the bottom-right.

25. Double-click the .pfx file.



The image shows a Windows 'Certificate Import Wizard' dialog box. It has a title bar with a back arrow and the text 'Certificate Import Wizard'. The main content area is divided into sections. The first section is titled 'Private key protection' and contains the text 'To maintain security, the private key was protected with a password.' Below this is a horizontal line. The next section is titled 'Type the password for the private key.' and contains a 'Password:' label followed by a text input field with a cursor. Below the input field is a checkbox labeled 'Display Password'. The third section is titled 'Import options:' and contains three checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' (unchecked), 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' (unchecked), and 'Include all extended properties.' (checked). At the bottom right of the dialog are two buttons: 'Next' and 'Cancel'.

← Certificate Import Wizard

Private key protection

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

☐ Display Password

Import options:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

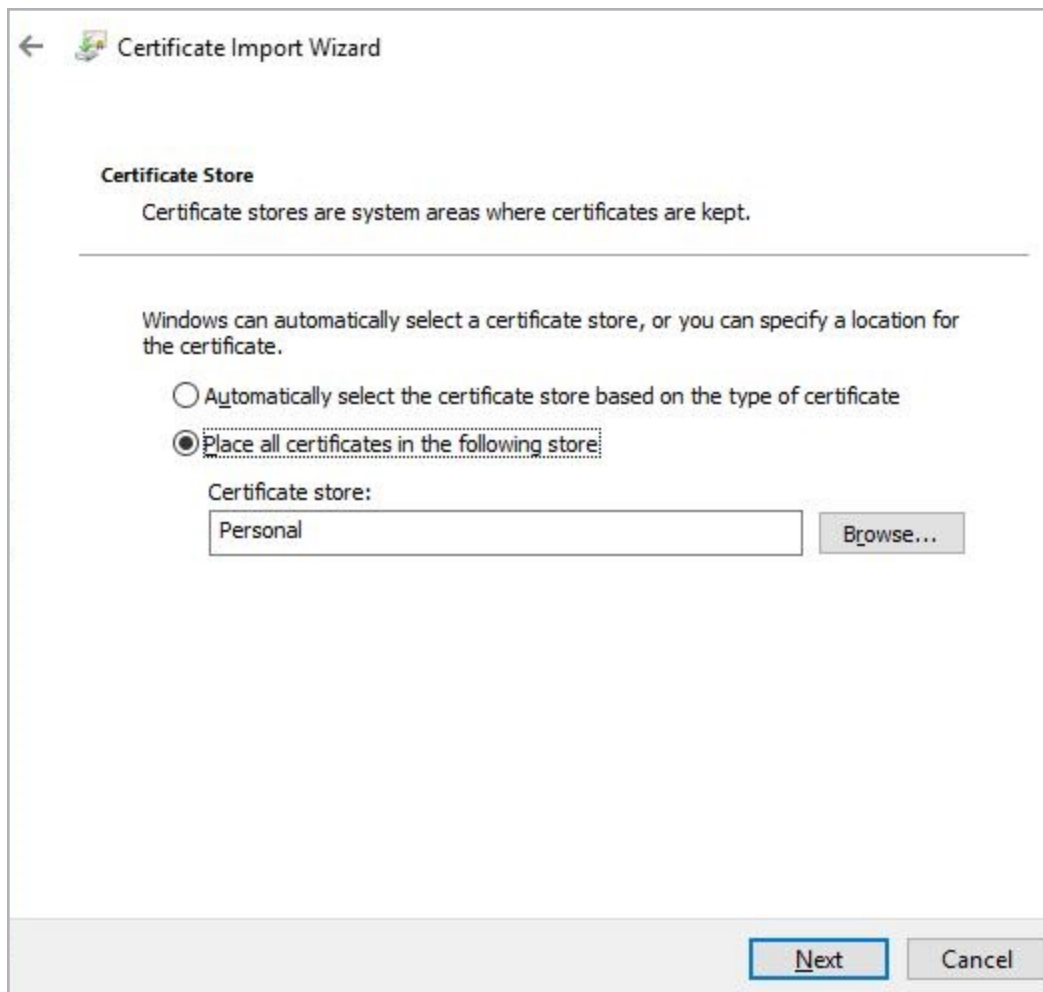
☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☒ Include all extended properties.

Next Cancel

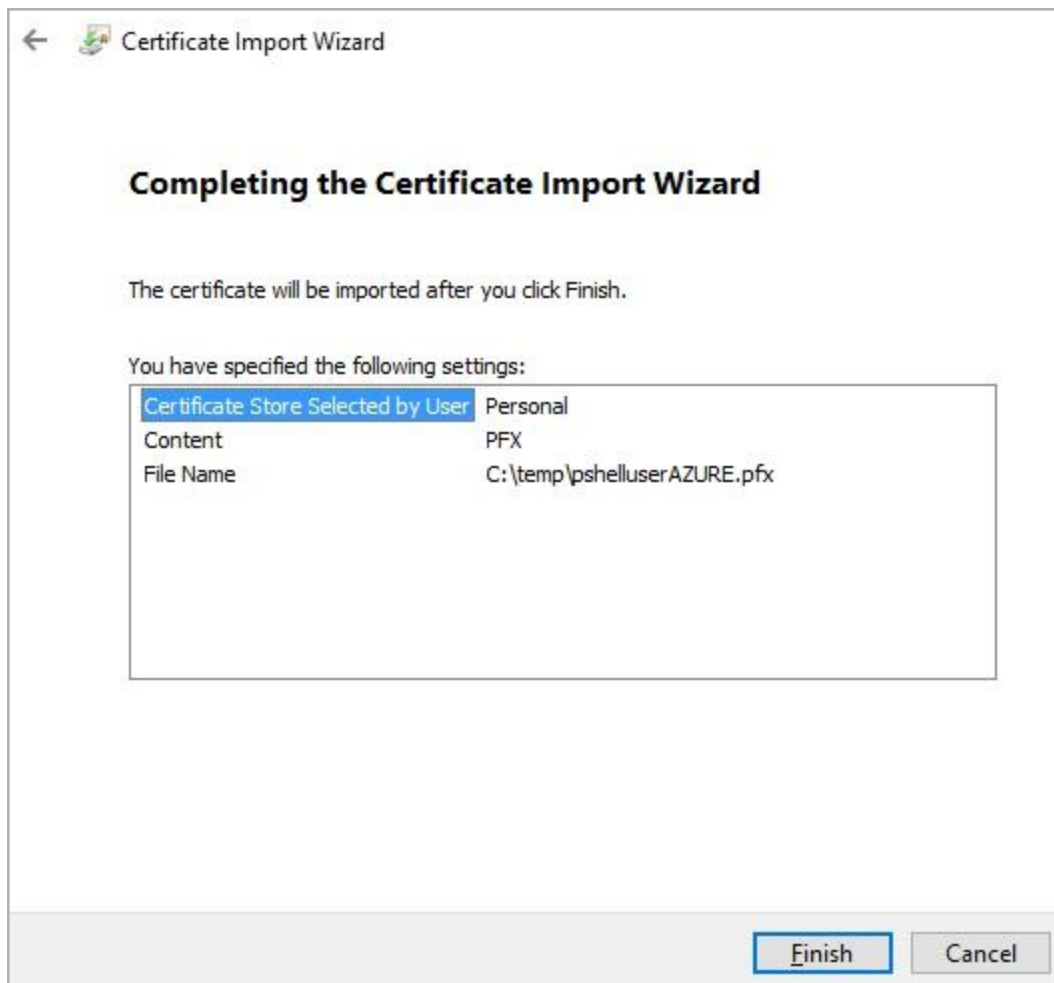
26. Enter the **Password** (if necessary).

27. Click **Next**.



28. Click **Browse** and select the **Personal** certificate store.

29. Click **Next**.



30. Review the settings and click **Finish**.

2.4.1.7 Specify the Certificate Details in the API

After configuring all of the options as outlined in the above sections, you need to specify the details of the certificate to run the API commands successfully. You can either do this using the **Initialize-Lm** command or in individual commands when they are run. The two parameters related to certificate-based authentication are:

- **SubjectCN:** This parameter is mandatory if you want to use certificate-based authentication. This is the certificate Common Name (CN). This is the username of the LoadMaster user that the certificate was generated for. If you do not specify the **CertificateStoreLocation**, the certificate is searched for in the **<CurrentUser>/My** location.
- **CertificateStoreLocation:** This parameter is optional. If you do not use it, the cmdlet searches for the certificate in the **<CurrentUser>/My** location (default). If the **CertificateStoreLocation** parameter is

- set, the API searches for the certificate in the specified location, for example **Cert:\<CurrentUser>\TrustedPeople**

2.5 Object Structure

As of the 7.2.39.0.334 version of the KEMP PowerShell wrapper, all the commands (except **Test-LmServerConnection**) return a PowerShell object with the following structure:

The **Test-LmServerConnection** command returns **True** if the LoadMaster is reachable by the API, **False** if not.

- **ReturnCode** (integer)
- **Response** (string)
- **Data** (PowerShell object, if any)

As a result of the new object structure, the current KEMP PowerShell wrapper is not compatible with scripts written based on an older version of the KEMP PowerShell wrapper (before July 2017).

The possible values for the **ReturnCode** field are:

- 200: The command completed successfully
- 4xx/500: The command ended with an error. The error code depends on the error type.

The possible values for the **Response** field are:

- Command successfully executed
- Description of the error when the command fails, for example **Unknown parameter value** **lmversion**.

The **Data** field contains the response, if any. The structure of this field depends on the command. The elements of this field can be accessed using the “dot” notation. If the command fails, this field is empty.

Example 1: Retrieve the installed LoadMaster firmware version:

```
$lma = Get-LmParameter -Param version -LoadBalancer 172.21.59.189 -SubjectCN user1
$lma | Format-List
ReturnCode : 200
Response   : Command successfully executed.
Data       : @{version=7.2.39.0.DEV-PRIVATE-user1}
$lma.Data.version
7.2.39.0.DEV-PRIVATE-user1
```

Example 2: Retrieve the available licenses for a specific Order ID:

```
$licDet = Get-LicenseType -KempId jbloggs@kemptechnologies.com -Password
ExamplePassword -LoadBalancer 172.21.59.85 -Credential $lm85Ba1Creds -OrderId
Example20170517
$licDet | Format-List
ReturnCode : 200
Response    : Command successfully executed.
Data        : @{License=System.Object[]}
$licDet.Data.License
id          : 0632b88b577c71591798268bcd4e01132f082309
name        : VLM-5000 ESP GEO with Basic 2 Years
available   : 1
description : VLM-5000 ESP GEO with Basic 2 Years
tethered    : False
LicenseStatus : Permanent License
BuyMoreAt   : https://www.kemptechnologies.com/buy-me-now?KEMPID=
jbloggs@kemptechnologies.com
id          : fc488d991cffb7a5958625427d6bfb0b3edc008e
name        : VLM-5000 WAF GEO with Basic 3 Years
available   : 1
description : VLM-5000 WAF GEO with Basic 3 Years
tethered    : False
LicenseStatus : Permanent License
BuyMoreAt   : https://www.kemptechnologies.com/buy-me-now?KEMPID=
jbloggs@kemptechnologies.com
name        : VLM-5000 with Enterprise Plus subscription
available   : 1
tethered    : 0
id          : 3eb92178611573946b422cf8d0df69d04c07fedc
LicenseStatus : Temp License
description  : VLM-5000 with Enterprise Plus subscription
BuyMoreAt   : https://www.kemptechnologies.com/buy-me-now?KEMPID=
jbloggs@kemptechnologies.com
```

In the above example, the `$licDet.Data.License` is an array and each single element of the array can be accessed using the “[]” notation. For example, to access the field name of the second element of the previous array we have to use the following notation: `$licDet.Data.License[1].name`. The index of the array starts from 0. The NULL object is returned if we try to access a non-existing element.

The benefits of the structure of the command answers are:

- It is easy to check for success/error (ReturnCode)
- There is a short description (Response)
- The Data field returns a PowerShell object when successful and null when there is an error

2.5.1 Errors

If the error is a functional one (for example using the wrong credentials, parameter value or LoadMaster IP address) the cmdlet returns a PowerShell object, as described, with a ReturnCode containing the code of the error and with Response containing the description of the error that has occurred.

For example: Try to get the firmware version installed on the LoadMaster using an invalid certificate (installed in the Windows machine but not belonging to any user inside the LoadMaster):


```
$lma = Get-LmParameter -Param version -LoadBalancer 172.21.59.85 -SubjectCN
user1
$lma
```

ReturnCode	Response	Data
-----	-----	----
	401 The remote server returned an error: (401) Unauthorized.	

If the error is due to a wrong/missing mandatory input, the cmdlet throws an exception.

For example: Get the firmware version installed on the LoadMaster using a certificate not installed in the Windows machine:

```
$lma = Get-LmParameter -Param version -LoadBalancer 172.21.59.189 -LBPort 8443 -SubjectCN
invalidcertificate
```

ERROR: Can't find a certificate with "invalidcertificate" as CN in the default Cert:\CurrentUser\My store.

At C:\Users\FabrizioCarpin\work\PowerShell\branches\PD-8213\Kemp.LoadBalancer.PowerShell\Kemp.LoadBalancer.PowerShell.psm1:273 char:5

```
+ Throw $errStr
```

```
+ ~~~~~
```

```
+ CategoryInfo          : OperationStopped: (ERROR: Can't fi...tUser\My
store.:String) [], RuntimeException
```

```
+ FullyQualifiedErrorId : ERROR: Can't find a certificate with "invalidcertificate"
as CN in the default Cert:\CurrentUser\My store.
```

For example: Get the firmware version installed on the LoadMaster without credentials/certificate:

```
$lma = Get-LmParameter -Param version -LoadBalancer 172.21.59.189 -LBPort 8443
```

ERROR: login method param is empty. Credentials or SubjectCN must be specified.

At C:\Users\FabrizioCarpin\work\PowerShell\branches\PD-8213\Kemp.LoadBalancer.PowerShell\Kemp.LoadBalancer.PowerShell.psm1:244 char:3

```
+ Throw $errStr
```

```
+ ~~~~~
```

```
+ CategoryInfo          : OperationStopped: (ERROR: login me...t be
specified.:String) [], RuntimeException
```

```
+ FullyQualifiedErrorId : ERROR: login method param is empty. Credentials or
SubjectCN must be specified.
```

2.6 Initially Configure a LoadMaster Using PowerShell API Commands

Several steps are involved in initially deploying a LoadMaster, such as accepting the End User License Agreement (EULA) and licensing the unit. Before the LoadMaster can be fully deployed, the EULAs must be displayed and accepted. These initial configuration steps can either be performed using the WUI or the API. The PowerShell API commands relating to initial configuration are in the sections below.

These commands should be run in sequential order.

2.6.1 Licensing Cloud LoadMasters

The two main licensing models for cloud LoadMasters are pay-per-use and Bring Your Own License (BYOL).

The Bring Your Own License (BYOL) model offers an alternative to the pay-per-use model. BYOL licenses are perpetual licenses which can include feature subscriptions. To use BYOL licensing, contact a KEMP representative to purchase a license. Then apply the license to the LoadMaster.

The pay-per-use licensing model enables you to pay for individual LoadMasters you need, for as long as you need to use them. You only pay for the usage consumed, and once you stop using them there are no additional costs or fees. Like BYOL subscription licenses, pay-per-use LoadMaster instances offer many different options for bandwidth throughput and add-on services.

Pay-per-use cloud LoadMasters are “pre-licensed”. Therefore, the following commands are not valid for pay-per-use LoadMasters: Read-LicenseEULA, Confirm-LicenseEULA, Confirm-LicenseEULA2 and Request-LicenseOnline. These commands are valid for BYOL cloud LoadMasters.

When deploying a pay-per-use LoadMaster, you can use the Set-LicenseInitialPassword command to configure the administrator password. The LoadMaster is ready to use after that point.

2.6.2 Initial Configuration Commands List

The initial configuration commands are listed below:

- EULA:
 - Read-LicenseEULA (mandatory)
 - Confirm-LicenseEULA (mandatory)
 - Confirm-LicenseEULA2 (mandatory)

These EULA commands must be run in the above order.

- License type:
 - Get-LicenseType (optional)
 - Get-AsLicenseType (optional)

These commands are optional when completing the licensing process. The **Get-LicenseType** command contacts the KEMP Licensing Server. The **Get-AsLicenseType** must be used with a KEMP 360 Central Activation Server instance that is acting as a “local licensing server”.

- Licensing:

- Request-LicenseOnline
- Request-LicenseOffline
- Request-LicenseOnPremise

To install the license on the LoadMaster, one of the above commands must be used:

- The online command is used when the LoadMaster can reach the KEMP licensing server.

- Otherwise, the offline command must be used. If using offline licensing, you must have the “BLOB” licensing text that KEMP sent in an email.

- The Request-LicenseOnPremise command is used to license a LoadMaster using a KEMP 360 Central acting as a “local licensing server”.

- Set password:
 - Set-LicenseInitialPassword (mandatory)

This command must be used to set the LoadMaster administrator (**bal**) password.

- Get license details:
 - Get-LicenseInfo (optional)
- Upgrade license:
 - Update-LicenseOnline (optional)
 - Update-LicenseOffline (optional)
- Legacy:
 - Get-LicenseAccessKey

2.6.3 Accept the EULAs

To license a LoadMaster, you must acknowledge the EULA licenses. This step involves three commands and they must be run in the following order:

1. Read-LicenseEULA
2. Confirm-LicenseEULA
3. Confirm-LicenseEULA2

For example:

```
$reula = Read-LicenseEULA -LoadBalancer 172.21.59.85 -Credential $lm85BalCreds
```

```
$reula
-----
ReturnCode Response Data
-----
200 Command successfully executed @{Eula=}
$reula.Data.Eula
MagicString Eula
-----
d15981f0-ec48-4558-8a3e-796e2036300d ...
```

The **MagicString** parameter must be used as input for the **Confirm-LicenseEULA** command. The **Type** parameter is optional. The default value for the **Type** parameter is **Trial**. The **Free** value must only be used for the Free LoadMaster.

```
$ceula = Confirm-LicenseEULA -Magic $reula.Data.Eula.MagicString `
                                -LoadBalancer 172.21.59.85 -
Credential $lm85BalCreds
$ceula
-----
ReturnCode Response Data
-----
200 Command successfully executed @{Eula2=}
$ceula.Data.Eula2
MagicString Eula2
-----
46181257-2f09-4094-a9cd-6af02f352180 ...
```

The last step is to run the **Confirm-LicenseEULA2** command. The **MagicString** parameter is from the **Confirm-LicenseEULA** output. The command is used to specify whether to use the Call Home feature. If it is enabled, the LoadMaster regularly contacts the KEMP Licensing Server to check for updates and other information. Specify the value (**yes/no**) as desired.

```
$ceula2 = Confirm-LicenseEULA2 -Magic $ceula.Data.Eula2.MagicString -Accept
yes
                                -LoadBalancer 172.21.59.85 -Credential
$lm85BalCreds
$ceula2
-----
ReturnCode Response Data
-----
200 Command successfully executed.
```

2.6.4 Retrieve the Available Licenses (optional)

Before running the command to license the LoadMaster (**Request-LicenseOnline/Request-LicenseOffline**) it is possible to retrieve the available license(s) for a specific KEMP ID from the KEMP Licensing Server using the **Get-LicenseType** command.

The parameters for this command are:

- KempId (mandatory)
- Password (mandatory)

- OrderId (optional)

The output of the command (when successful) has the following structure:

```
ReturnCode : 200
Response   : Command successfully executed.
Data       : @{License=}
```

The field **Data.License** contains details about the the license(s) and it always includes the temporary license option. For example:

```
$licDet.Data.License
id           : 0632b88b577c71591798268bcd4e01132f082309
name         : VLM-5000 ESP GEO with Basic 2 Years
available    : 1
description  : VLM-5000 ESP GEO with Basic 2 Years
tethered     : False
LicenseStatus : Permanent License
BuyMoreAt    : https://www.kemptechnologies.com/buy-me-
now?KEMPID=jbloggs@kemptechnologies.com
id           : fc488d991cffb7a5958625427d6bfb0b3edc008e
name         : VLM-5000 WAF GEO with Basic 3 Years
available    : 1
description  : VLM-5000 WAF GEO with Basic 3 Years
tethered     : False
LicenseStatus : Permanent License
BuyMoreAt    : https://www.kemptechnologies.com/buy-me-now?KEMPID=
jbloggs@kemptechnologies.com
name         : VLM-5000 with Enterprise Plus subscription
available    : 1
tethered     : 0
id           : 3eb92178611573946b422cf8d0df69d04c07fed
LicenseStatus : Temp License
description  : VLM-5000 with Enterprise Plus subscription
BuyMoreAt    : https://www.kemptechnologies.com/buy-me-now?KEMPID=
jbloggs@kemptechnologies.com
```

In this example, the customer purchased two licenses. The third entry is the temporary license.

If the KEMP ID does not exist, the command returns the string "License type information not available".

2.6.4.1 Example without Specifying an Order ID

Without an Order ID, the command only returns the temporary license details:

```
$licDet = Get-LicenseType -KempId jbloggs@kemptechnologies.com -Password
supersecretpasswd -LoadBalancer 172.21.59.85 -
Credential $lm85Ba1Creds
$licDet
ReturnCode Response Data
-----
200 Command successfully executed. @{License=System.Object[]}
```

```
$licDet.Data.License
name         : VLM-5000 with Enterprise Plus subscription
available    : 1
tethered     : 0
id           : 3eb92178611573946b422cf8d0df69d04c07fed
```

```
LicenseStatus : Temp License
description   : VLM-5000 with Enterprise Plus subscription
BuyMoreAt    : https://www.kemptechnologies.com/buy-me-
now?KEMPID=jbloggs@kemptechnologies.com
```

2.6.4.2 Example with a Valid Order ID

If a valid Order ID is provided, the command returns an array of licenses containing the purchased license (s) and the temporary license details:

```
$licDet = Get-LicenseType -KempId gigio@gigetto.com -Password
supersecretpasswd -LoadBalancer 172.21.59.85 -Credential $lm85Ba1Creds -
OrderId Example20170517
$licDet | Format-List
ReturnCode : 200
Response    : Command successfully executed.
Data        : @{{License=System.Object[]}}
$licDet.Data.License
id          : 0632b88b577c71591798268bcd4e01132f082309
name        : VLM-5000 ESP GEO with Basic 2 Years
available   : 1
description : VLM-5000 ESP GEO with Basic 2 Years
tethered    : False
LicenseStatus : Permanent License
BuyMoreAt   : https://www.kemptechnologies.com/buy-me-
now?KEMPID=jbloggs@kemptechnologies.com
id          : fc488d991cffb7a5958625427d6bfb0b3edc008e
name        : VLM-5000 WAF GEO with Basic 3 Years
available   : 1
description : VLM-5000 WAF GEO with Basic 3 Years
tethered    : False
LicenseStatus : Permanent License
BuyMoreAt   : https://www.kemptechnologies.com/buy-me-now?KEMPID=
jbloggs@kemptechnologies.com
name        : VLM-5000 with Enterprise Plus subscription
available   : 1
tethered    : 0
id          : 3eb92178611573946b422cf8d0df69d04c07fede
LicenseStatus : Temp License
description  : VLM-5000 with Enterprise Plus subscription
BuyMoreAt   : https://www.kemptechnologies.com/buy-me-now?KEMPID=
jbloggs@kemptechnologies.com
```

The answer is an array and you can retrieve each element of the array by using the usual array syntax, for example, to get the first element of the array:

```
$licDet.Data.License[0]
id          : 0632b88b577c71591798268bcd4e01132f082309
name        : VLM-5000 ESP GEO with Basic 2 Years
available   : 1
description : VLM-5000 ESP GEO with Basic 2 Years
tethered    : False
LicenseStatus : Permanent License
BuyMoreAt   : https://www.kemptechnologies.com/buy-me-now?KEMPID=
jbloggs@kemptechnologies.com
```

2.6.4.3 Example with an Invalid (Undefined) KEMP ID

An example with an invalid (or non-existing) KEMP ID is below:

```
$err = Get-LicenseType -KempId invalid@invalid.co.uk -Password bla2017bla `
                                     -LoadBalancer 172.21.59.85 -Credential
$lm85Ba1Creds
ReturnCode : 200
Response   : Command successfully executed.
Data       : @{Licenses=License type information not available}
$err.Data.Licenses
License type information not available
```

2.6.4.4 Retrieve License Types when using Activation Server Functionality

If you are licensing the LoadMaster using a KEMP 360 Central Activation Server, a similar command (**Get-AsLicenseType**) is used to retrieve the available licenses. The parameters for this command are:

- aslipaddress (mandatory): IP address of the KEMP 360 Central Activation Server instance
- aslport (mandatory): The KEMP 360 Central Activation Server listening port
- aslname (optional): The KEMP 360 Central Activation Server Fully Qualified Domain Name (FQDN)

2.6.5 License the LoadMaster

The commands to license the LoadMaster (initially license the LoadMaster for the first time, not updating an existing LoadMaster license) are **Request-LicenseOnline** and **Request-LicenseOffline**.

To use the **Request-LicenseOnline** command, the LoadMaster must be able to connect to the KEMP Licensing Server. If this is not possible, the **Request-LicenseOffline** command can be used.

The **Request-LicenseOnPremise** command is used to license a LoadMaster using a KEMP 360 Central as a “Local Licensing Server”.

The **Request-LicenseOnline** command interface contains the **OrderId** and **LicenseTypeId** parameters. When you purchase a product from KEMP, KEMP provide you with the **OrderId**. The **OrderId** is a unique string that is a pointer to the record that details what was purchased. The **OrderId** is a container – there may be multiple license types for one **OrderId**. The **LicenseTypeId** is the “license ID” that can be retrieved using the **Get-LicenseType** command, as shown in the above examples.

If you specify the **OrderId** but not the **LicenseTypeId**, the first license in the list matching the specified Order ID is used. This is the first license defined (the oldest) for that order ID.

If you specify both the **OrderId** and **LicenseTypeId**, the specific license matching both the Order ID and License Type ID is used.

If you do not specify either an **OrderId** or **LicenseTypeId**, a temporary license is applied.

If you specify a **LicenseTypeId** but not an **OrderId**, an error message is returned. This is an invalid combination – the Order ID must also be specified if using the License Type ID.

The following table summarizes the above text:

OrderId (not mandatory)	LicenseTypeId (not mandatory)	License Given to the LoadMaster
Used	Not used	First license in the list matching the specified Order ID
Used	Used (value from Get-LicenseType)	The specific license matching the Order ID and License Type ID
Not used	Not used	Temporary license
Not used	Used (value from Get-LicenseType)	Invalid combination (error is returned). The Order ID must also be specified.

2.6.5.1 Online Licensing Example

The below example uses online licensing and requests a specific license (both the **OrderId** and **LicenseTypeId** must be used):

```
$lictype = Get-LicenseType -KempId jbloggs@kemptechnologies.com -Password
supersecretpassword -LoadBalancer 172.21.59.85 -Credential $lm85BalCreds -OrderId
marvel20170511-01
$lictype | Format-List
Response : 200
Data : Command successfully executed.
$lic = Request-LicenseOnline -LoadBalancer 172.21.59.85 -Credential
$lm85BalCreds -KempId jbloggs@kemptechnologies.com -Password
supersecretpassword -LicenseTypeId $lictype.Data.License[0].id -OrderId
marvel20170511-01
$lic | Format-List
Response : 200
Data : Command successfully executed.
```

2.6.5.2 Offline Licensing Example

An example using the offline licensing method is below:

```
$offline_lic = Request-LicenseOffline -Path .\blob-85.blob -LoadBalancer
172.21.59.85
$offline_lic
Response : 200 Command successfully executed.
```


2.6.6 Set the Initial Password for the LoadMaster

After licensing, you must set the administrator password before you can start using the LoadMaster. Use the **Set-LicenseInitialPassword** command to do this, for example:

```
$setp = Set-LicenseInitialPassword -Passwd balsupersecretpassword -
LoadBalancer 172.21.59.85`
```

```
Credential $lm85BalCreds
$setp | Format-List
ReturnCode : 200
Response   : Command successfully executed.
Data       :
```

2.6.7 Retrieve the License Details (optional)

You can use the **Get-LicenseInfo** command to retrieve the LoadMaster license details.

```
$license_details = Get-LicenseInfo -LoadBalancer 172.21.59.85 -Credential
$lm85BalCreds
```

ReturnCode	Response	Data
200	Command successfully executed.	@{LicenseInfo=}
\$license_details.Data.LicenseInfo		
uuid	:	941b6d65-1758-40a3-8a89-a9b45a8a8512
ActivationDate	:	Wed May 17 16:47:46 UTC 2017
LicensedUntil	:	unlimited
SupportLevel	:	Basic 2 years
SupportUntil	:	Fri May 17 04:00:00 UTC 2019
LicenseType	:	VLM-5000 ESP GEO
LicenseStatus	:	Single Perm
ApplianceModel	:	VLM-5000 ESP GEO
MaxVS	:	0
MaxRS	:	0
Bandwidth	:	5000
TpsLimit	:	10000
HA	:	no
FirstHA	:	no
ModSecurity	:	yes
AFE	:	yes
ViewAFE	:	yes
ESP	:	yes
IPSEC	:	2
SingleCPU	:	no
VLM	:	yes
VlmPlatform	:	VMWARE
SKU	:	VLM_OVF_64
FreeLicense	:	no
Temporary	:	no
ASL	:	no
MandatoryTether	:	no
MultipleConnect	:	no

2.6.8 Update a LoadMaster License

The LoadMaster license can be updated using the **Update-LicenseOnline** or **Update-LicenseOffline** command.

Here is an example using the online command:

```
$licupdate = Update-LicenseOnline -KempId fabrizio@eagle.com -Password
kempkemp -LoadBalancer 172.21.59.85 -
Credential $lm85BalCreds
$licupdate
ReturnCode Response Data
-----
200 Command successfully executed.
```

You can check the updated license by running the **Get-LicenseInfo** command.

2.7 Code Snippet Examples

Refer to the sections below for some code snippet examples.

2.7.1 Online Licensing

The following prerequisites are assumed:

- A KEMP LoadMaster with an IP address has been deployed and is ready to be set up
- A valid KEMP ID and password exists to get the license from the KEMP Licensing Server

```
# (1) CREATE THE CREDENTIALS
$passwd = ConvertTo-SecureString "<<your password>>" -AsPlainText -Force
$creds = New-Object System.Management.Automation.PSCredential("bal", $passwd)
$LMIP = <<LoadMaster IP address>>
$KEMPID = <<Customer KEMP ID>>
$KEMPPASSWD = <<Customer KEMP PASSWORD>>
# (2) Virtual Service and Real Server details (for more details about the
configuration parameters see the official KEMP documentation:
https://kemptechnologies.com/loadmaster-documentation/)
$VSIP = <<Virtual Service IP>>
$VSPORT = <<Virtual Service Port>>
$VSProtocol = <<Virtual Service Protocol (tcp/udp)>>
$RSIP = <<Real Server IP>>
$RSPORT = <<Real Server Port>>
# (3) GET the EULA
$reula = Read-LicenseEULA -LoadBalancer $LMIP -Credential $creds
if ($reula.ReturnCode -ne 200) {
# ERROR: exit
return $reula
}
# (4) CONFIRM the EULA (mandatory)
$ceula = Confirm-LicenseEULA -Magic $reula.Data.Eula.MagicString `
-LoadBalancer $LMIP -Credential $creds
if ($ceula.ReturnCode -ne 200) {
# ERROR: exit
return $ceula
}
# (5) CONFIRM/NOT CONFIRM the EULA2 (your choice)
$accept = "yes"
$accept = "no"
$ceula2 = Confirm-LicenseEULA2 -Magic $ceula.Data.Eula2.MagicString `
-Accept $accept -LoadBalancer $LMIP -Credential $creds
if ($ceula2.ReturnCode -ne 200) {
```

```
# ERROR: exit
return $ceula2
}
# (6) LICENSE the machine
$lic = Request-LicenseOnline -LoadBalancer $LMIP -Credential $creds `
                                -KempId $KEMPID -Password $KEMPPASSWD
if ($lic.ReturnCode -ne 200) {
# ERROR: exit
return $lic
}
# (7) SET the Initial Password
$setp = Set-LicenseInitialPassword -Passwd $passwd -LoadBalancer $LMIP `
                                    -Credential $creds
if ($setp.ReturnCode -ne 200) {
# ERROR: exit
return $setp
}
# (8) CREATE a Virtual Service
$vs = New-AdcVirtualService -VirtualService $VSIP -VSPort $VSPORT `
                            -VSProtocol $VSPROTOCOL -LoadBalancer $LMIP -Credential $creds
if ($vs.ReturnCode -ne 200) {
# ERROR: exit
return $vs
}
# (9) CREATE a Real Server
$rs = New-AdcRealServer -VirtualService $VSIP -VSPort $VSPORT `
                        -VSProtocol $VSPROTOCOL -RealServer $RSIP -RealServerPort $RSPORT `
                        -LoadBalancer $LMIP -Credential $creds
if ($rs.ReturnCode -ne 200) {
# ERROR: exit
return $rs
}
}
```

2.7.2 Initialize the LoadMaster Connection Parameters

In the above examples, the required parameters, **LoadBalancer** and **Credential**, can be initialized before running the commands with the **Initialize-LmConnectionParameters** command. If you do this, it is not necessary to specify these parameters in each command.

For example:

```
$lma = Initialize-LmConnectionParameters -Address $LMIP -Credential $creds
$lma | Format-List
ReturnCode : 200
Response   : Command successfully executed.
Data       : @{Connection=; Login=}
After the initialization, for example, the command to create a vs will become:
$vs = New-AdcVirtualService -VirtualService $VSIP -VSPort $VSPORT `
                            -VSProtocol $VSPROTOCOL
if ($vs.ReturnCode -ne 200) {
# ERROR: exit
return $vs
}
}
```

2.7.3 Enable the API

You can enable the API using the command **Enable-SecAPIAccess**. The LoadMaster must be licensed for this command to work.

```
$seapi = Enable-SecAPIAccess -LoadBalancer $LMIP -Credential $creds
$seapi | Format-List
ReturnCode : 200
Response   : The API is enabled
Data       :
```

If you license a LoadMaster using the API, the API is automatically enabled.

2.8 Known Issues with Beta PowerShell Wrapper

The 7.2.39.0.334 version of the KEMP PowerShell wrapper has the following known issues:

- The **New-GeoCluster** command fails if you try to add an already existing cluster.
- GEO custom locations do not restore correctly.
- The **New-SdnController** fails in a specific scenario: if you create an SDN controller or multiple SDN controllers and delete all the SDN controllers, you cannot add a new SDN controller.
- In the **Set-GeoFQDN** command, the parameter **SiteFailureDelay** is specified in minutes but the returned value is in seconds.
- A 200 success message is returned when the **Get-GeoFQDN** or **Get-GeoCluster** command is run for a non-existing FQDN/cluster.

References

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

WUI, Configuration Guide

KEMP LoadMaster, Product Overview

User Management, Feature Description

DoD Common Access Card Authentication, Feature Description

Document History

Date	Change	Reason for Change	Version	Resp.
July 2016	Major updates	Help text moved into module	11.0	LB
Oct 2016	Release updates	Updates for 7.2.36	12.0	LB
Jan 2017	Release updates	Updates for 7.2.37	13.0	POC
Mar 2017	Release updates	Updates for 7.2.38	14.0	LB
June 2017	Release updates	Updates for 7.2.39	15.0	LB
June 2017	Minor changes	Enhancements made	16.0	LB
June 2017	Minor changes	Enhancements made	17.0	LB