VMware vRealize Orchestrator

Feature Description

UPDATED: 22 March 2021

Copyright Notices

Table of Contents

1 Introduction 6
1.1 Document Purpose 6
1.2 Intended Audience 7
1.3 Related Firmware Version 7
1.4 Prerequisites 7
2 Install the Kemp Orchestrator Plugin 8
3 Using the Kemp Orchestrator Plugin 12
3.1 Inventory 12
3.2 Workflows 13
3.3 Files 14
3.3.1 Delete Files 14
3.3.2 Upload Files 18
3.3.2.1 Uploading Files which are Bigger than 2MB 21
3.3.2.1.1 Using SCP to Copy a File to the Orchestrator Server 22
3.3.2.1.2 Use cURL to Download the File 22
3.3.2.1.3 Configuring Permissions 23
3.4 LoadMasters 23
3.4.1 Add LoadMaster 23
3.4.2 Add Certificate 25
3.4.3 Backup Certificates 31
3.4.4 Backup LoadMaster 35

3.4.5 Delete Certificate 39
3.4.6 Disable API 42
3.4.7 Enable API 45
3.4.8 Get Parameter 48
3.4.9 Install Patch 52
3.4.10 Reboot LoadMaster 54
3.4.11 Remove LoadMaster 57
3.4.12 Restore Certificates 59
3.4.13 Restore LoadMaster 64
3.4.14 Set Credentials 69
3.4.15 Set Parameter 71
3.5 Virtual Services 76
3.5.1 Add Virtual Service 76
3.5.2 Assign Virtual Service Certificates 78
3.5.3 Modify Virtual Service Name 83
3.5.4 Remove Virtual Service 86
3.6 Sub Virtual Services 89
3.6.1 Add SubVS 89
3.6.2 Modify SubVS Name 92
3.6.3 Remove SubVS 95
3.7 Real Servers 98
3.7.1 Add Real Server to Sub Virtual Service 98

3.7.2 Add Real Server to Virtual Service 101

3.7.3 Remove Real Server 104

4 Uninstall the Kemp Orchestrator Plugin 108

4.1 Uninstall the Workflows 108

4.2 Remove the Kemp Orchestrator Plugin 109

4.3 Restart the Service 110

5 Appendix A - Get and Set Parameters 113

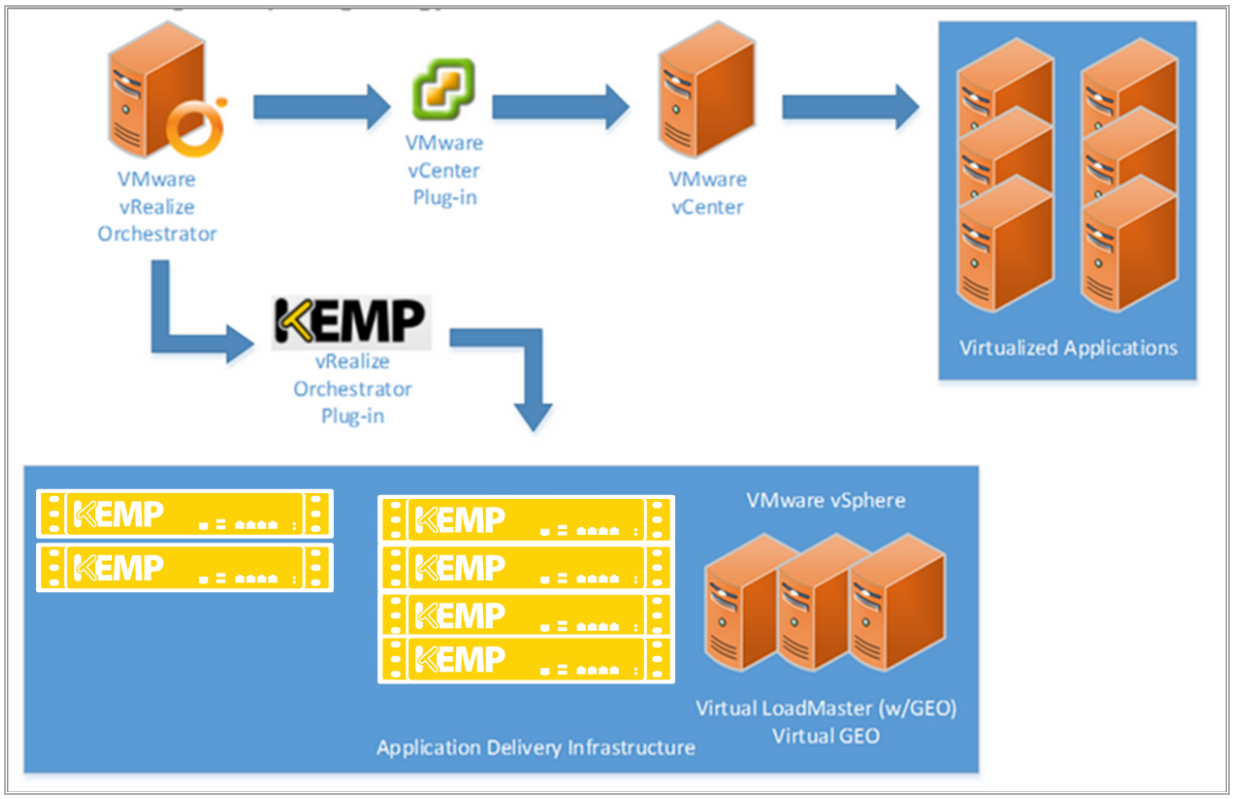
6 Appendix B - Memory and CPU Usage Details 119

References 121

Last Updated Date 122

1 Introduction

VMware vRealize Orchestrator allows administrators to develop complex automation tasks, then quickly access and launch workflows from the VMware vSphere client or various triggering mechanisms such as vROPs, vCAC, and so on.



Kemp have developed a plugin for Orchestrator which acts as a front-end for the Kemp Java API commands. When this plugin is installed, users can perform a number of tasks on the LoadMaster using the Orchestrator interface. The plugin allows Orchestrator to send commands (via workflows) to and receive information back from the Kemp LoadMaster and GEO products.

1.1 Document Purpose

The purpose of this document is to describe how to install and use the Kemp Orchestrator plugin. The document provides step-by-step instructions on how to run the various Kemp workflows which are added when the plugin is installed.

1.2 Intended Audience

This document is intended to be used by anyone who would like to use Orchestrator to manage their LoadMasters.

1.3 Related Firmware Version

Published with LMOS version 7.2.48.3 LTS. This document has not required substantial changes since 7.2.48.3 LTS. However, the content is in sync with the latest LoadMaster LTS firmware.

1.4 Prerequisites

Below are some prerequisites to be aware of before using the Kemp Orchestrator plugin:

- If using the default self-signed certificate which is generated by the LoadMaster, please ensure it is registered properly with the systems and that it is trusted. Please refer to VMware documentation, or your Operating System documentation, for instructions on how to do this.

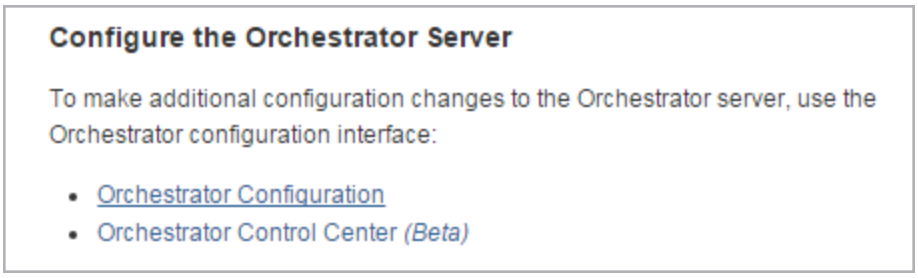
  > If the certificate is not trusted there may be issues running the workflows.

- If using an FQDN as opposed to an IP address, please ensure that the DNS is properly configured.

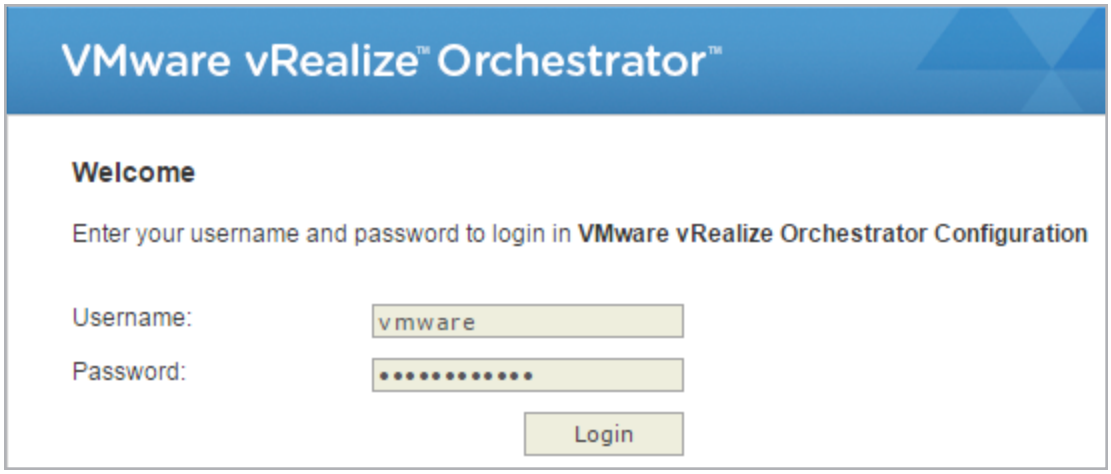
2 Install the Kemp Orchestrator Plugin

Before using Orchestrator to manage a Kemp LoadMaster, the Kemp Orchestrator plugin must be installed. To do that, first download the Kemp Orchestrator plugin from the VMware Solution Exchange. Then, follow the steps below:

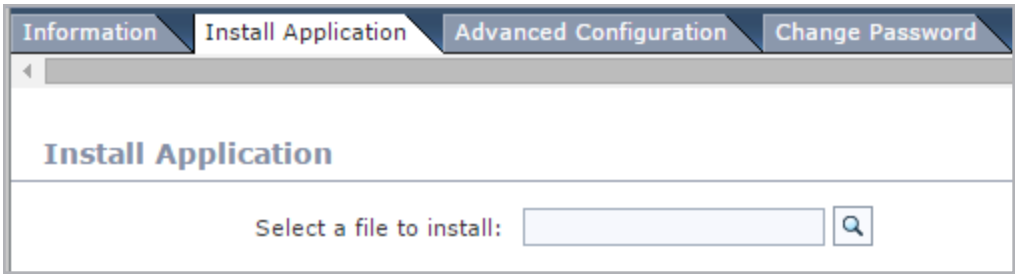
1. In a web browser, navigate to the IP address of the Orchestrator server followed by the :8281 port.



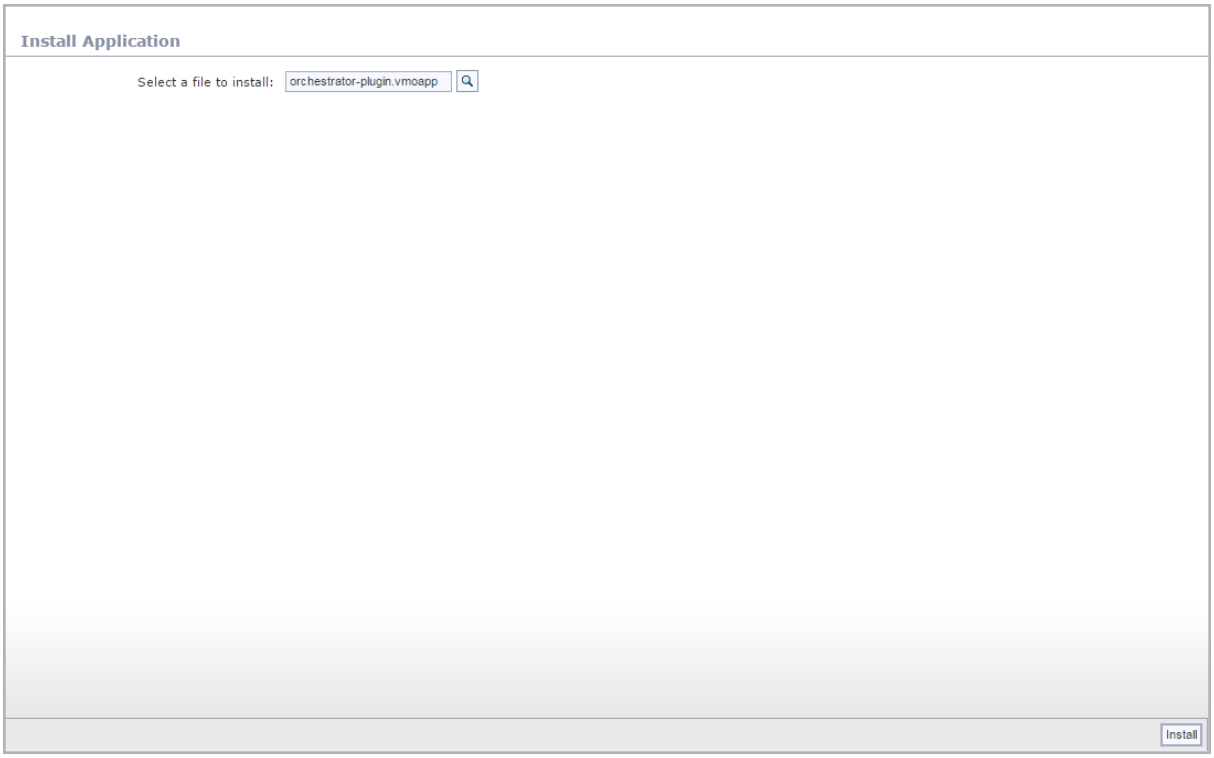
2. Click the **Orchestrator Configuration** link.



3. Enter the Orchestrator credentials and click **Login**.



4. Select the **Install Application** tab.
5. Click the magnifying glass icon.

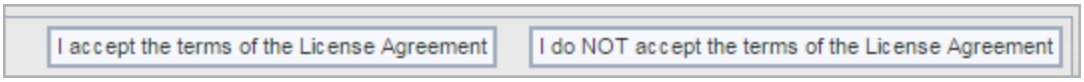


6. Browse to and select the Kemp Orchestrator plugin file (.vmo app file).

> If you cannot see the plugin file, you may need to select **All Files** in the bottom-right corner.

7. Click **Install** in the bottom-right.

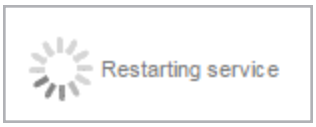
> It might take a few seconds to upload the plugin before moving on to the next screen.



8. To accept the license agreement, click **I accept the terms of the License Agreement**.

9. The plugin is now installed, but before it can be used the Orchestrator service needs to be restarted. To do this, click **Startup Options** on the left.

10. Click **Restart service**.



11. Wait for the service to restart.

12. A message will appear when the service has been restarted.

The Kemp Orchestrator plugin should now be installed and ready to use.

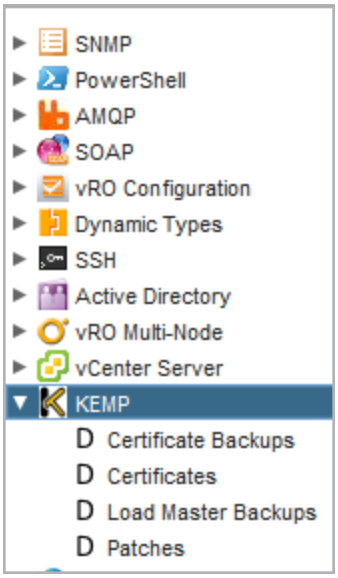
3 Using the Kemp Orchestrator Plugin

3.1 Inventory

There is an **Inventory** section in Orchestrator which will list any LoadMasters that have been added to Orchestrator. There are also a number of Kemp directories which are created when the Kemp Orchestrator plugin is installed. To view these, follow the steps below:

1. Select the **Run** mode from the drop-down in the top-left.

2. Select the **Inventory** tab (icon of a jigsaw puzzle piece with a page behind it).



When any Kemp files are uploaded to the Orchestrator, for example certificate or patch files, Kemp recommends saving those files in the relevant Kemp directories. The certificate and LoadMaster backups will automatically save into the relevant directories when the related workflows are run.

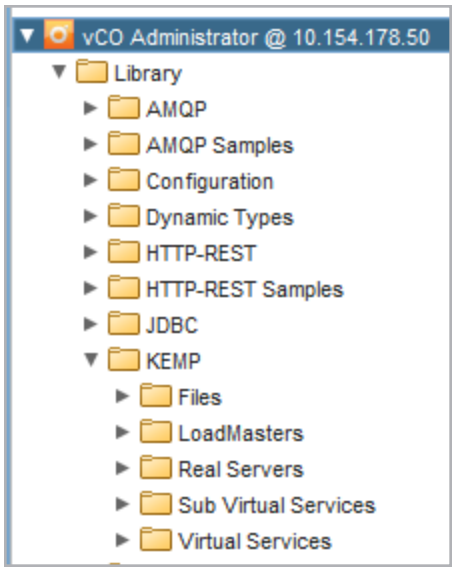
3.2 Workflows

After the plugin has been installed, a number of Kemp workflows will be available. These workflows can be used to perform various tasks in the LoadMaster.

The workflows can be accessed by following the steps below:

1. Select the **Run** mode from the drop-down in the top-left.

2. Select the **Workflows** tab (blue icon).



3. Expand the **Library** directory.

4. Expand the **Kemp** directory.

5. Each of the sub-directories within the **Kemp** directory contain various workflows that can be run. To run a workflow:

a) Expand the relevant directory.

b) Select the relevant workflow.

c) Click the green play icon (Start workflow) in the top-left.

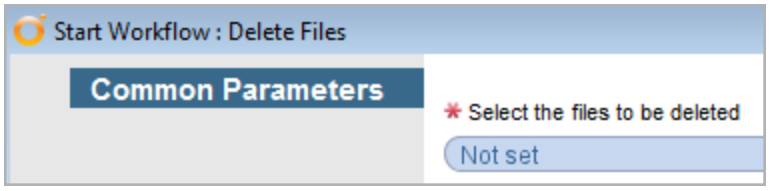
d) A screen will then appear which will contain relevant fields relating to that workflow. Fill out the fields and click Submit.

The steps to run each of the workflows are the same, but the fields that appear on each of the screens will differ. Refer to the sections below for more information. The section names correspond to the directory names in Orchestrator.

3.3 Files

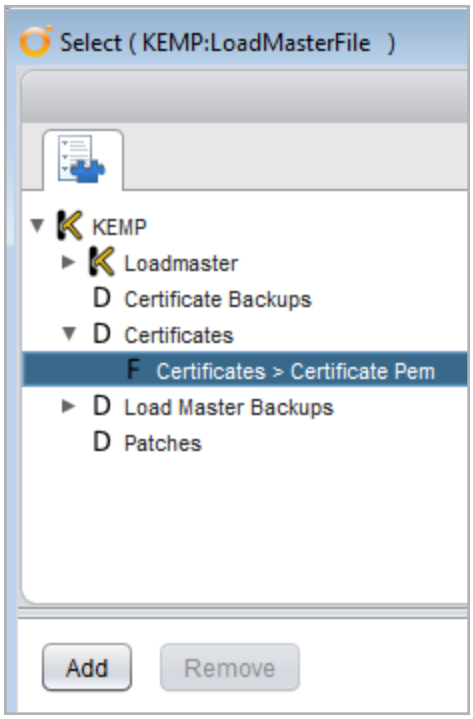
Files can be uploaded to and deleted from Orchestrator. For further details, refer to the sections below:

3.3.1 Delete Files

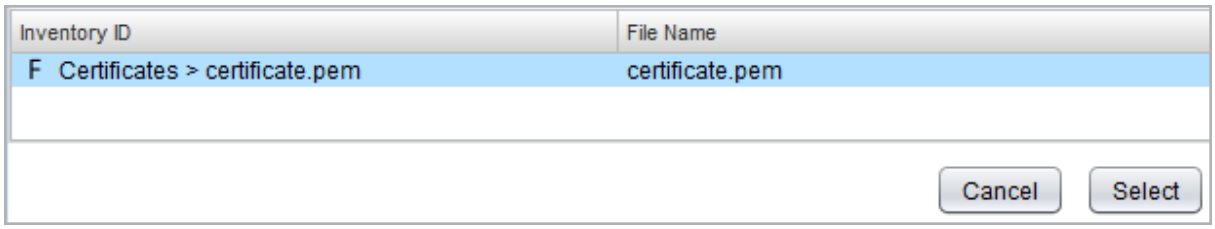


1. Click **Not set**.

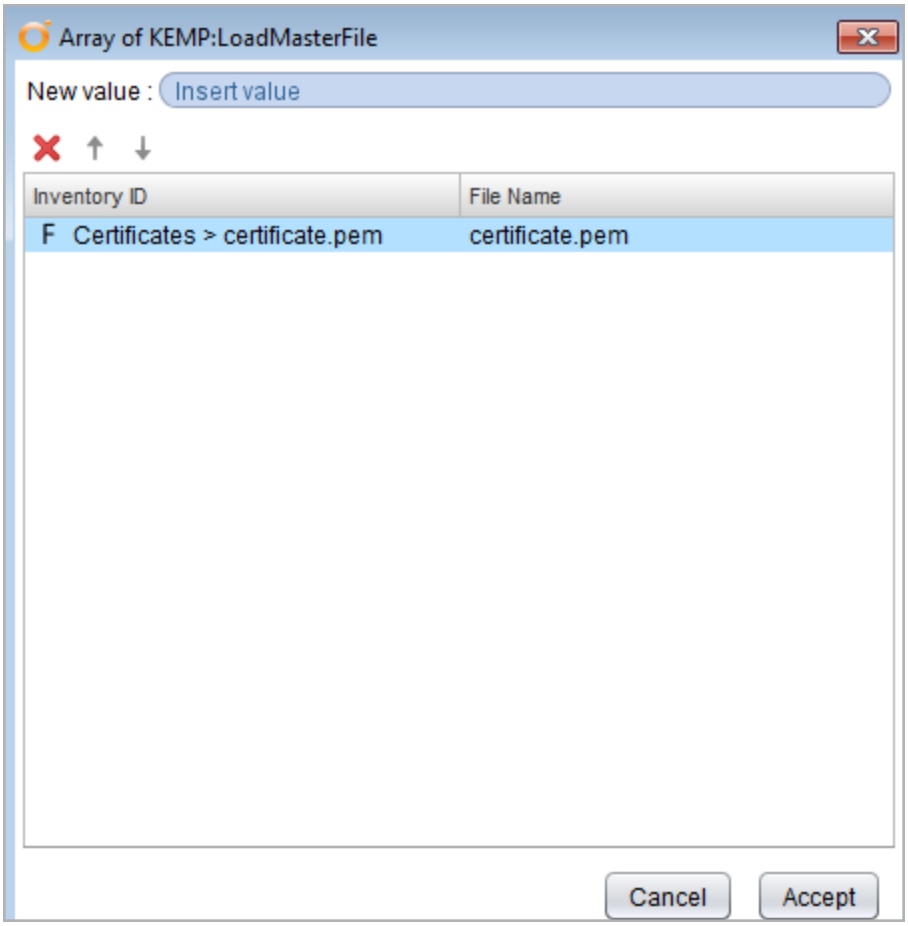
2. Click **Insert value**.



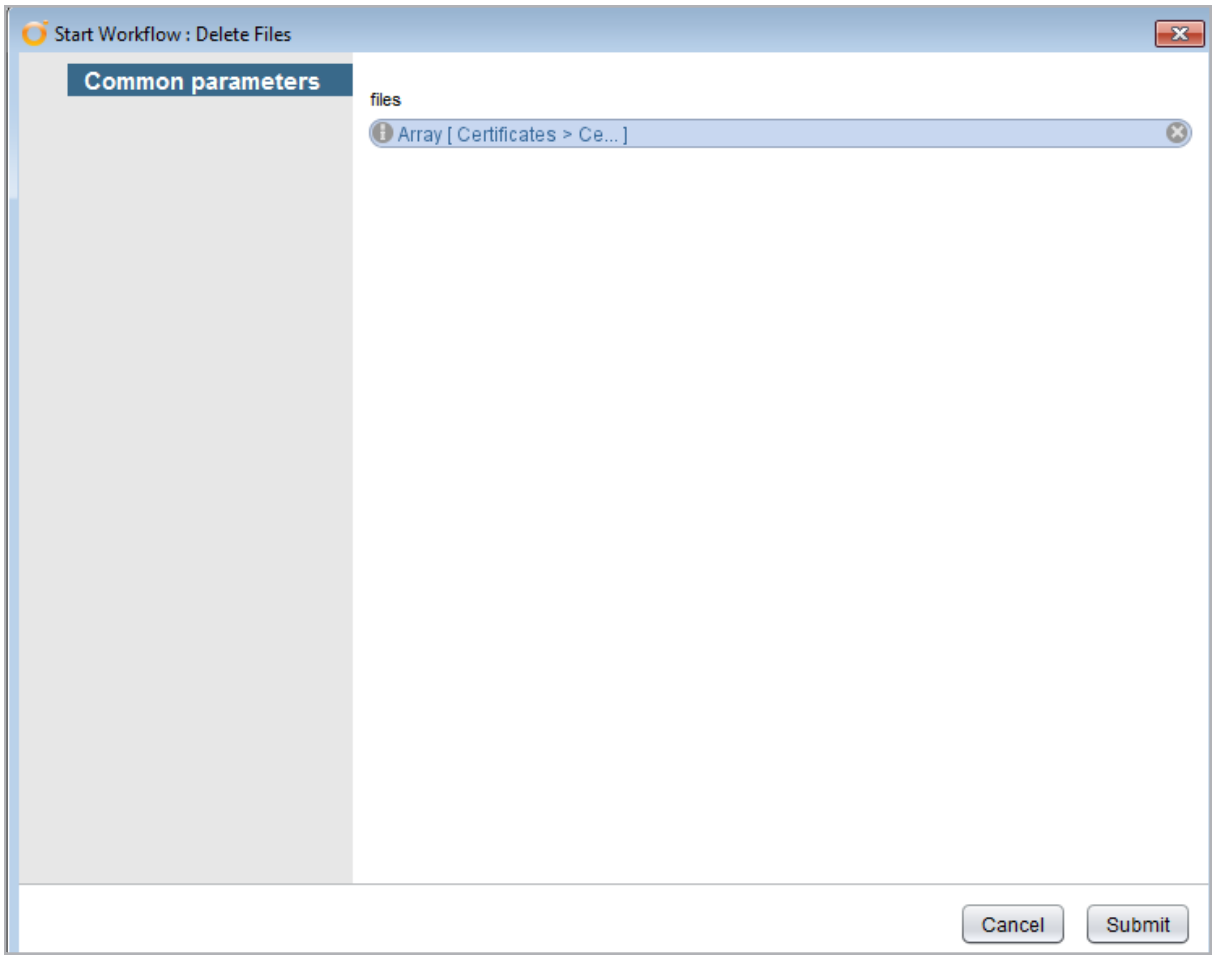
3. Expand the **Kemp** directory.
4. Expand the relevant directory where the file is located.
5. Select the relevant file to be deleted.
6. Click **Add**.



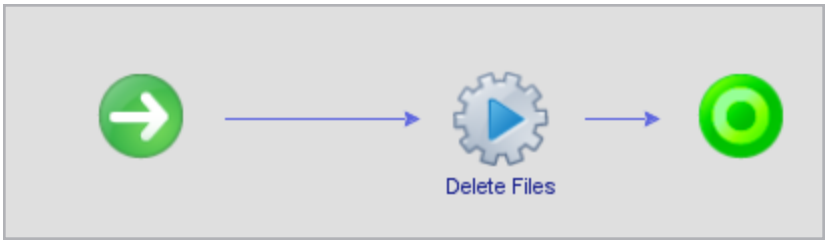
7. Click **Select**.



8. Click **Accept**.

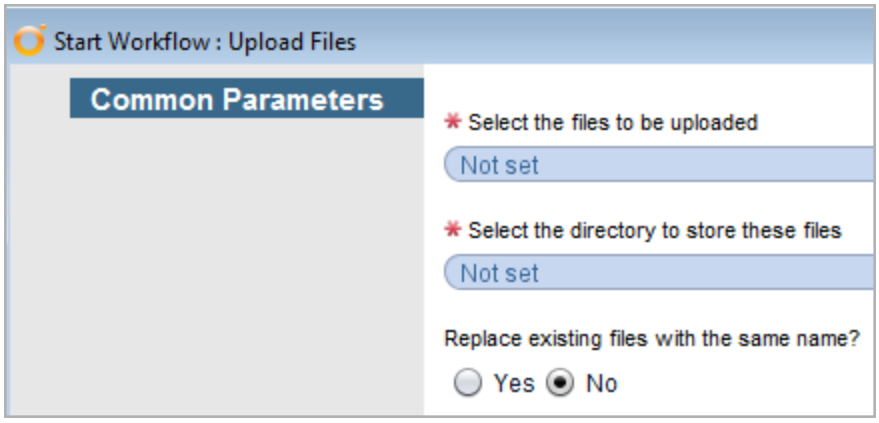


9. Click **Submit**.



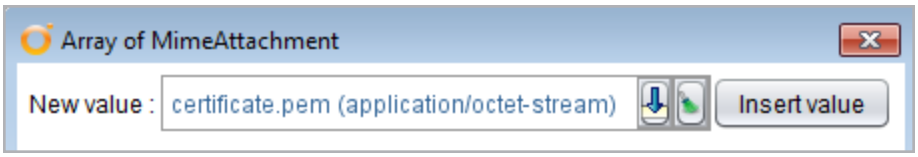
10. Wait for the deletion to complete.

3.3.2 Upload Files



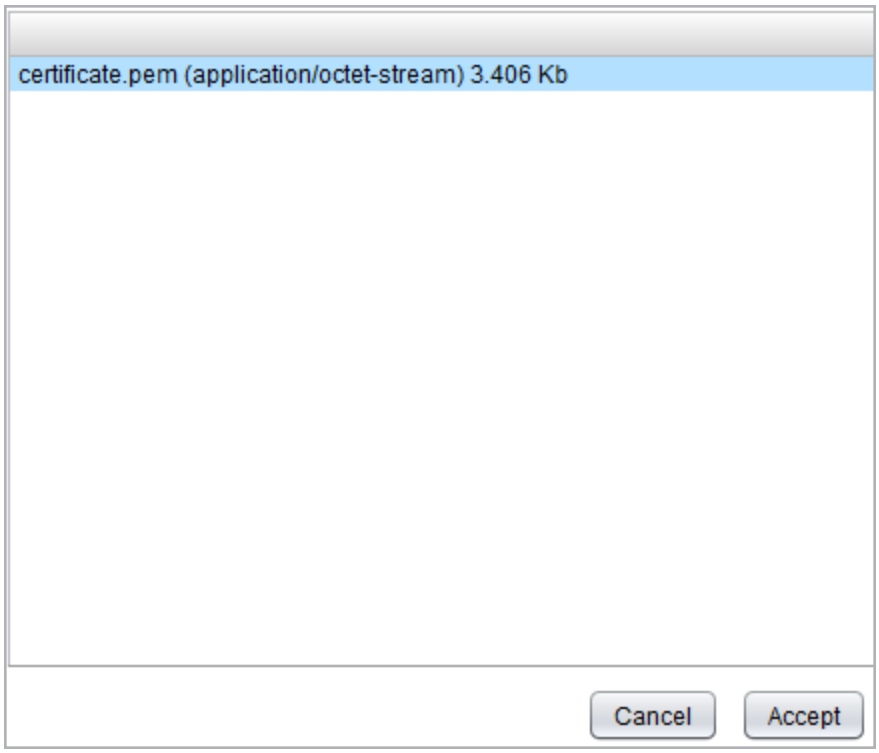
1. Click **Not set** in the **Select files to be uploaded** field.

2. Click **Not set**.
3. Browse to and select the relevant file to be uploaded.

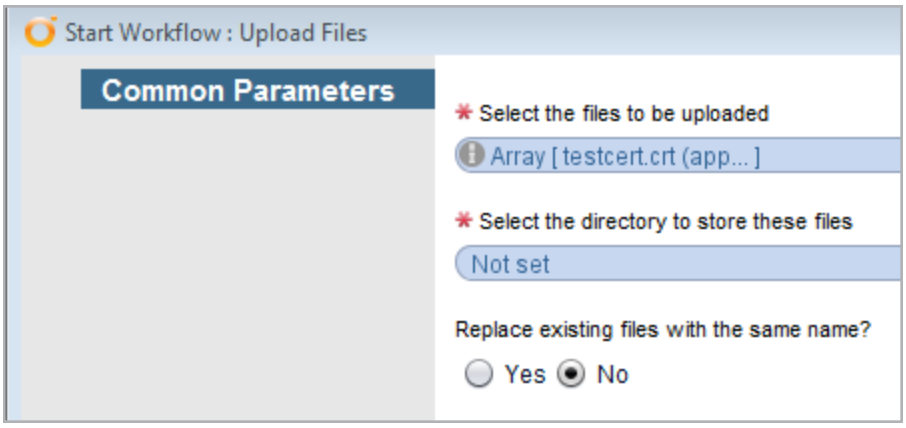


4. Click **Insert value**.

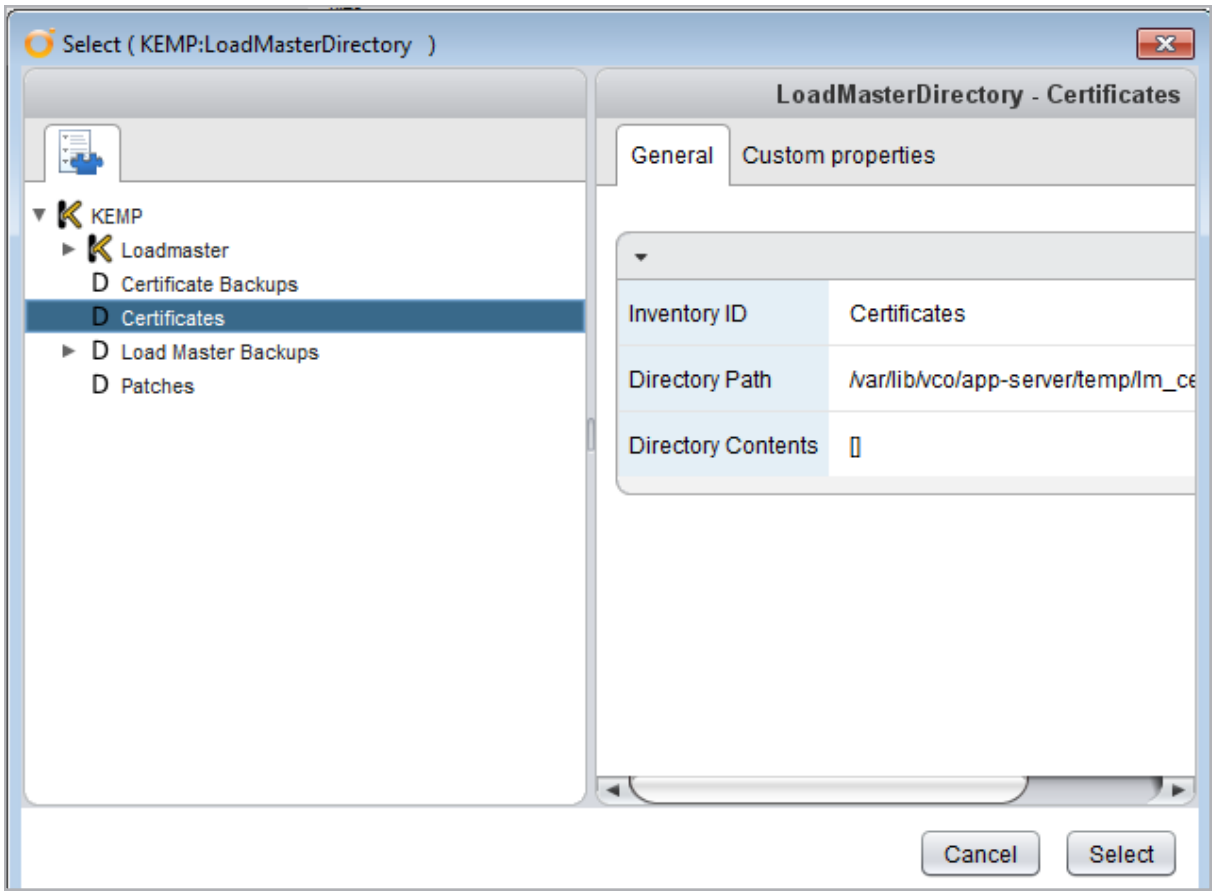
> Multiple files can be uploaded at the same time, if needed. Simply browse to and select another file and click **Insert value** to add it to the list of files to be uploaded.



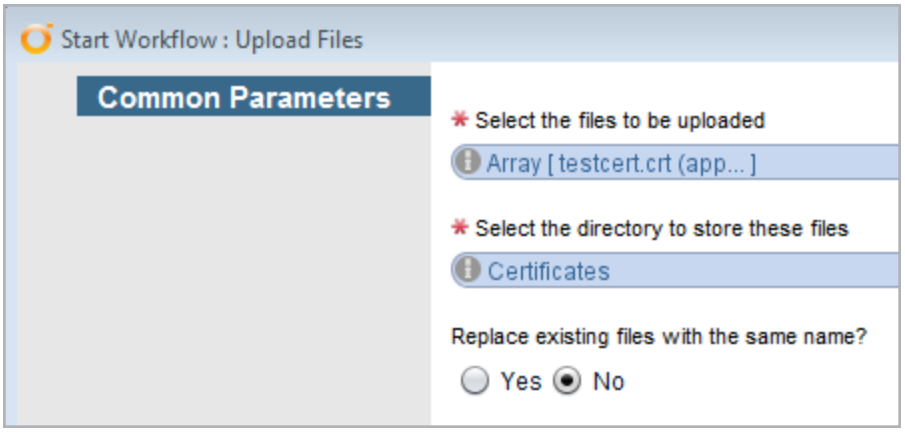
5. Click **Accept**.



6. Click **Not set** in the **Select the directory to store these files** field.

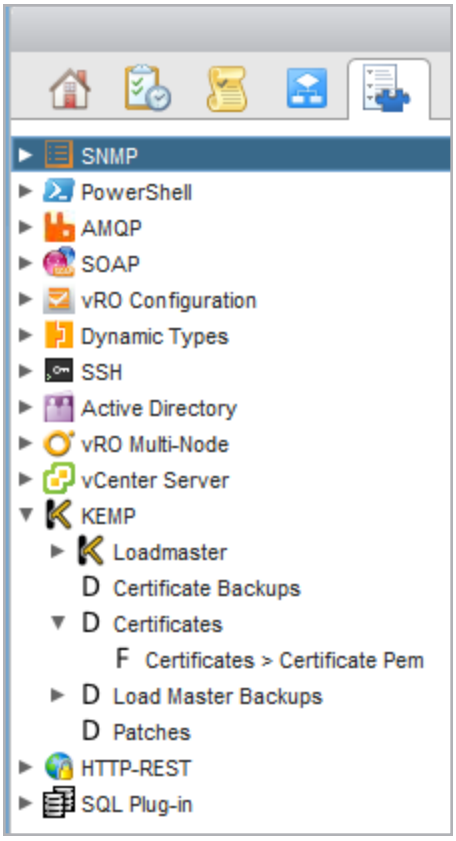


7. Expand the **Kemp** directory.
8. Select the relevant directory to store the file in.
9. Click **Select**.



10. If you want to replace an existing file of the same name, select **Yes**.

11. Click **Submit** to upload.



The file will then be visible in the **Inventory** tab in the relevant directory.

3.3.2.1 Uploading Files which are Bigger than 2MB

There is a limit of 2MB on the file sizes that can be uploaded via the Kemp Orchestrator plugin. This means that firmware upgrade patch files are not able to be uploaded using the method listed in the section above. This section outlines a workaround that can be used to upload files greater than 2MB in size.

The following are valid LoadMaster directories on the Orchestrator server:

- lm_config_backups
- lm_certs
- lm_certs_backups
- lm_patches

You can use a number of options to copy/download the file to the Orchestrator Server. Two of the options - using SCP or using cURL, are outlined below.

3.3.2.1.1 Using SCP to Copy a File to the Orchestrator Server

This process requires SSH access to be enabled when deploying the Orchestrator appliance. Follow the steps below:

1. Navigate to the directory containing the file to transfer on the source machine.
2. Run the following command:

scp <File_To_Transfer> root@<Orchestrator_Server_IP_Address>:/var/lib/vco/app-server/temp/<LoadMaster_Directory>/<Filename>

> In order for the files to be visible in the Orchestrator client, one of the four directories listed in the **Uploading Files which are Bigger than 2MB** section must be used in place of **<LoadMaster_Directory>**.

3. After authenticating with the server, the file transfer should proceed.

3.3.2.1.2 Use cURL to Download the File

The file must then be downloaded using a cURL command:

1. Connect to the Orchestrator server via SSH.

> Unless additional users have been configured on the server, you must log in as **root**.

2. Navigate to /var/lib/vco/app-server/temp/<LoadMasterDirectory>

> Replace **<LoadMasterDirectory>** with one of the directories listed in the **Uploading Files which are Bigger than 2MB** section.

3. Invoke cURL with the **-o <Filename>** parameter to transfer the output of the command to a file, for example:

curl -u user:password -o <NewFilename> <URL>/<File_To_Download>

3.3.2.1.3 Configuring Permissions

After the file has been successfully transferred, the permissions of the file must be modified in order for it to be accessible to the Orchestrator client. To modify the permissions, run the following command:

chown vco <FileName>

> If this step is not performed, the files in question will not be visible in the Orchestrator client.

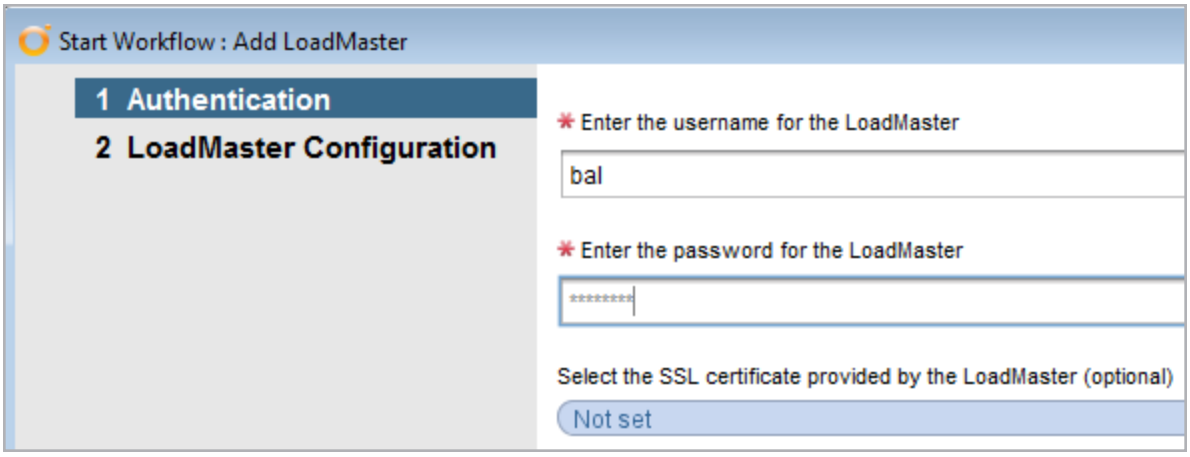
3.4 LoadMasters

In the **LoadMasters** directory, there are a number of workflows that can be executed which relate to managing LoadMasters, such as adding and removing LoadMasters from Orchestrator. For details on each of the LoadMaster workflows, refer to the sections below.

Before any of the other LoadMaster workflows can be run on a LoadMaster, the relevant LoadMaster needs to be added to Orchestrator. The first section below provides details on the **Add LoadMaster** workflow.

3.4.1 Add LoadMaster

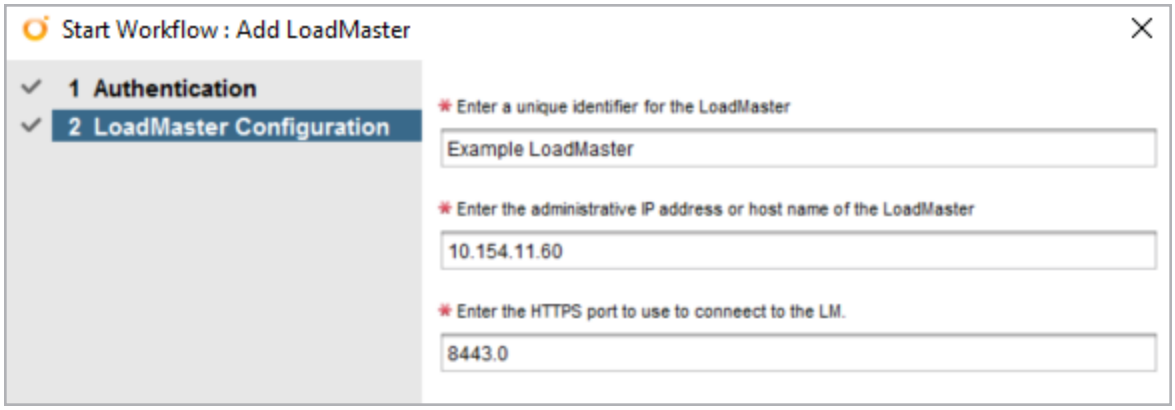
A LoadMaster can be added to Orchestrator using the **Add LoadMaster** workflow. A LoadMaster must be added to Orchestrator before any workflows can be run on that LoadMaster.



1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

3. Click **LoadMaster Configuration**.



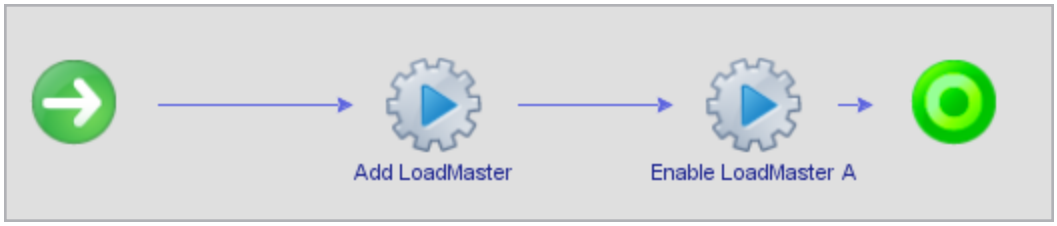
4. Enter a recognizable name in the **Enter a unique identifier for the LoadMaster** text box. This is a friendly name for the LoadMaster, which appears in Orchestrator.

5. Enter the IP address of the LoadMaster to be added.

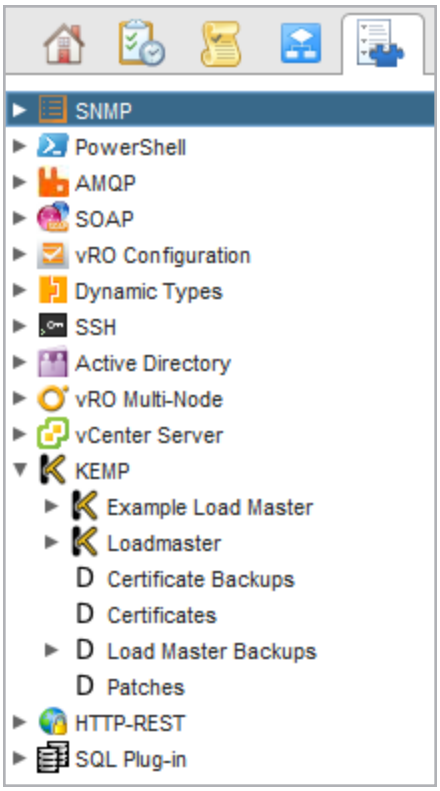
6. Enter the HTTPS port to use to connect to the LoadMaster.

> If you cannot see the port field, you may need to install the latest Kemp package. To do this, select the **Administer** option from the drop-down at the top, go to the **Packages** tab on the left, select the **com.kemptechnologies** package, click the **Import package** icon and import the latest Kemp package. Both the .dar and the .package files must be updated. The latest Kemp package is available on the Kemp website.

7. Click **Submit**.



8. Wait for the LoadMaster to be added.



The LoadMaster will then be listed in the **Kemp** directory in the **Inventory** tab.

3.4.2 Add Certificate

Before uploading a certificate to the LoadMaster, the certificate file must first be uploaded to Orchestrator. For step-by-step instructions on how to upload a file, refer to the **Upload Files** section.

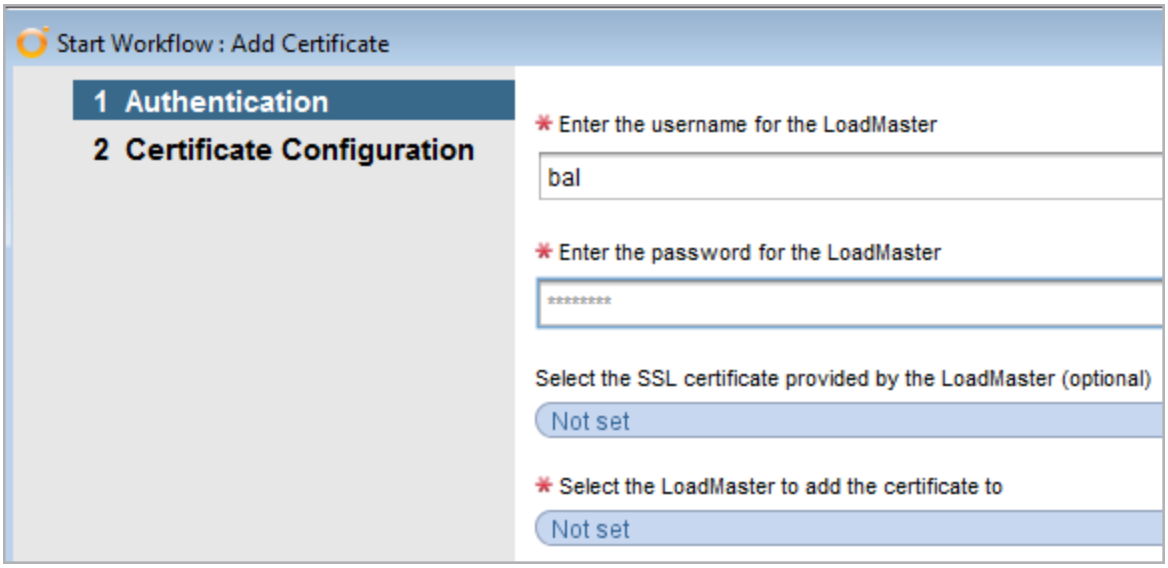
testcert.crt

```
-----BEGIN CERTIFICATE-----
MIICyzCCAjQCCQD9Zrq+3HKfJDANBgkqhkiG9w0BAQsFADCBqTELMAkGA1UEBhMC
SUUxEDAOBgNVBAgMB011bnN0ZXIxETAPBgNVBAcMCExpbWVyaWNrMRowGAYDVQQK
DBFLRU1QIFRlY2hub2xvZ2llczEcMBoGA1UECwwTUHJvZHVjdCBEZXZlbG9wbWVu
dDEOMAwGA1UEAwwFamFtZXMxKzApBgkqhkiG9w0BCQEWHGpvYnJpZW5Aa2VtcHRl
Y2hub2xvZ2llcy5jb20wHhcNMTUwNzI4MTU1MTQ4WhcNMTYwNzI3MTU1MTQ4WjCB
qTELMAkGA1UEBhMCSUUxEDAOBgNVBAgMB011bnN0ZXIxETAPBgNVBAcMCExpbWVy
aWNrMRowGAYDVQQKDBFLRU1QIFRlY2hub2xvZ2llczEcMBoGA1UECwwTUHJvZHVj
dCBEZXZlbG9wbWVudDEOMAwGA1UEAwwFamFtZXMxKzApBgkqhkiG9w0BCQEWHGpv
YnJpZW5Aa2VtcHRlY2hub2xvZ2llcy5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAPZyfvEy+JeX4JT336h3IZqd022E8jsSMShZazcuI/GICrBbAGowhBtf
kVoESNpq7PsyaQR0PYfqJii41HUwqJo/Wr/8ulBoewYzoLAGzYfpAe6Rax+lKTc7
7mlKoQ3zheBk9Hj3fw1RToSgU9F5oiQJT3jT6zprt0sFuBp+UC8JAgMBAAEwDQYJ
KoZIhvcNAQELBQADgYEAeoGA22dXIVAIZ0G8uYOne/KOg7QhV+RXlB6a9j5lQW6E
H72GzQaI3K1lTgkP/UKUTCTjQgVw+4tHx3eU+7Dq9BXA4fx30bvgfONCxBHG8eXy
N6gw8BAapDftliwRCklZjBjRtdpP+G8kk7OmPh2ZZOvCY4ylSeWZPDgLcy0tYsw=
-----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,59951F4DADCDF43D

/8x45hW4xrUpX6eDalZfNDFVN8AUx+saxRYnRYvPSuic463o5UhxRUXi+TUE6eeF
CqOB5k5ZeFn2n7x45AHRX1auVGvt4g6oaFZH+GXPvdWCSQWEsZTrcQp7KCXy7zth
+rn5qsFVqCIxsfdw2ZEV4intoysSj89Fxbqqs8BME9WETCu2w7NN2lBS6ji3fv/f
uMSS/cOOUv2jPCpMAvaDGmqCKtOy8dKfJlySKhWFacOCjdGyU7uw+SrP/IpzljBV
YWyyxmxSXzmRdsN2d0L1Az8L3h921amHIRCmXs8Hc2vNGDnN9zdJ+SF3vKs256FN
OvmScty9zs362nl+nUWTPSqFhDsb6bWY7hMJMARGVTfi/Qjw75XoEQpj0jdDy4oq
hCvsliAwU+FC9I1j+bKUU4z3J7CSEkFdtJk4iRsfzk9oGC8gdj6zOfsV090SyIQs
2RxKXo1U0RrsAwmYdpQPK5TRLWDnyyIajsHjI2fH3wHOPcwTIlWkv+VzOC1ohKzK
dExxW6GAoUgDbbsLuqT4y93x9E+IWAlOBpJ4Z5s4LKkyaiD0jzSvP5OG+Mo17+jg
dcKvyJcWuXqs6wI7m/hIeS4GhhqlJjDiuARX60Ws3NcyX4ntWXq8edx1PXvR2+cW
oesvuxzqFBncwgnBw01jryWt+7u8TIuOQVUjJlMtaeSYifjofKPP3c/Xud0FE8ck
1SEKK+wDTQp8/j7iDxkfyzlh0Ti+NneY2TLsIF+YhLqSvbu2rHkITEBn6PLiTH5k
V789ENrdQJU50b+riVKyzZhh2YsWuD3xWK/5RAT83FSi5+N37PQIMA==
-----END RSA PRIVATE KEY-----
```

When uploading a certificate file via Orchestrator (or via the Kemp API), both the certificate and key must be concatenated into the one file. The certificate file must be listed on top, followed by the private key at the bottom - this is the format which is required by the API which is what the Kemp Orchestrator plugin is based upon. An example file is shown in the screenshot above.

After a certificate file has been uploaded to Orchestrator, it can then be uploaded to the LoadMaster using the **Add Certificate** workflow.

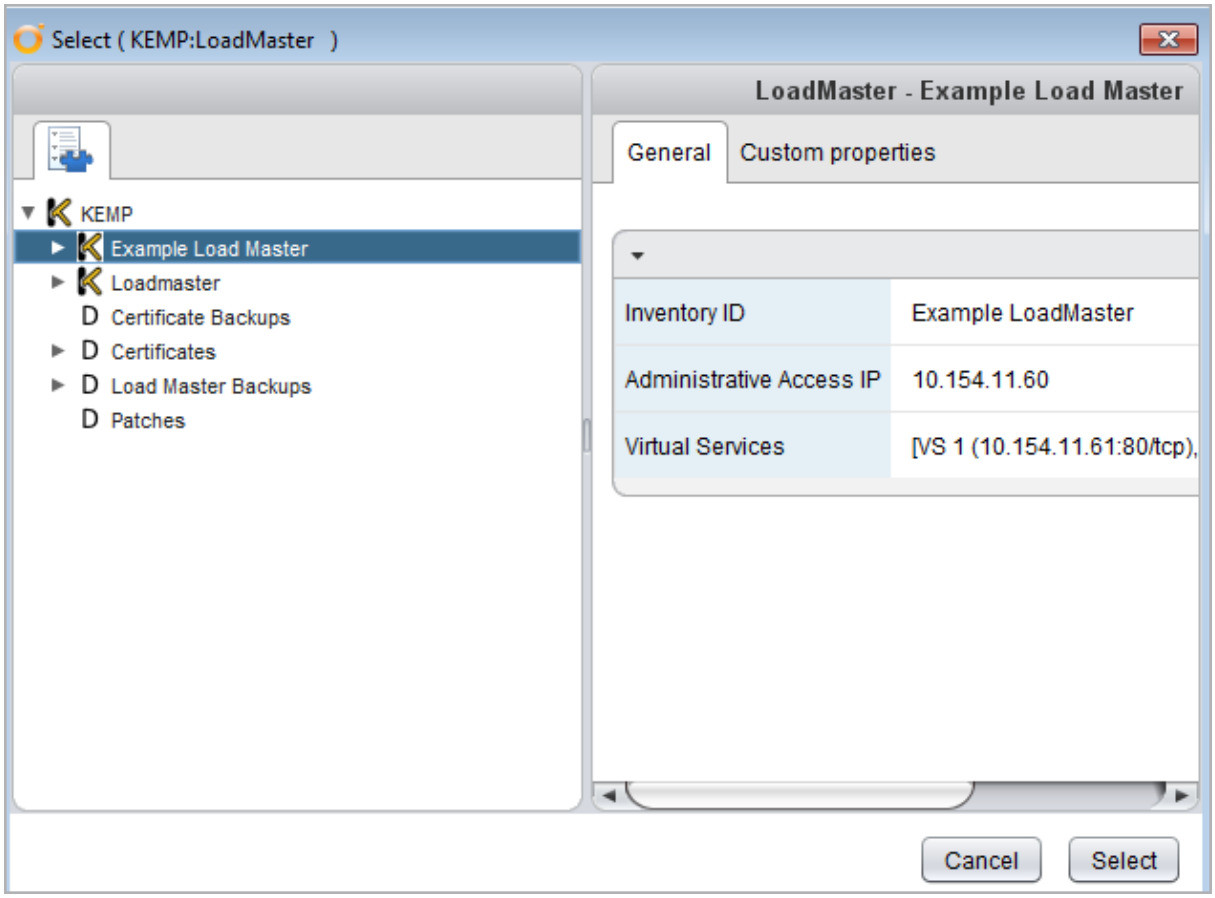


1. Enter the username and password to access the LoadMaster.

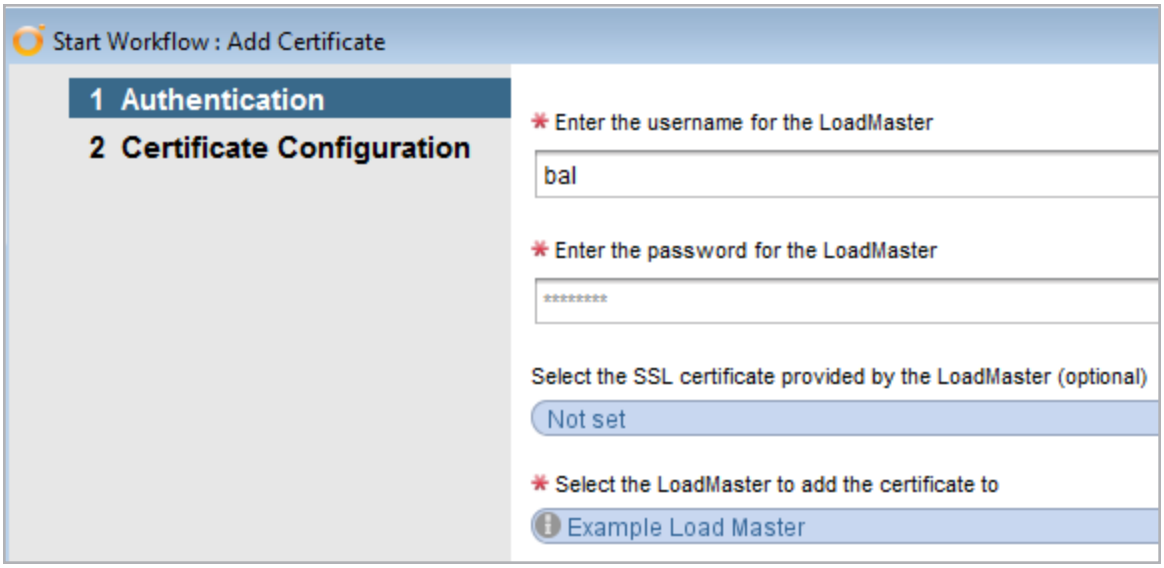
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

> This is the certificate file used to authenticate to the LoadMaster - this is not the field used to upload a new certificate.

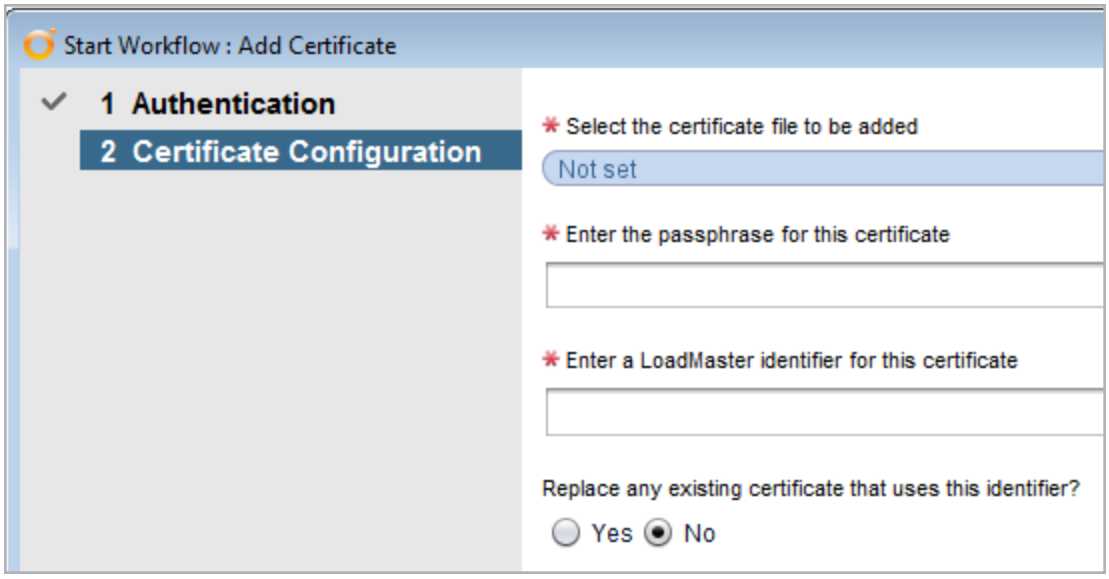
3. Click **Not set** in the **Select the LoadMaster to add the certificate to** field.



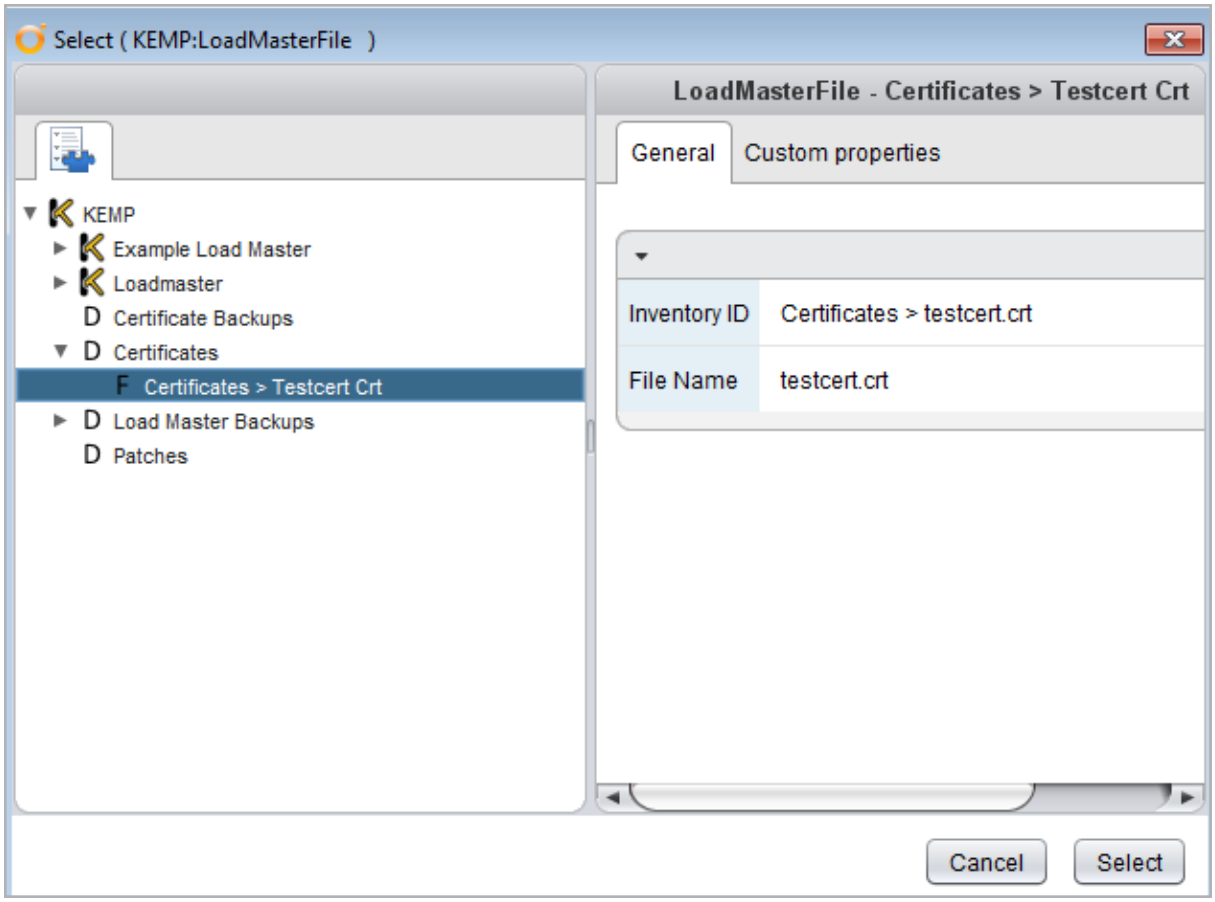
4. Expand the **Kemp** directory.
5. Select the relevant LoadMaster.
6. Click **Select**.



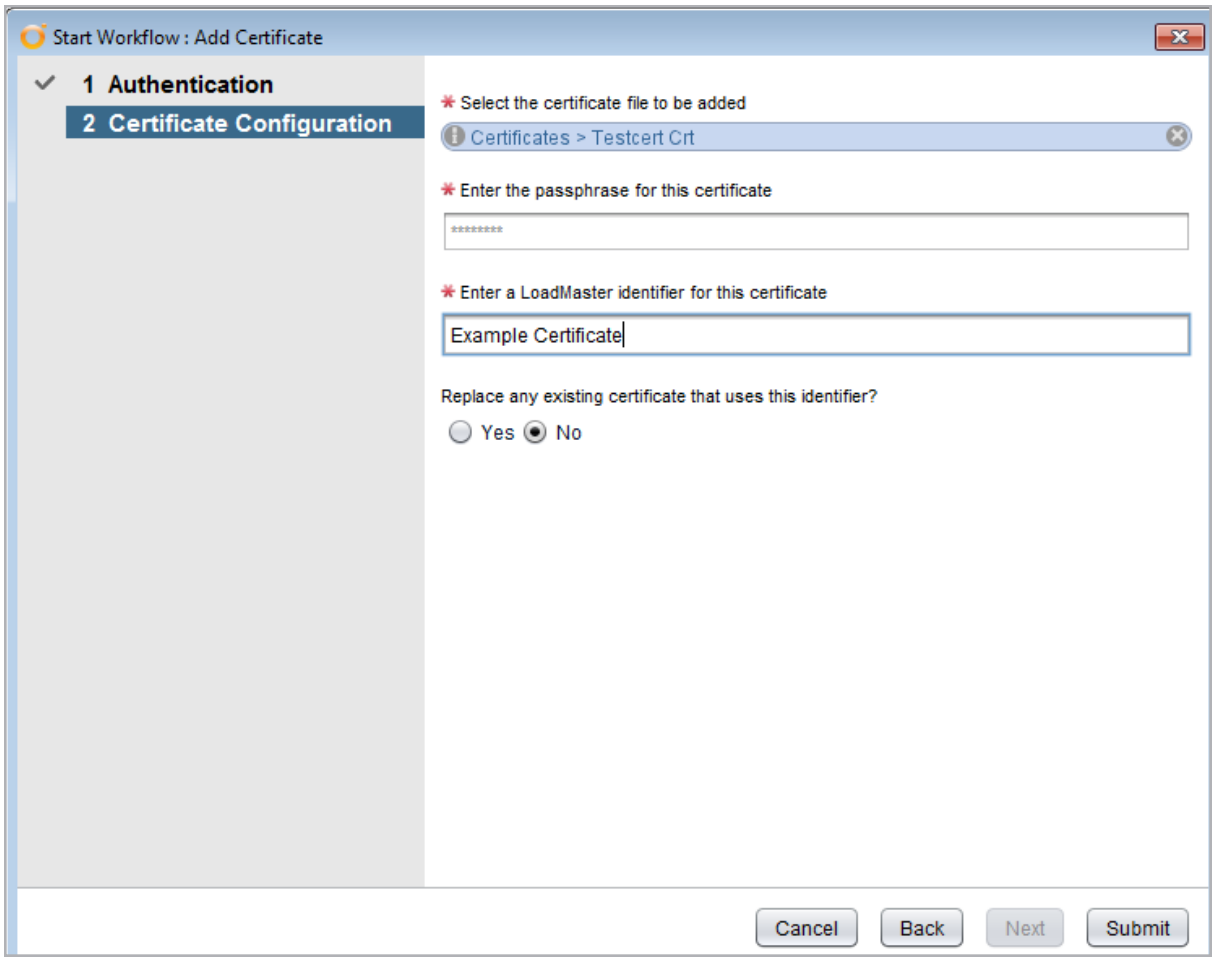
7. Click **Certificate Configuration**.



8. Click **Not set**.



9. Expand the **Kemp** directory.
10. Expand the **Certificates** directory.
11. Select the relevant certificate.
12. Click **Select**.



13. Enter the passphrase which was used when creating the certificate in the **Enter the passphrase for this certificate** text box.

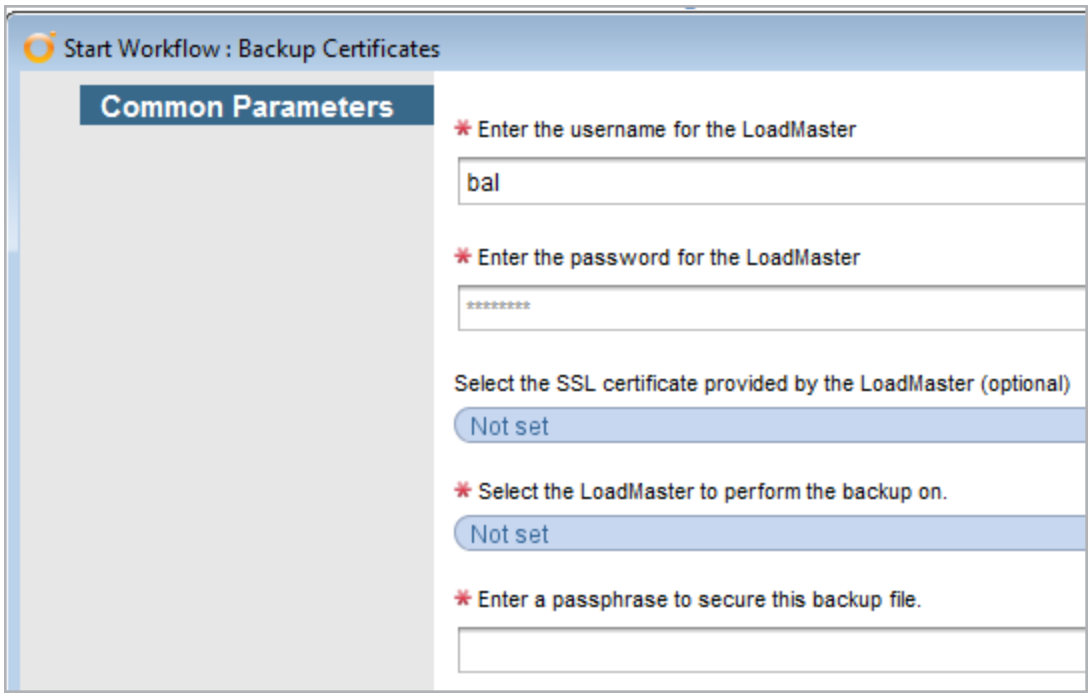
14. Enter a recognizable name for the certificate in the **Enter a LoadMaster identifier for this certificate** text box. This is a friendly name for the certificate which will be displayed in the LoadMaster.

15. If replacing an existing certificate of the same name, select **Yes**.

16. Click **Submit**.

3.4.3 Backup Certificates

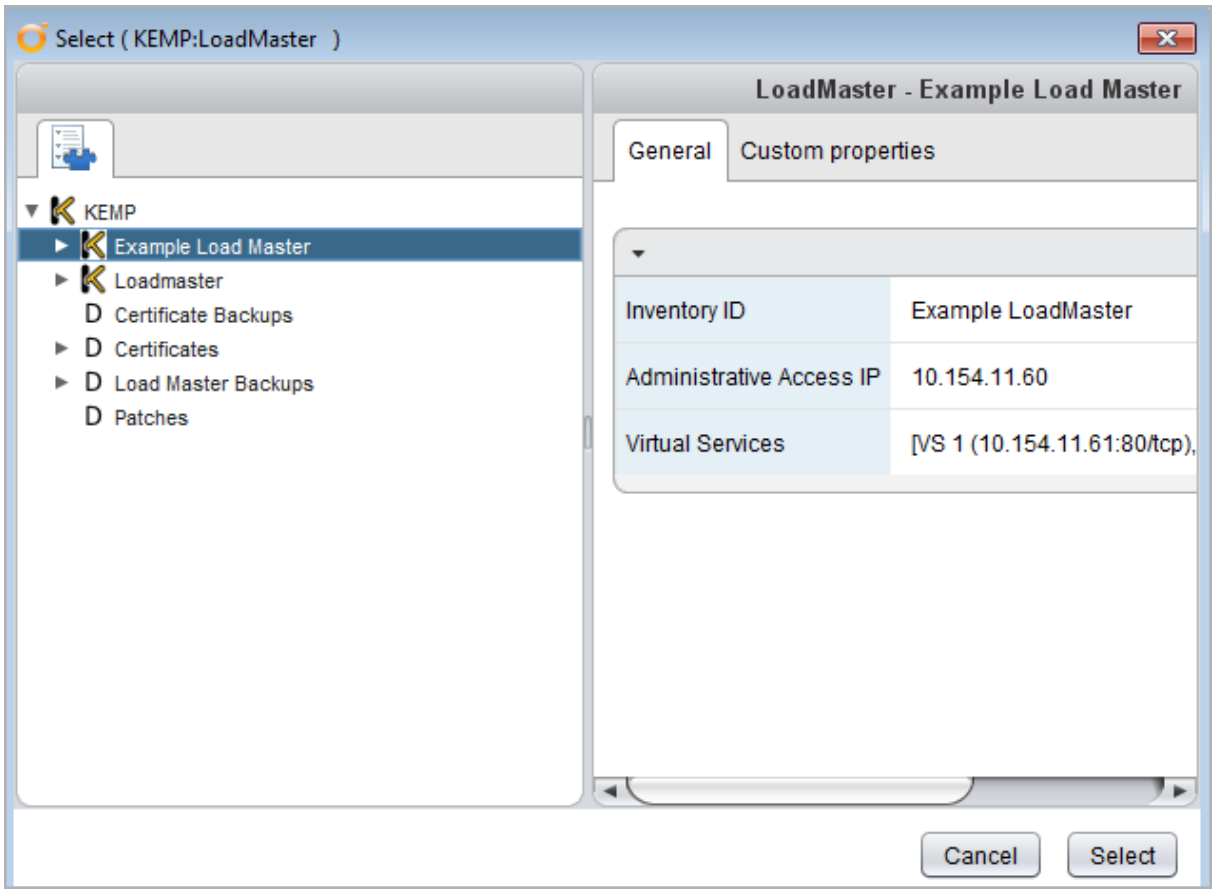
The certificates on a LoadMaster can be backed up via Orchestrator. To do this, run the **Backup Certificates** workflow.



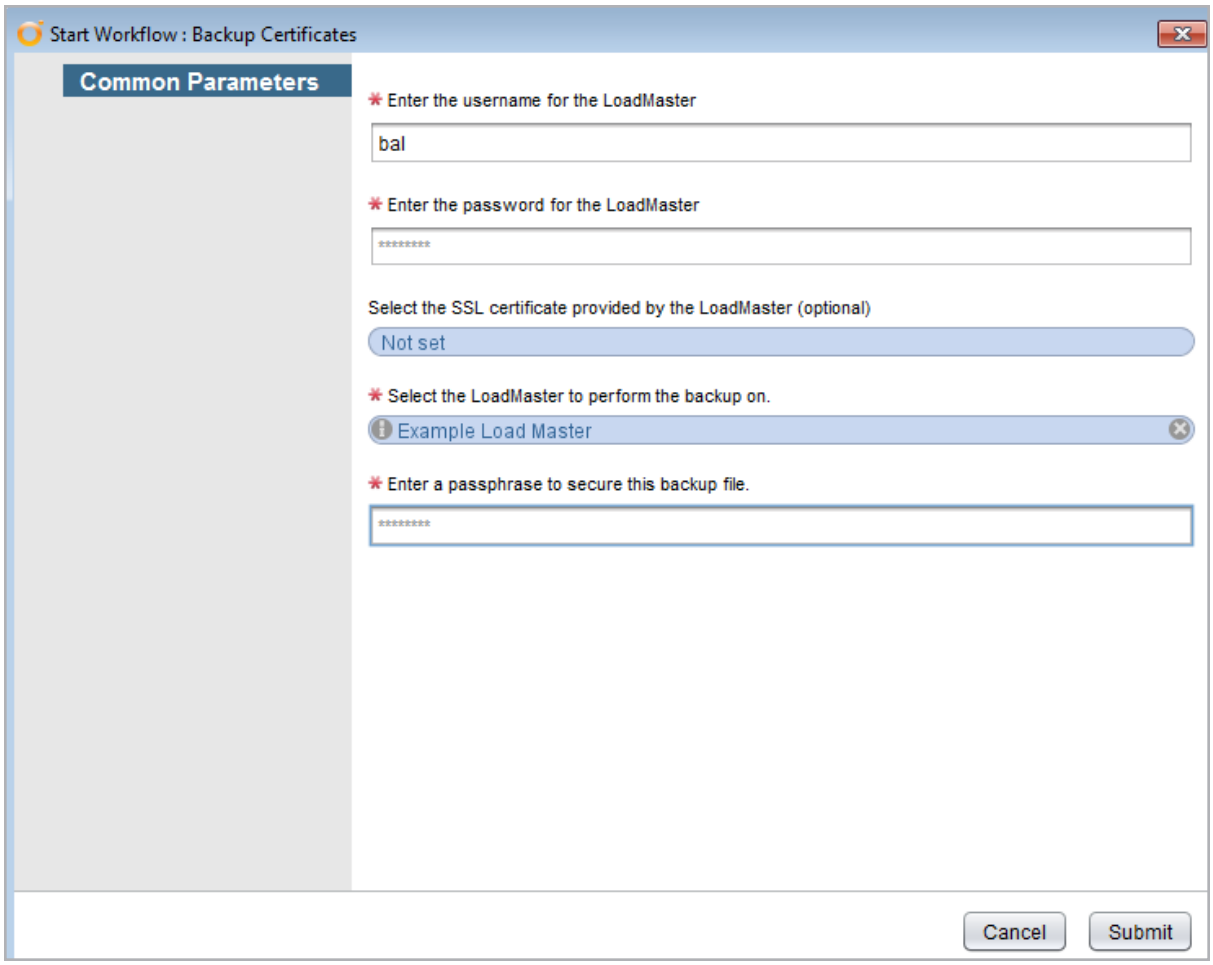
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

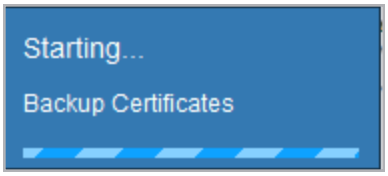
3. Click **Not set** in the **Select the LoadMaster to perform the backup on** field.



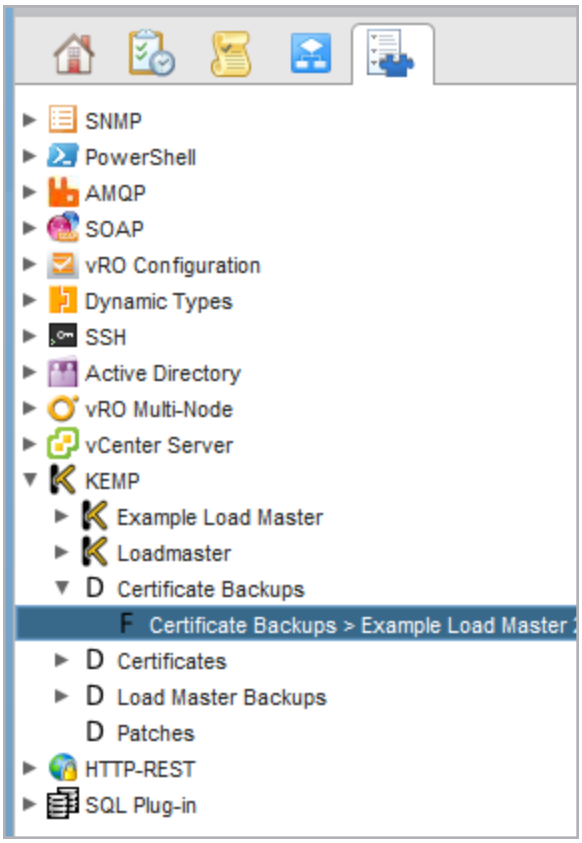
4. Expand the **Kemp** directory.
5. Select the relevant LoadMaster.
6. Click **Select**.



7. Enter a passphrase to secure this backup file.
8. Click **Submit**.



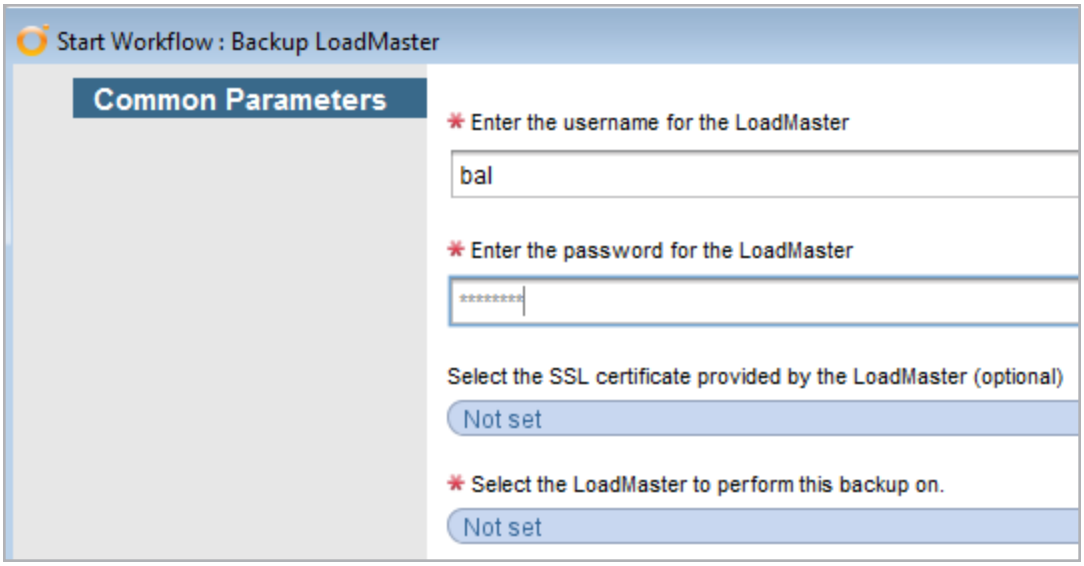
9. Wait for the backup to complete.



The backup will be saved to the **LoadMaster Backups** directory in the **Inventory** tab.

3.4.4 Backup LoadMaster

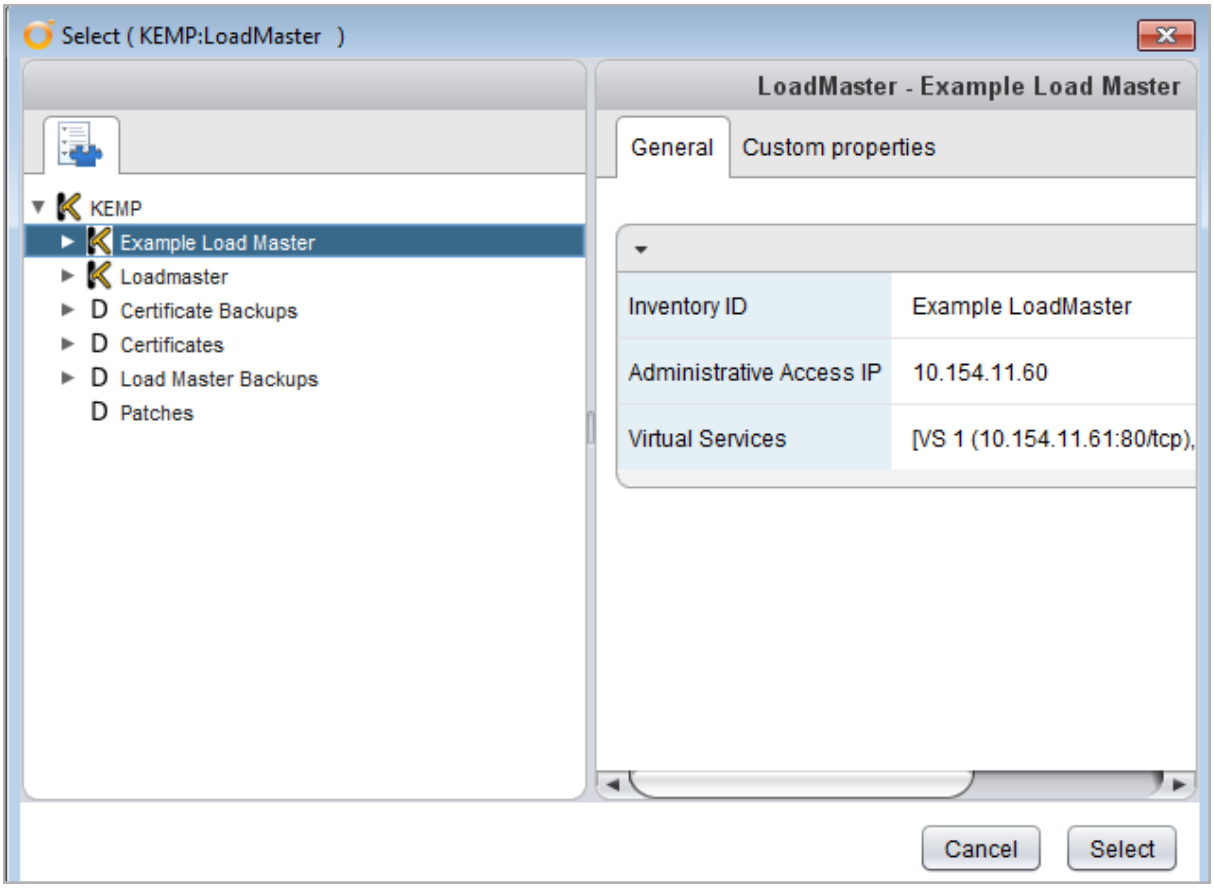
The LoadMaster configuration can be backed up via Orchestrator. To do this, run the **Backup LoadMaster** workflow.



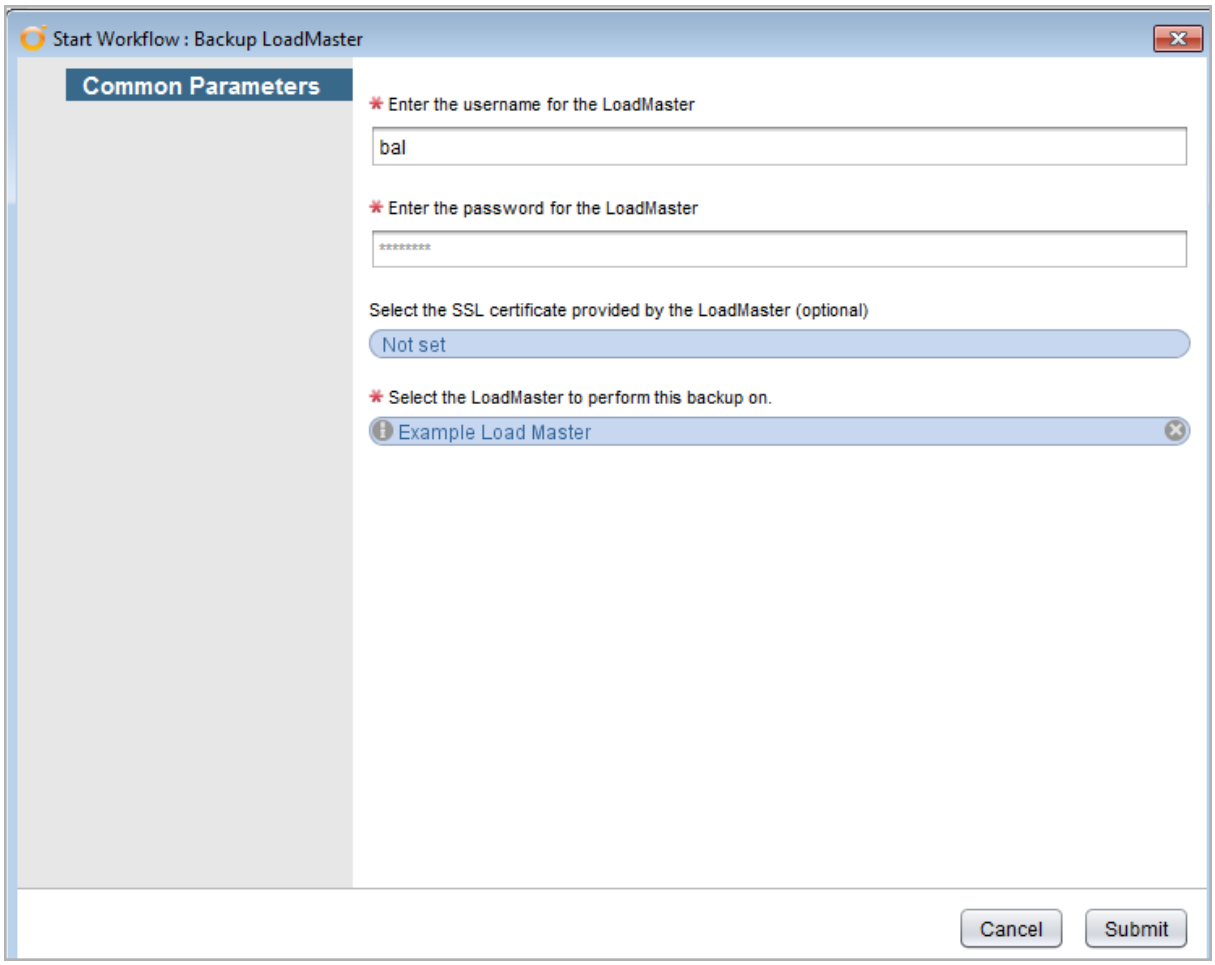
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

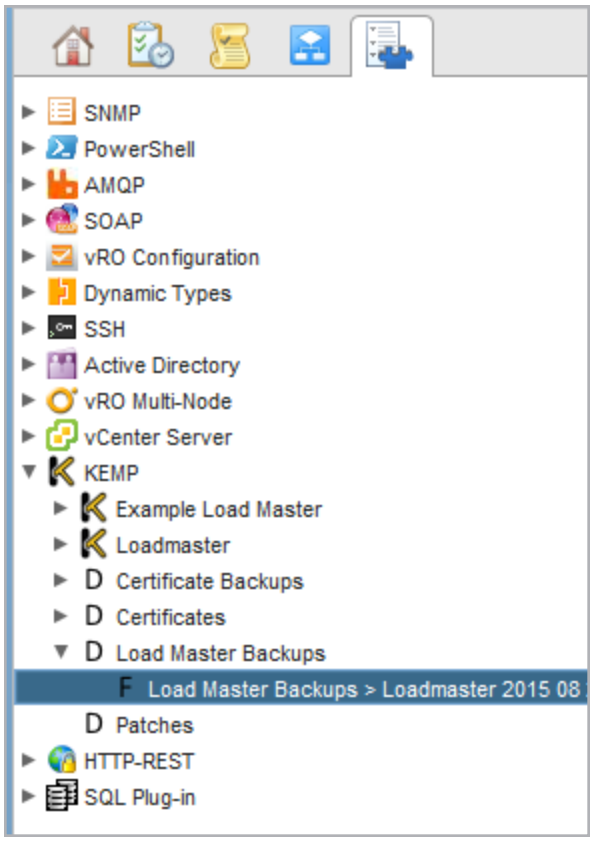
3. Click **Not set** in the **Select the LoadMaster to perform this backup on** field.



4. Expand the **Kemp** directory.
5. Select the relevant LoadMaster.
6. Click **Select**.



7. Click **Submit**.



The backup will be stored in the **LoadMaster Backups** directory in the **Inventory** tab. The backup can be restored to a LoadMaster via Orchestrator. For instructions on how to do this, refer to the **Reboot LoadMaster** section.

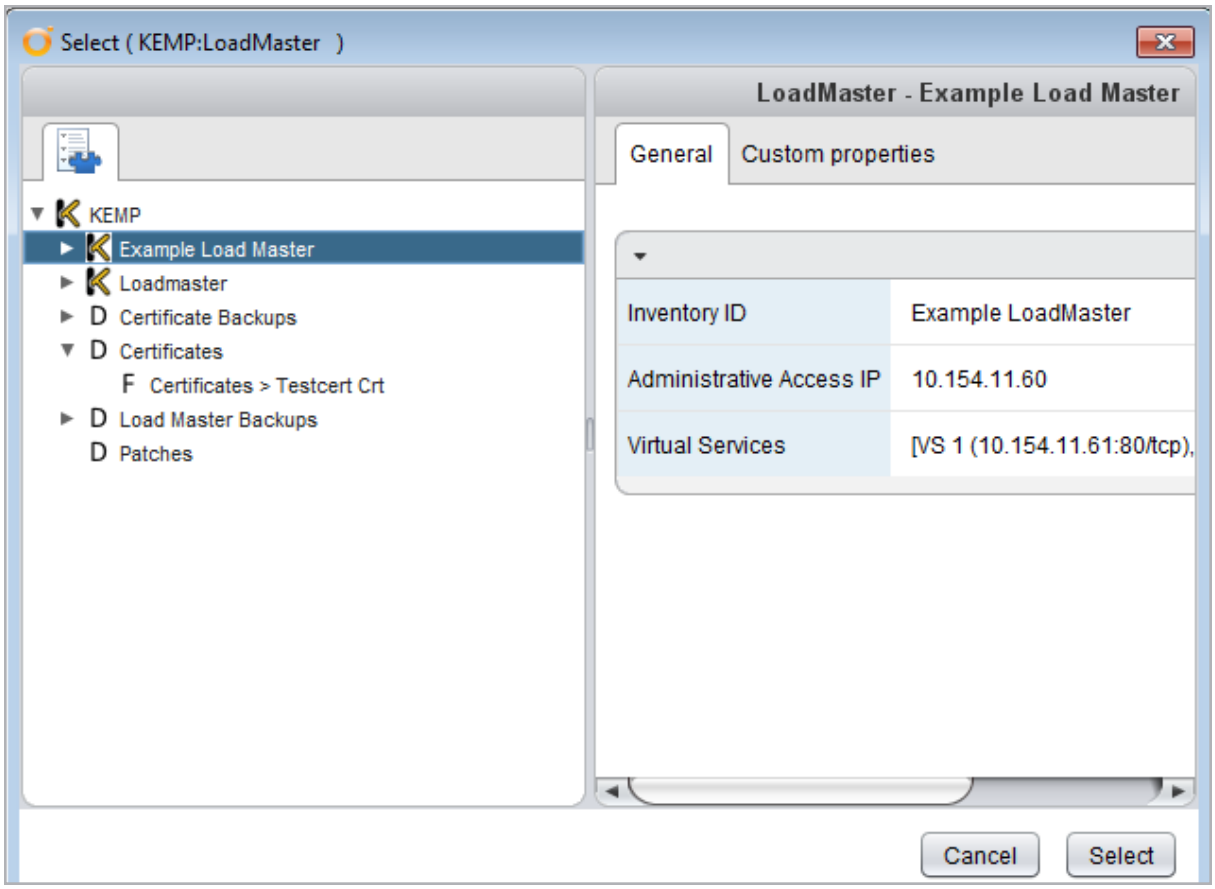
3.4.5 Delete Certificate

Certificates can be deleted from the LoadMaster by running the **Delete Certificates** workflow.

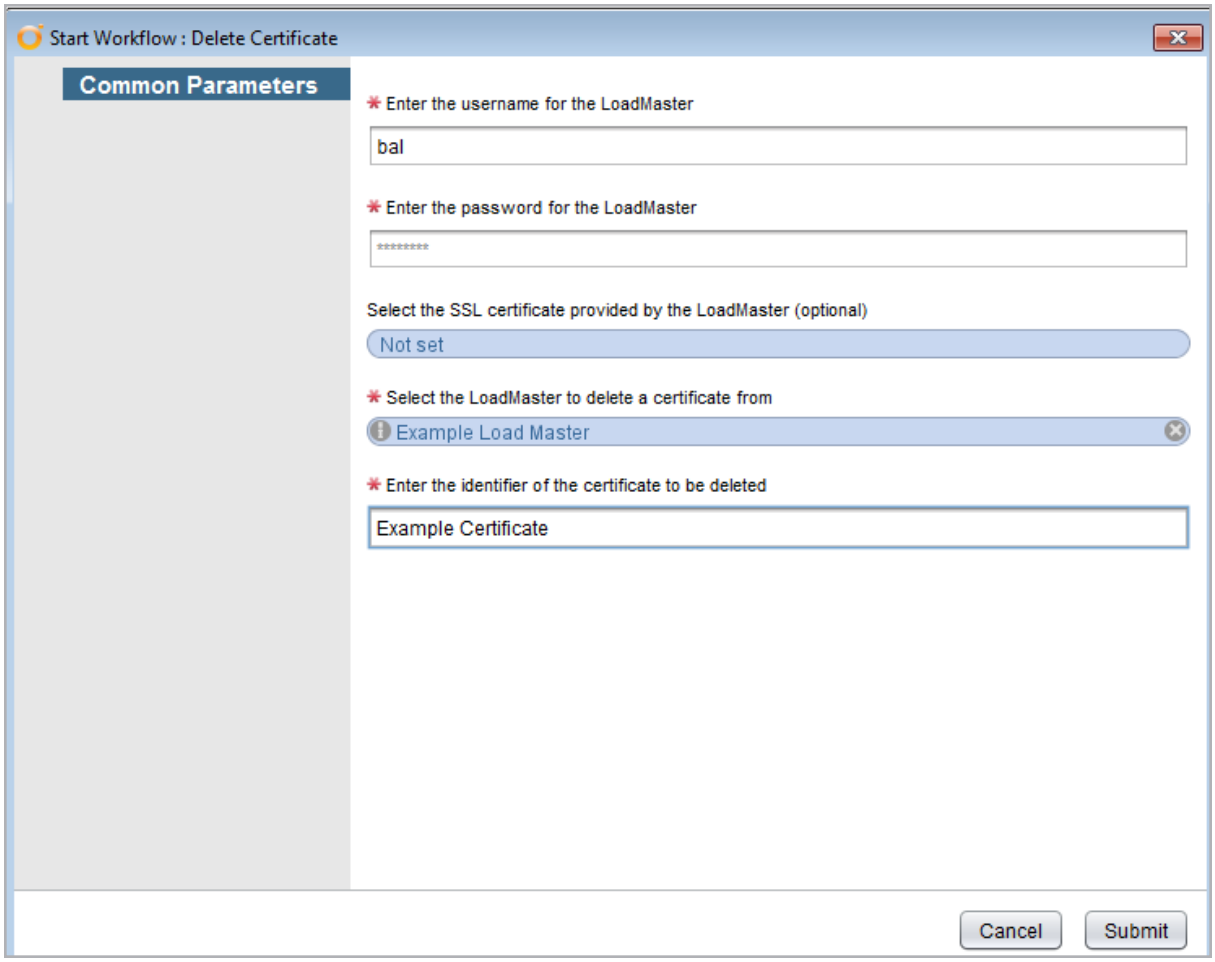
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

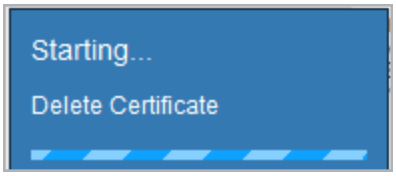
3. Click **Not set** in the **Select the LoadMaster to delete a certificate from** field.



4. Expand the **Kemp** directory.
5. Select the relevant LoadMaster.
6. Click **Select**.



7. Enter the identifier of the certificate to be deleted.
8. Click **Submit**.

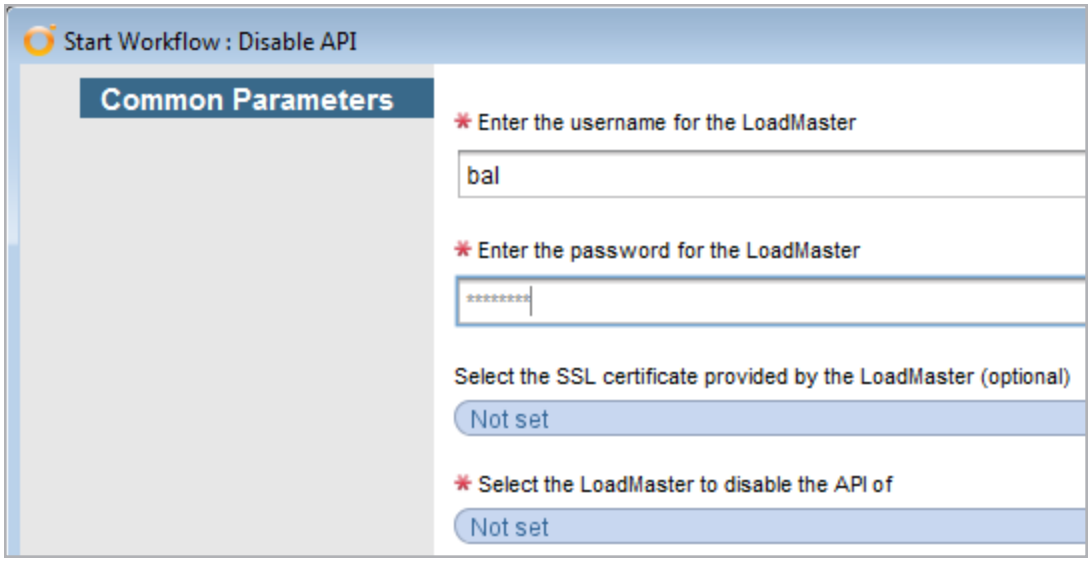


9. Wait for the deletion to finish.

3.4.6 Disable API

The API interface on the LoadMaster can be disabled via Orchestrator.

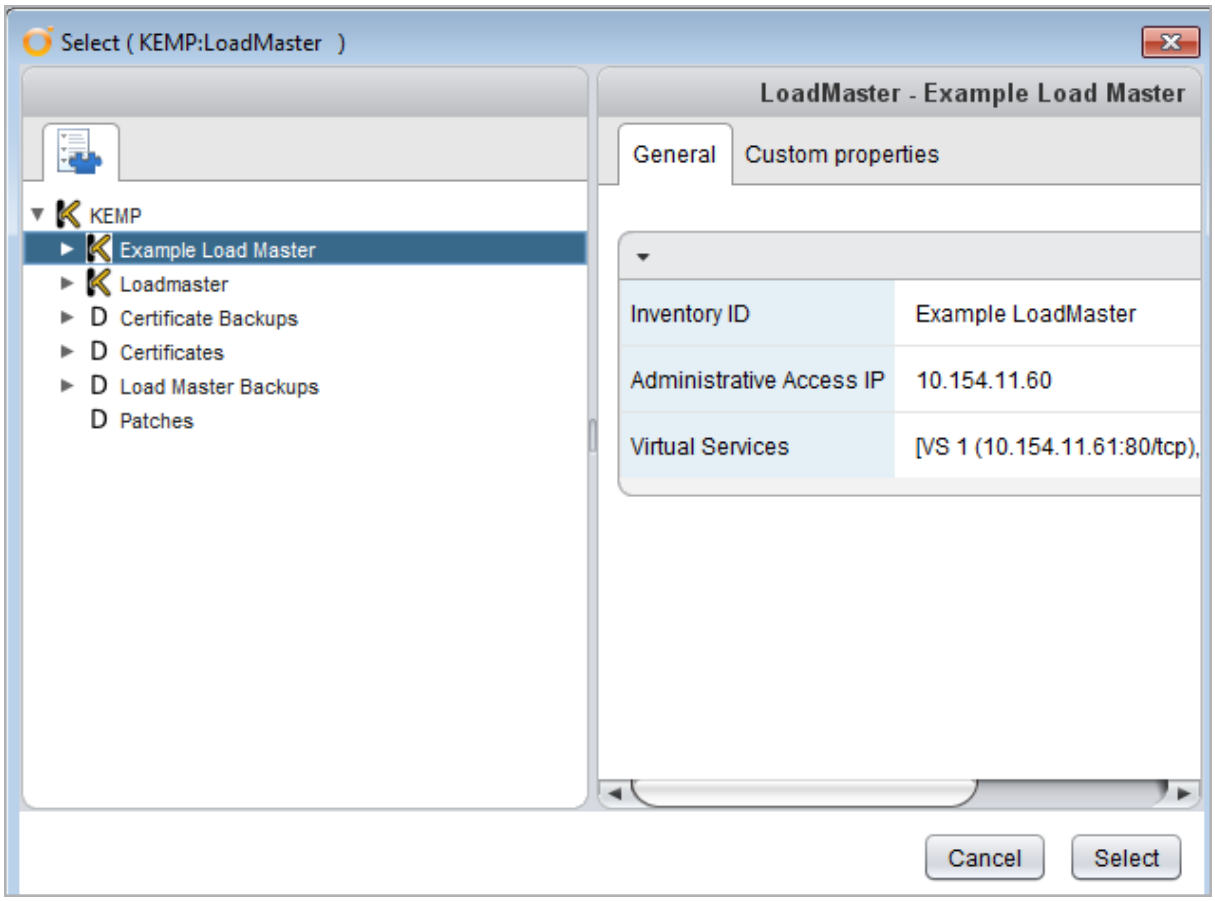
If the API is disabled, most of the workflows will not work. The only workflows that will work when the API is disabled are **Add LoadMaster** and **Enable API**.



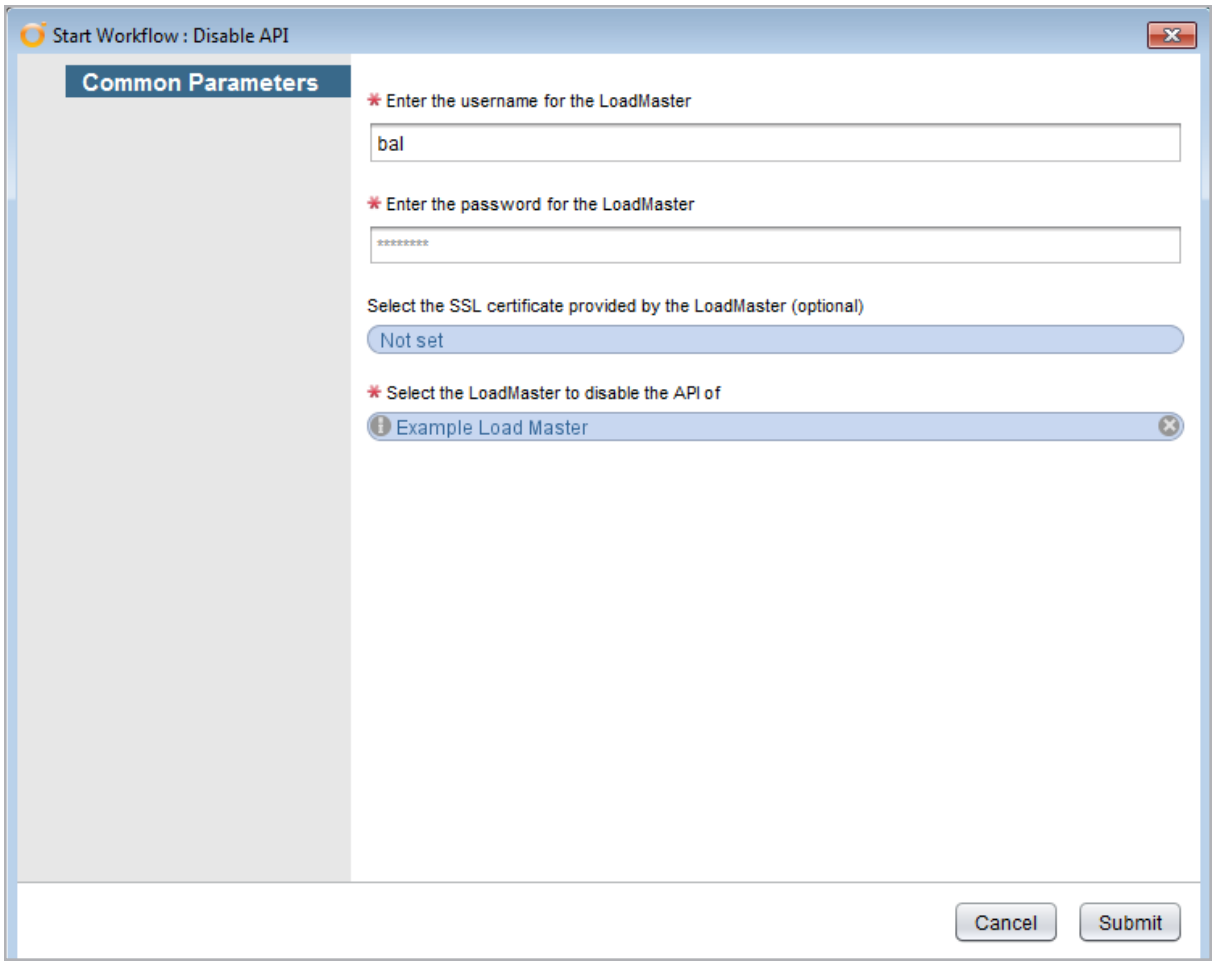
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

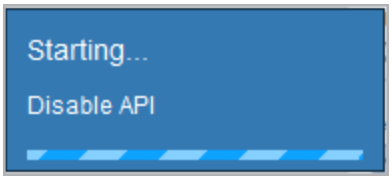
3. Click **Not set** in the **Select the LoadMaster to disable the API of** field.



4. Expand the **Kemp** directory.
5. Select the relevant LoadMaster.
6. Click **Select**.



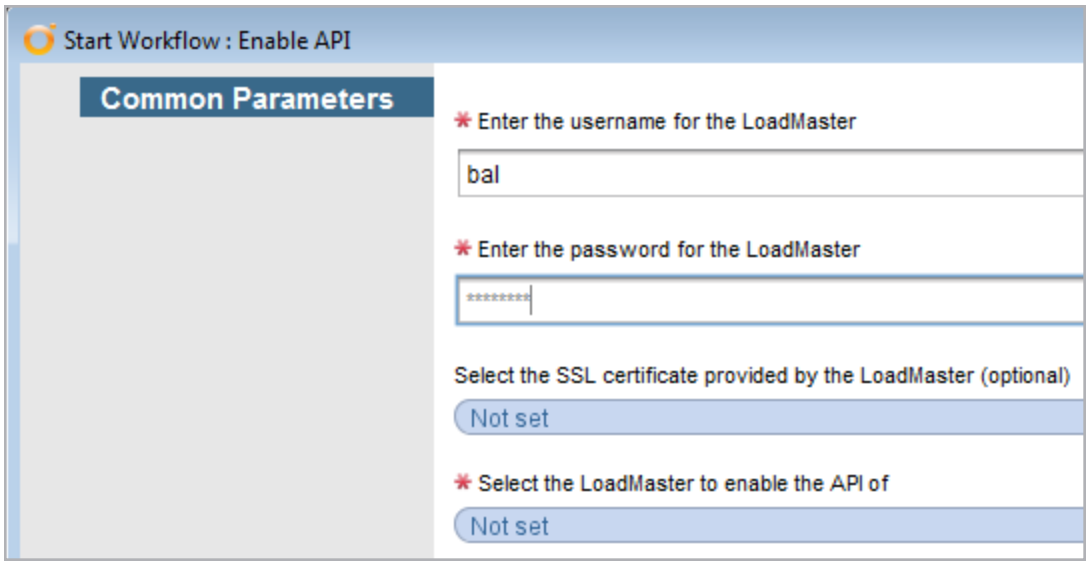
7. Click **Submit**.



8. Wait for the API to be disabled.

3.4.7 Enable API

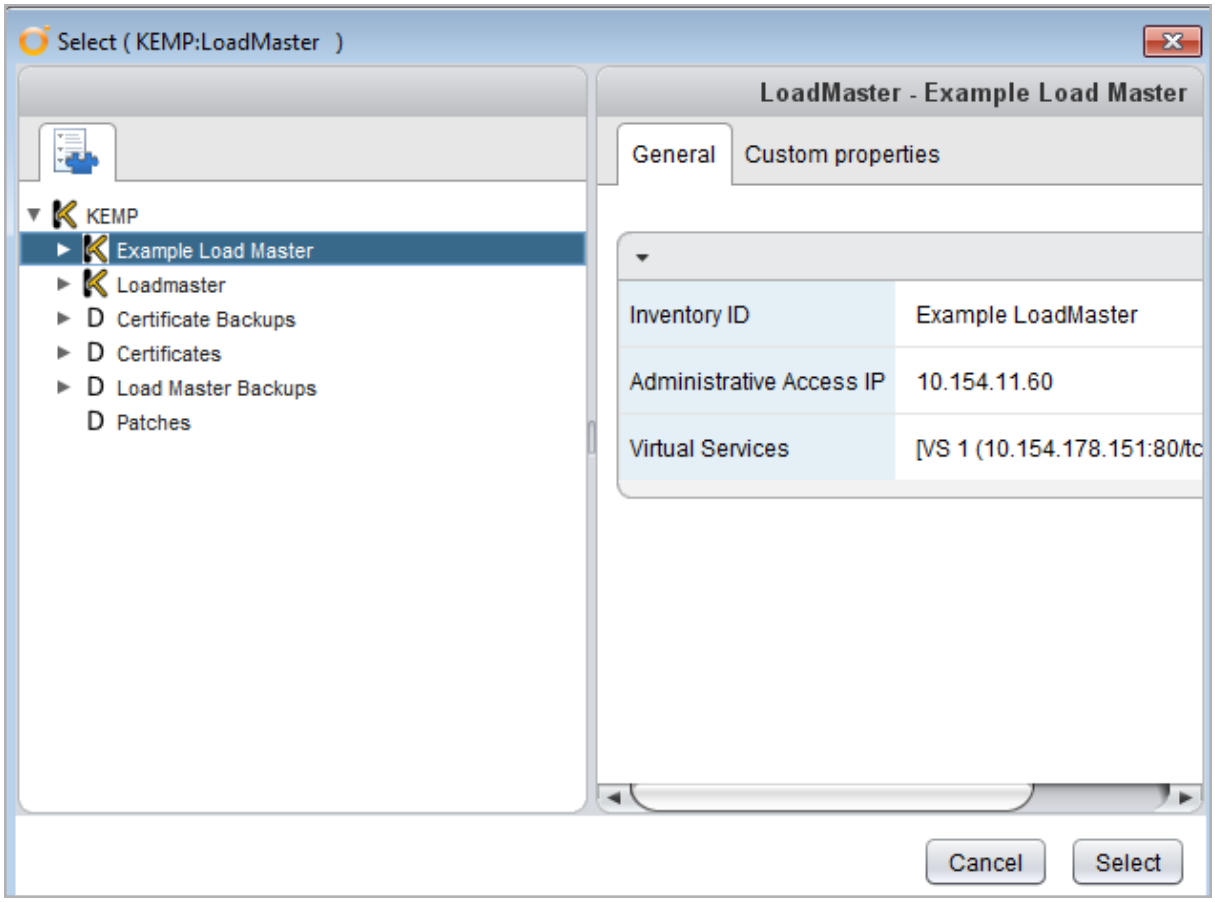
The API interface of a LoadMaster which exists in Orchestrator can be enabled via Orchestrator. The API interface needs to be enabled on a LoadMaster for most of the workflows to run. To enable the API, run the **Enable API** command.



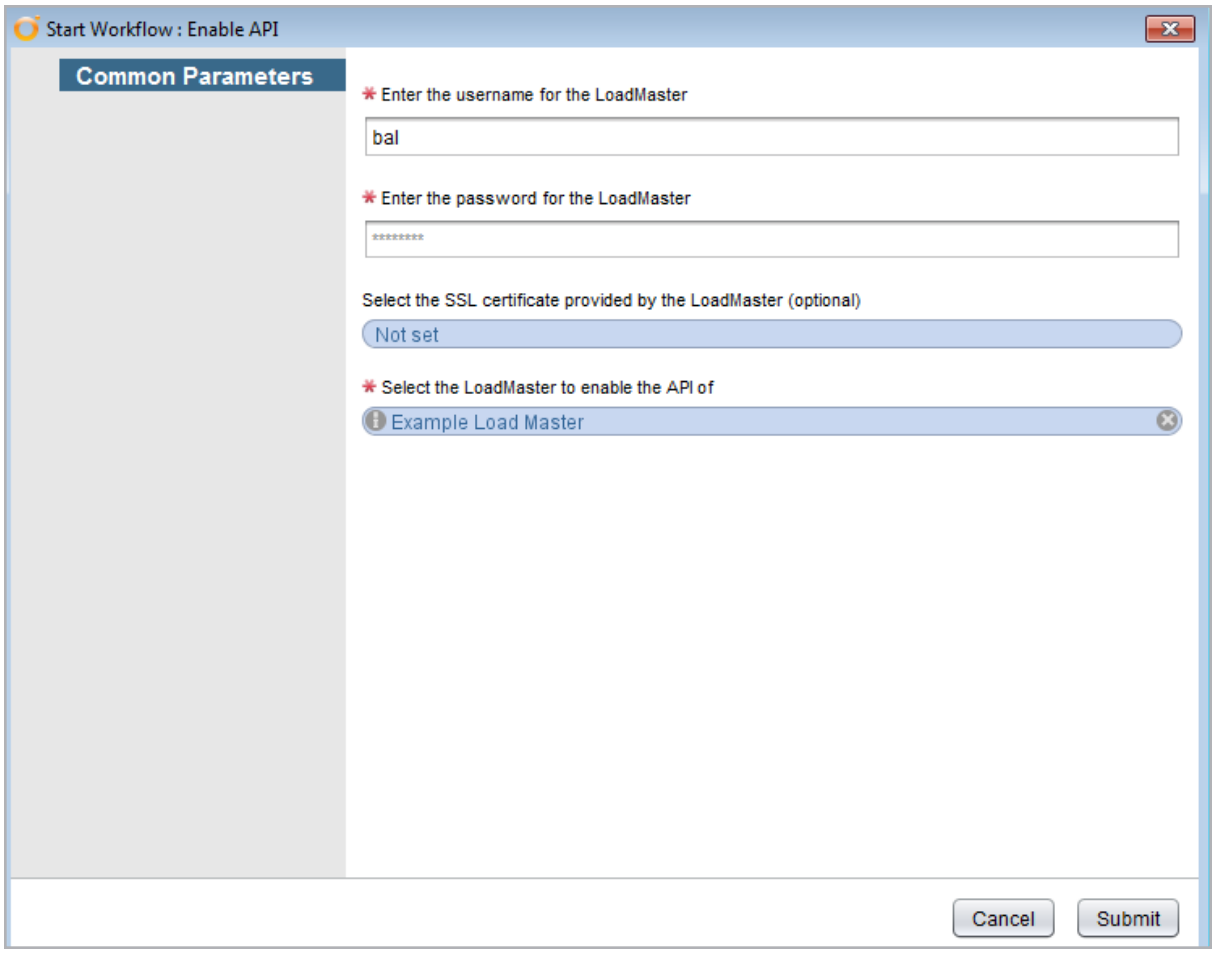
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

3. Click **Not set** in the **Select the LoadMaster to enable the API of** field.



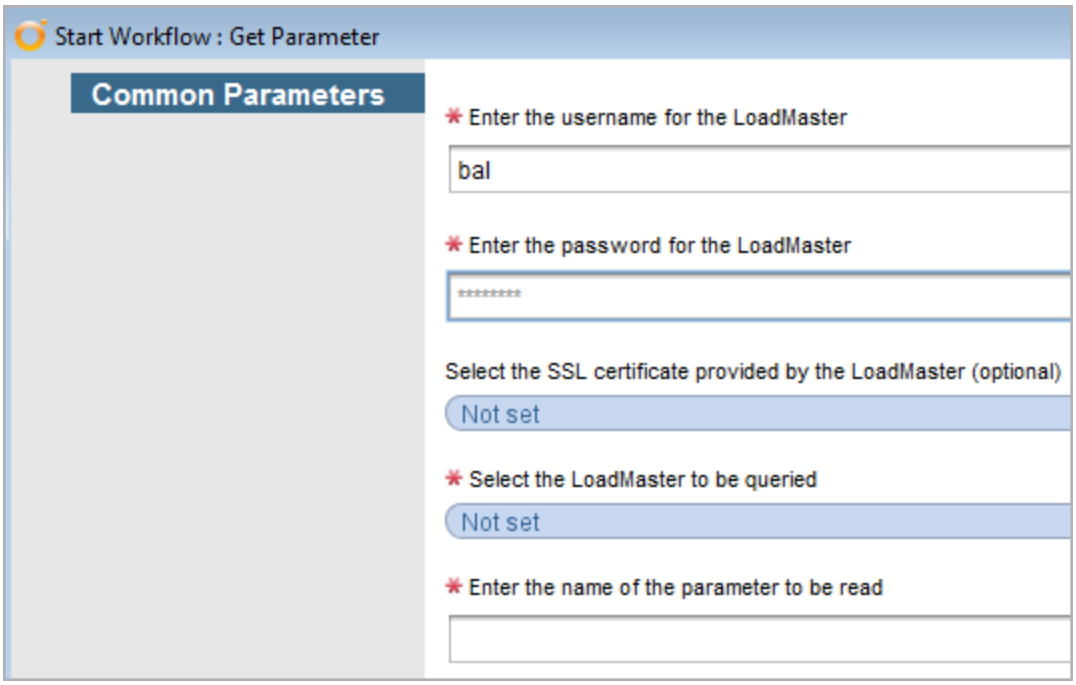
4. Expand the **Kemp** directory.
5. Select the relevant LoadMaster.
6. Click **Select**.



7. Click **Submit**.

3.4.8 Get Parameter

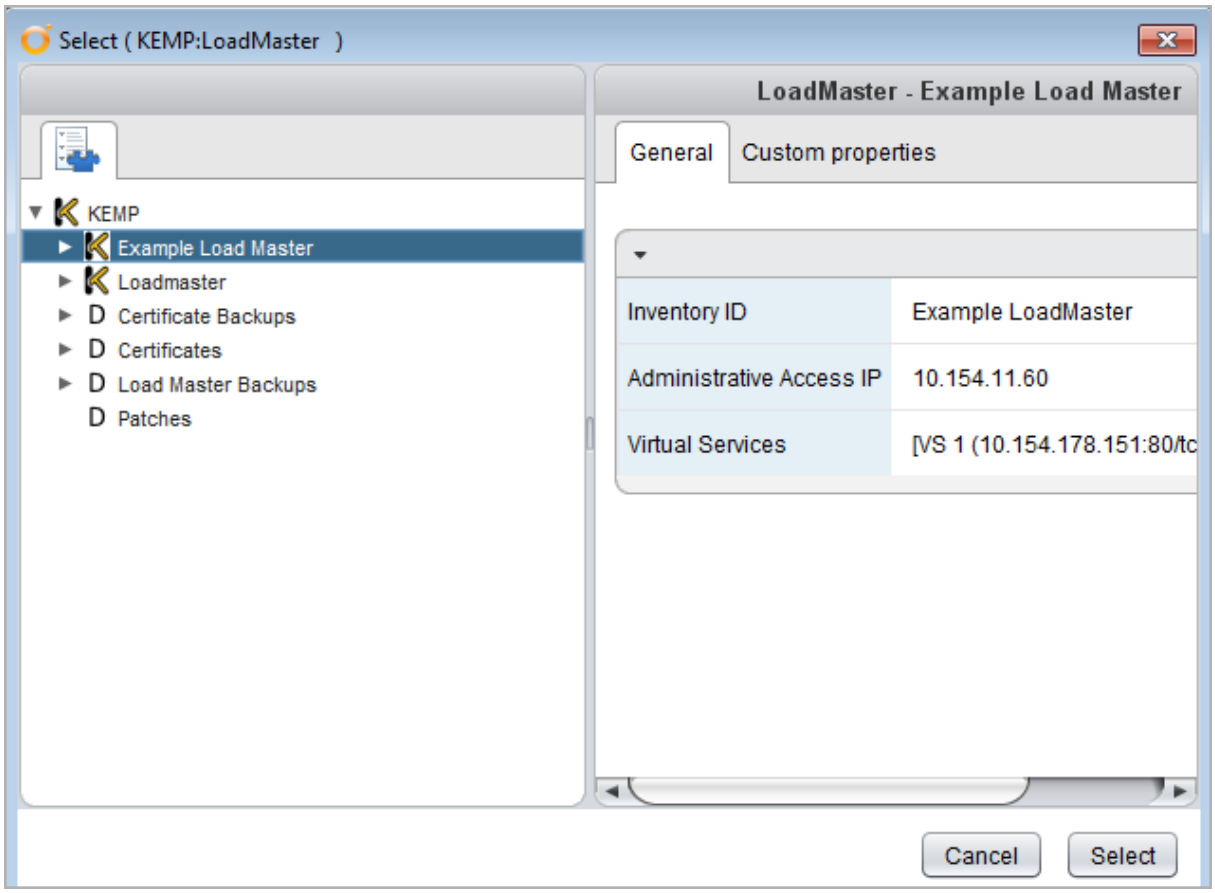
The **Get Parameter** workflow can be used to retrieve a number of LoadMaster field values. For a list of parameter names that can be retrieved, refer to **Appendix A - Get and Set Parameters**.



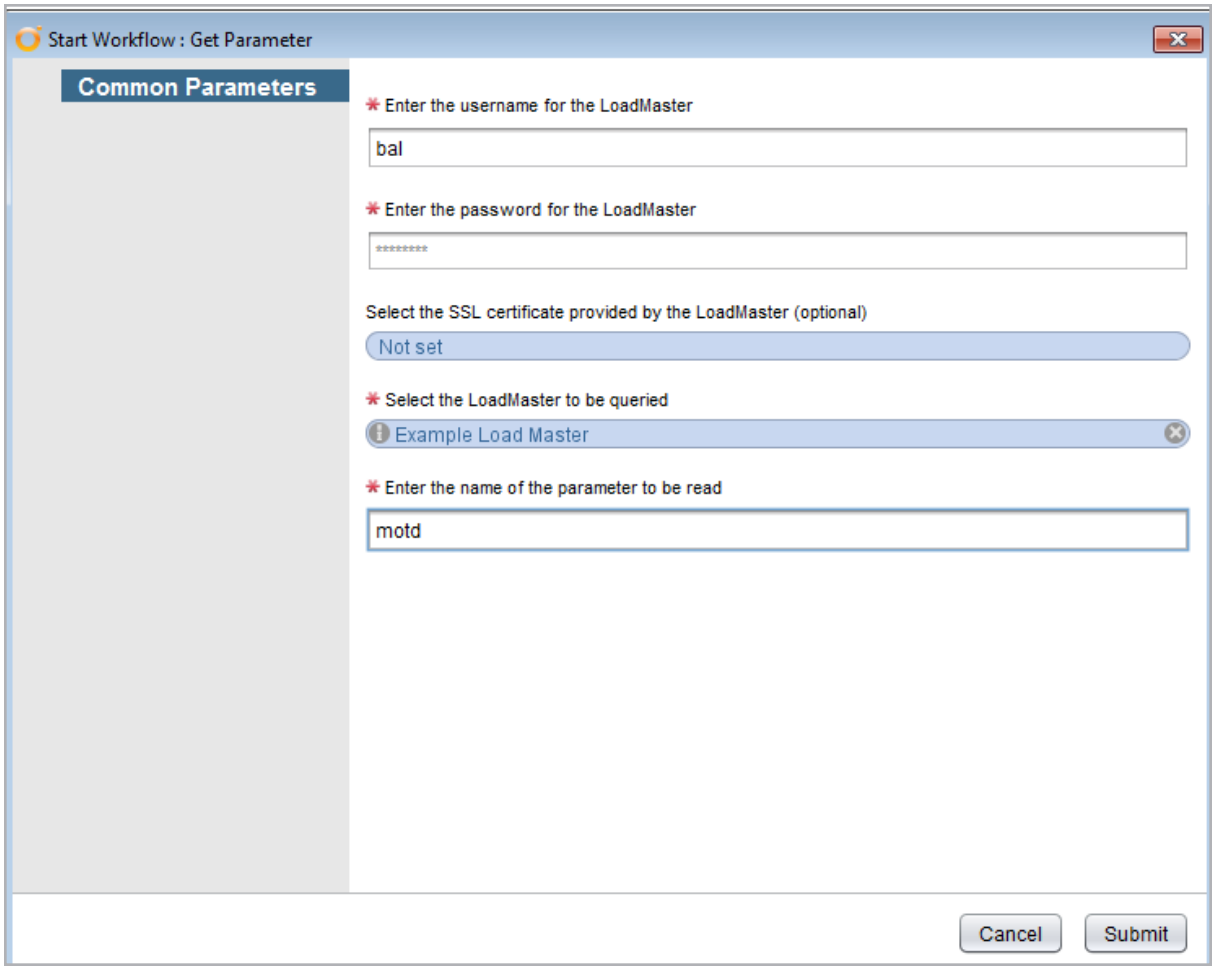
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

3. Click **Not set** in the **Select the LoadMaster to be queried** field.

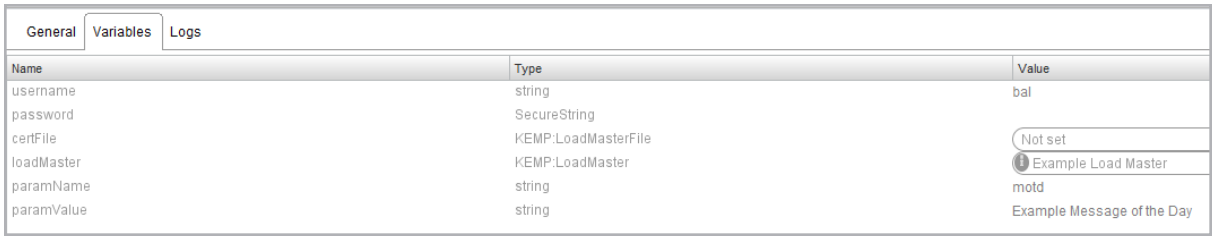


4. Expand the **Kemp** directory.
5. Select the LoadMaster to retrieve the value from.
6. Click **Select**.



7. Enter the relevant parameter name in the **Enter the name of the parameter to be read** field.

8. Click **Submit**.



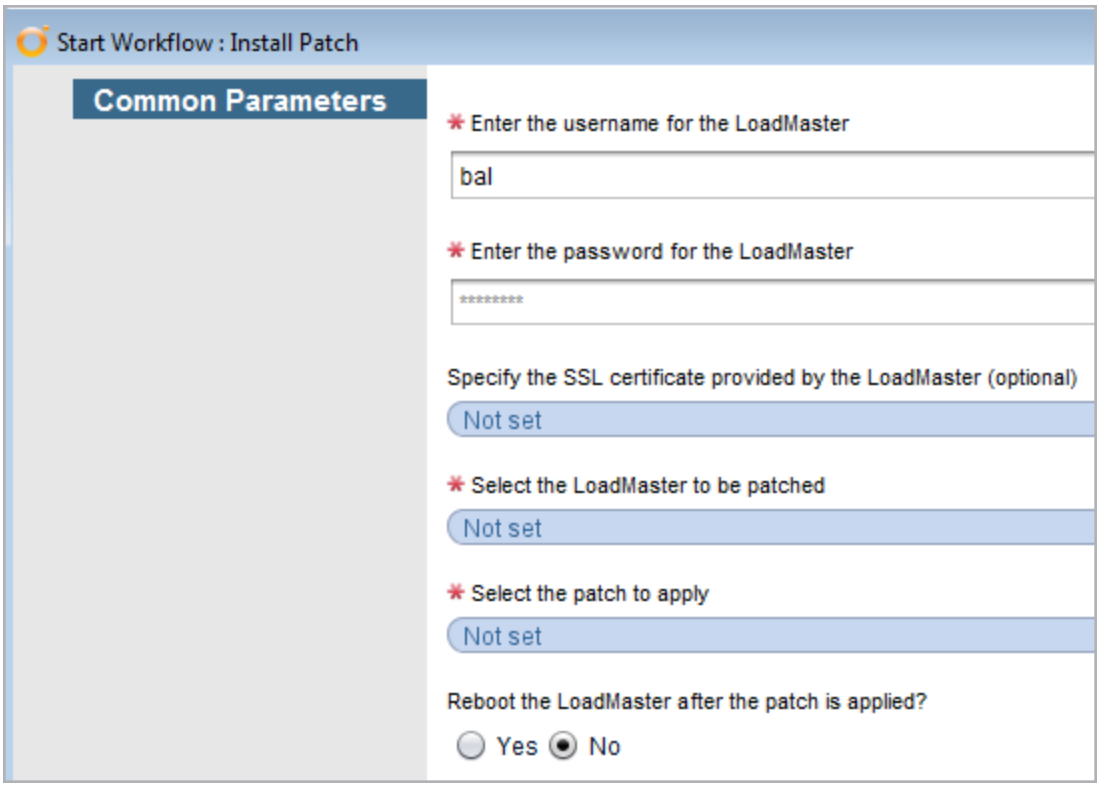
9. To view the value, select the **Variables** tab at the bottom.

10. The parameters and their values will be displayed.

3.4.9 Install Patch

The LoadMaster firmware can be updated with a firmware patch file via Orchestrator. Before uploading the firmware patch file to the LoadMaster, first it must be uploaded to Orchestrator. For step-by-step instructions on how to upload a file, refer to the **Upload Files** section.

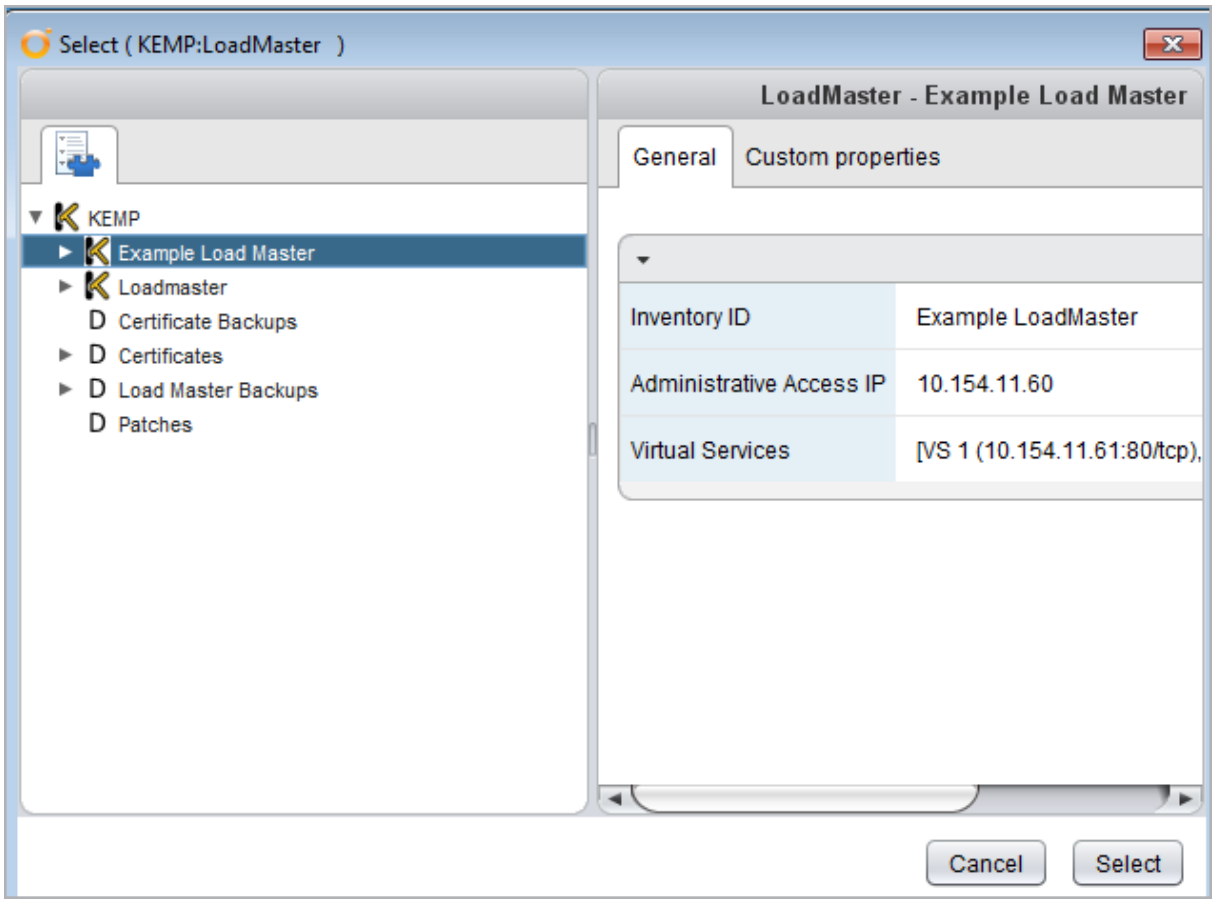
After a firmware patch file has been uploaded to Orchestrator, run the **Install Patch** workflow to update the LoadMaster.



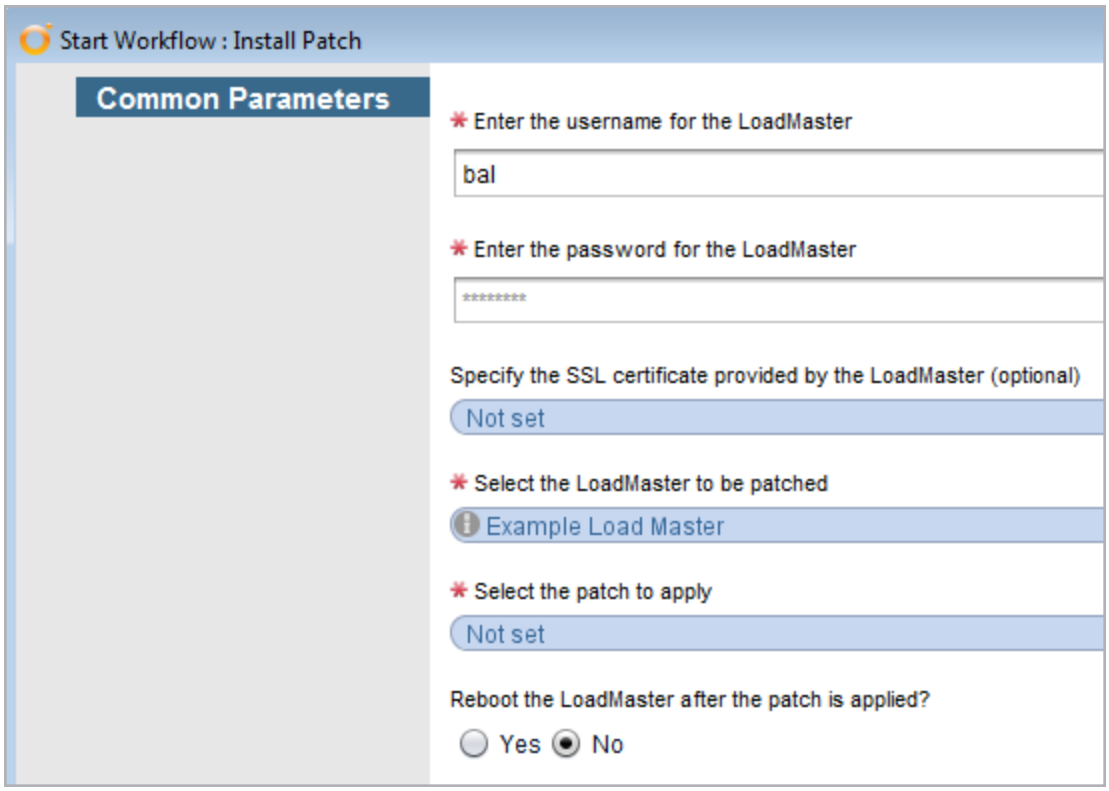
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

3. Click **Not set** in the **Select the LoadMaster to be patched** field.



4. Expand the **Kemp** directory.
5. Select the LoadMaster to be patched.
6. Click **Select**.



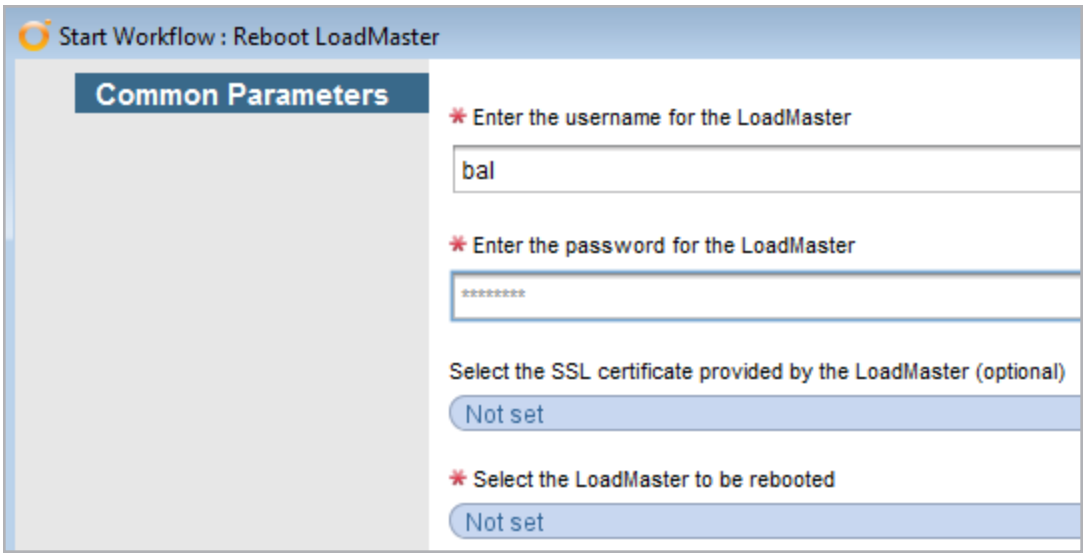
7. Click **Not set** in the **Select the patch to apply** field.
8. Expand the **Kemp** directory.
9. Expand the **Patches** directory.
10. Select the relevant patch file.
11. Click **Select**.
12. Select **Yes** to reboot the LoadMaster after the patch has been uploaded.

    The LoadMaster must be rebooted after the patch file has been installed in order for the changes to be applied correctly.

13. Click **Submit**.
14. Wait for the installation and reboot to complete.

3.4.10 Reboot LoadMaster

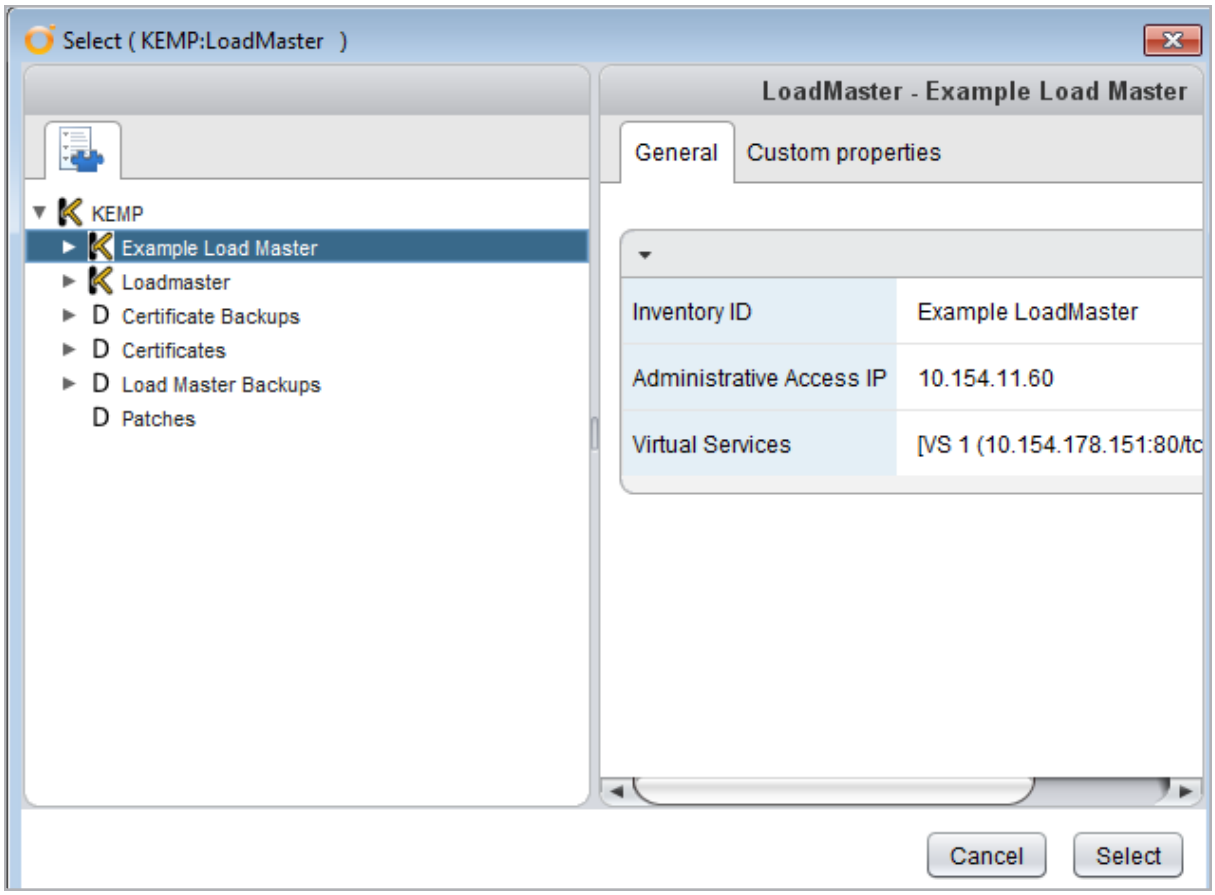
A LoadMaster which exists in Orchestrator can be rebooted via Orchestrator. To reboot a LoadMaster, run the **Reboot LoadMaster** workflow.



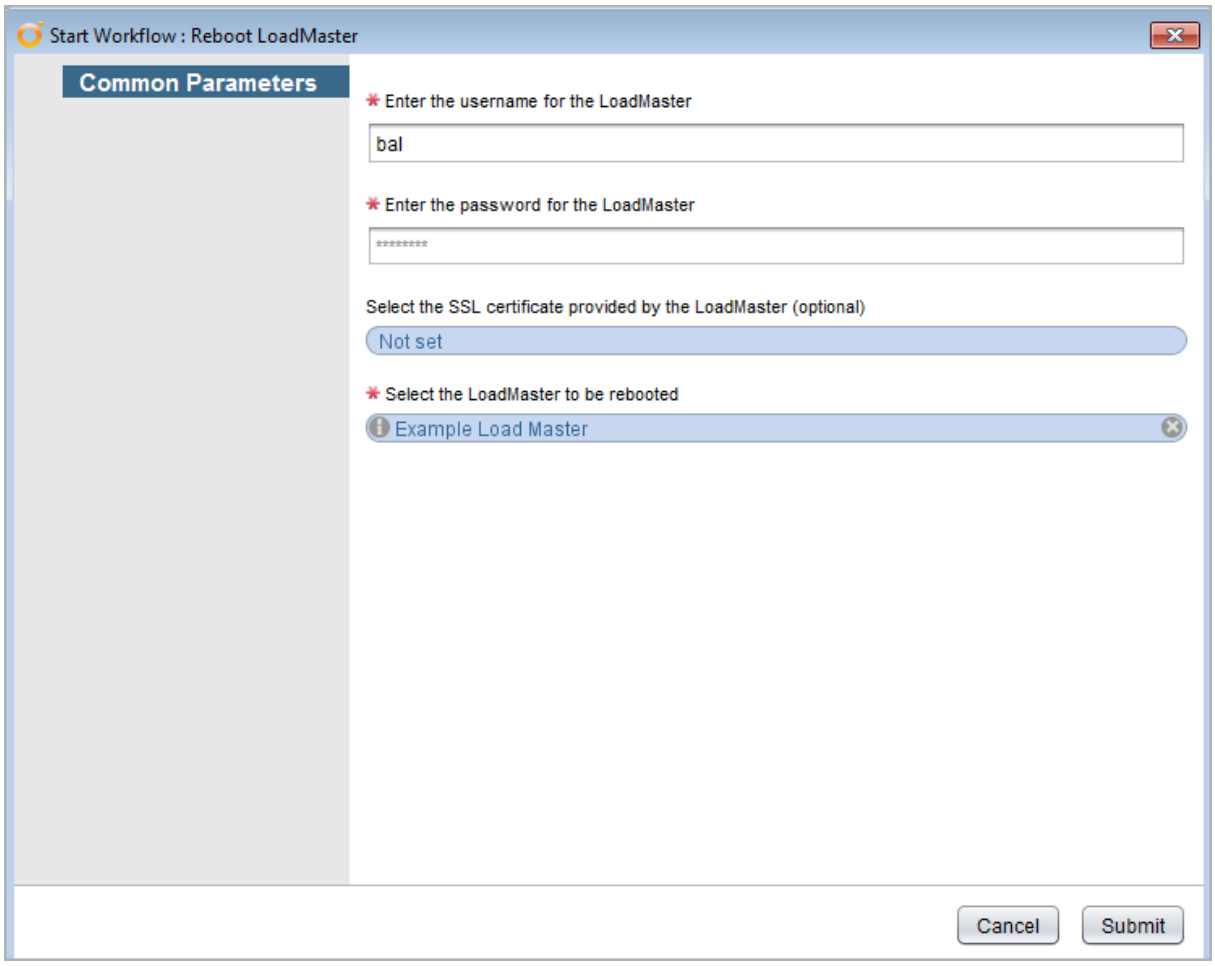
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

3. Click **Not set** in the **Select the LoadMaster to be rebooted** field.



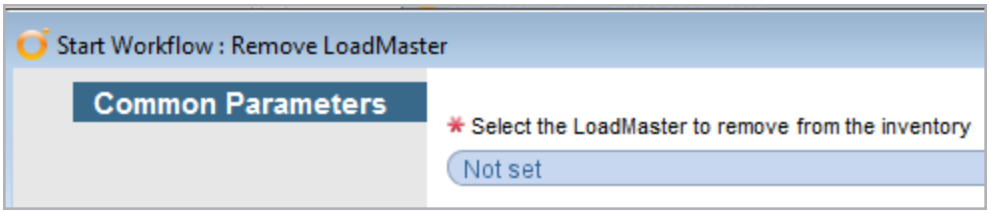
4. Select the relevant LoadMaster to be rebooted.
5. Click **Select**.



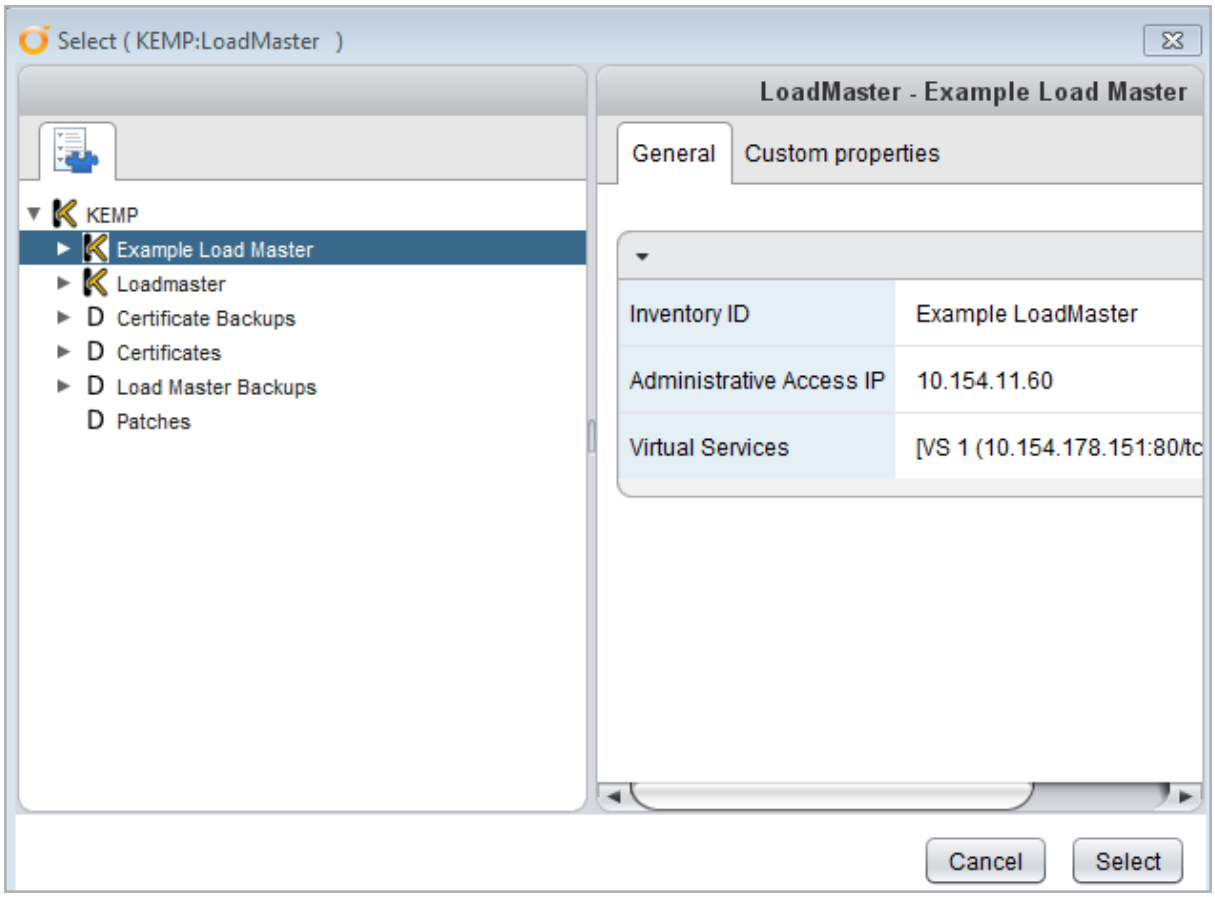
6. Click **Submit**.
7. Wait for the LoadMaster to reboot.

3.4.11 Remove LoadMaster

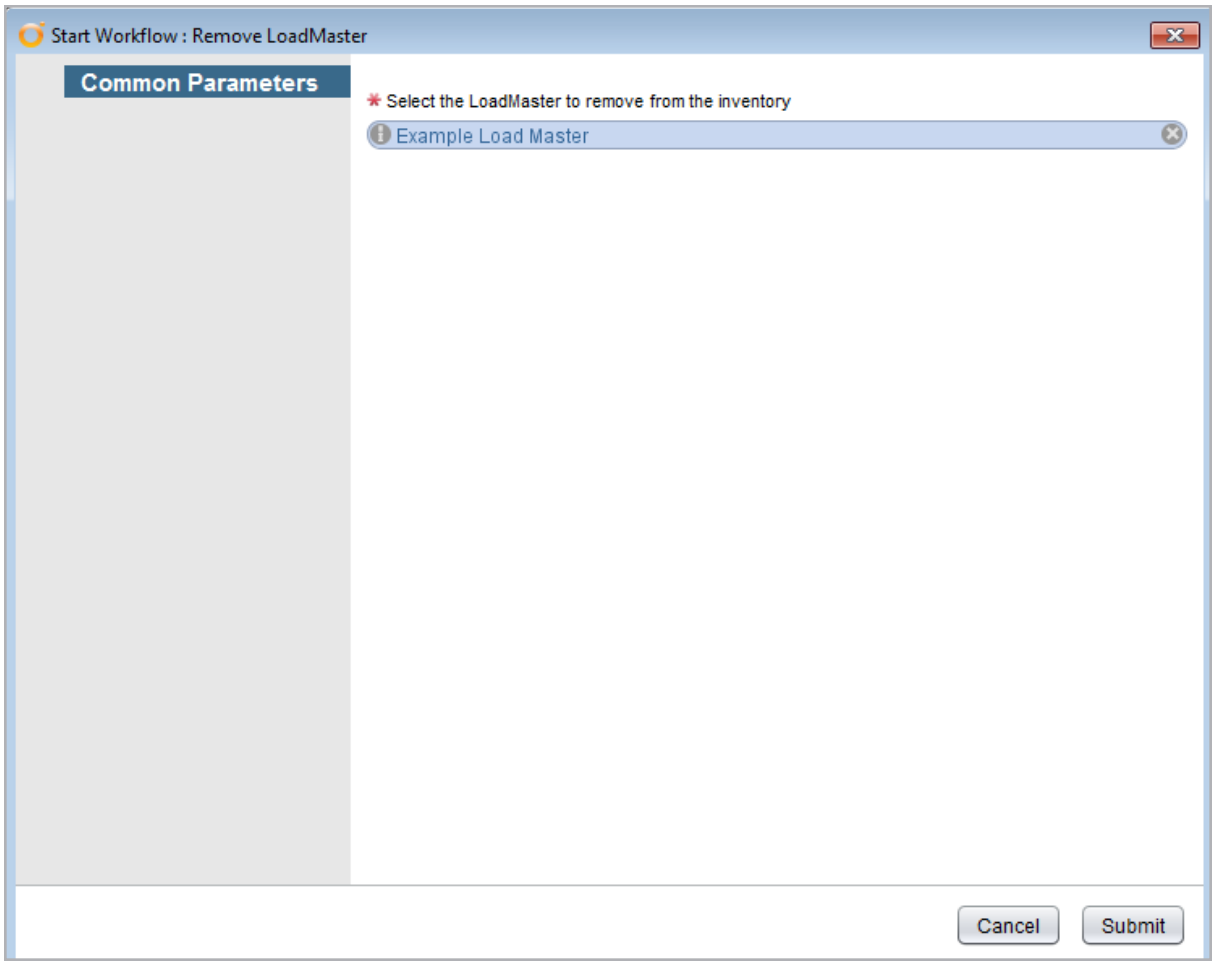
A LoadMaster can be removed from Orchestrator by running the **Remove LoadMaster** command.



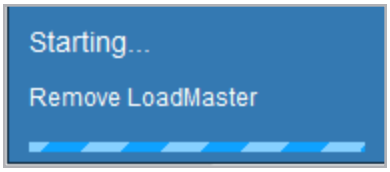
1. Click **Not set**.



2. Select the relevant LoadMaster.
3. Click **Select**.



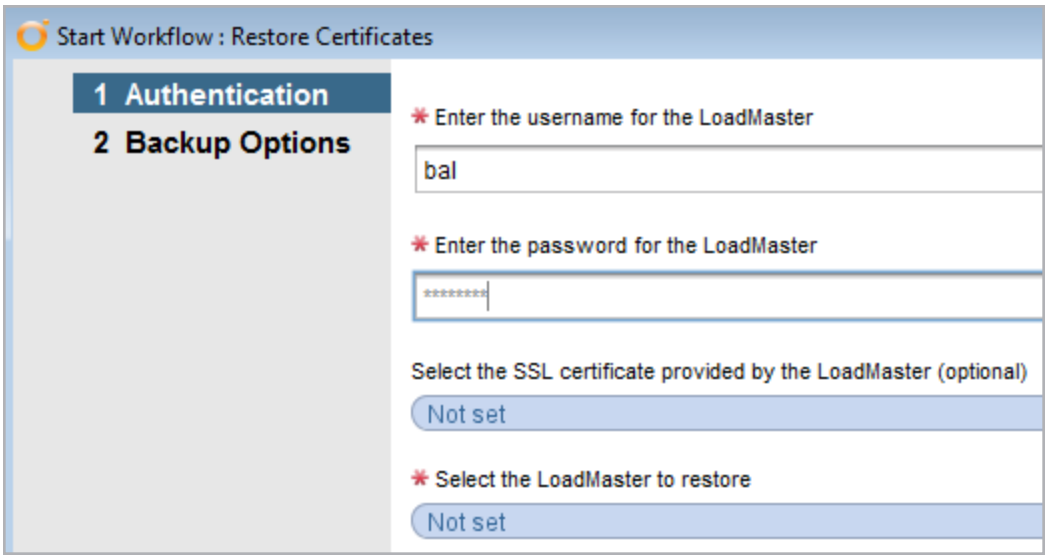
4. Click **Submit**.



5. Wait for the LoadMaster to be removed.

3.4.12 Restore Certificates

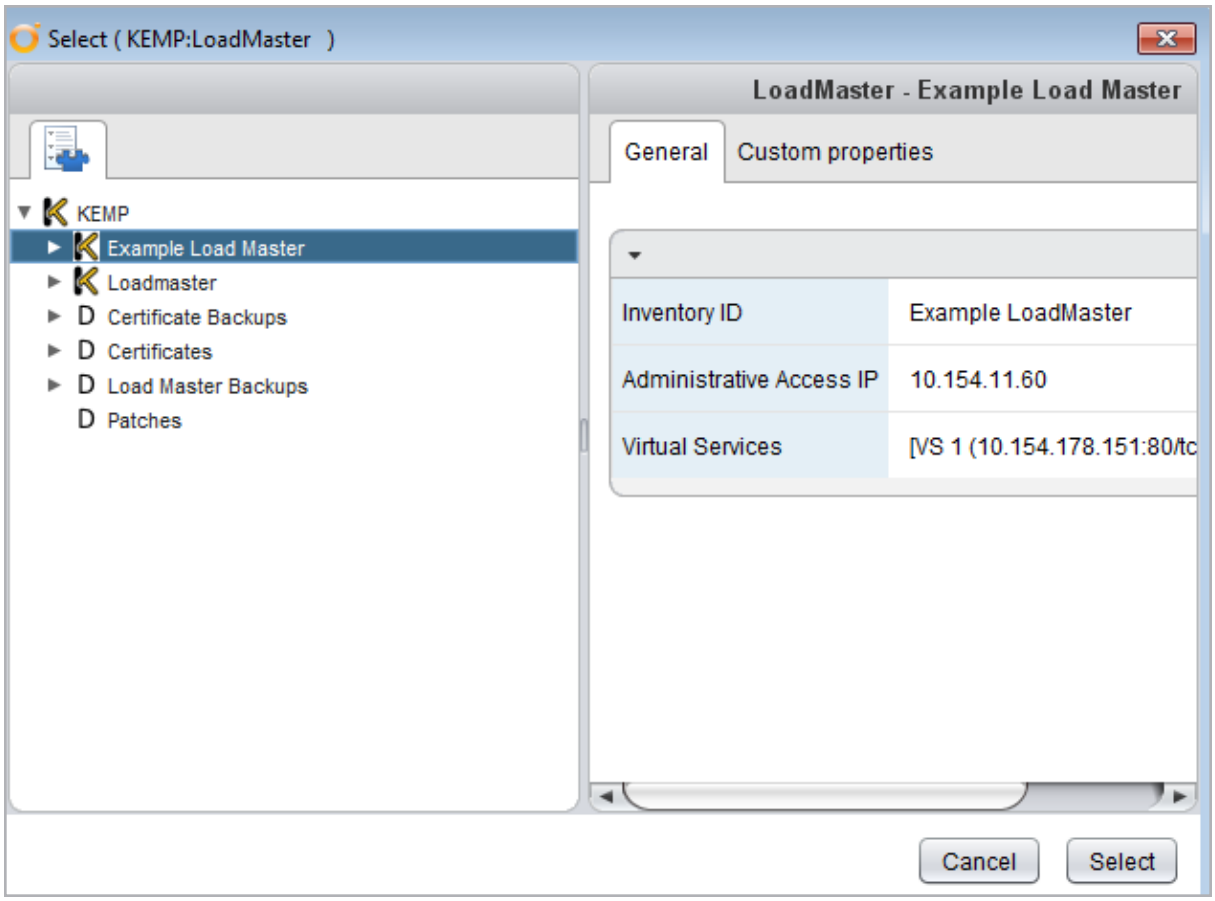
If a certificate backup file exists in Orchestrator, it can be restored to a LoadMaster. To back up the certificates on a LoadMaster, refer to the **Backup Certificates** section. To restore the certificates, run the **Restore Certificates** command.



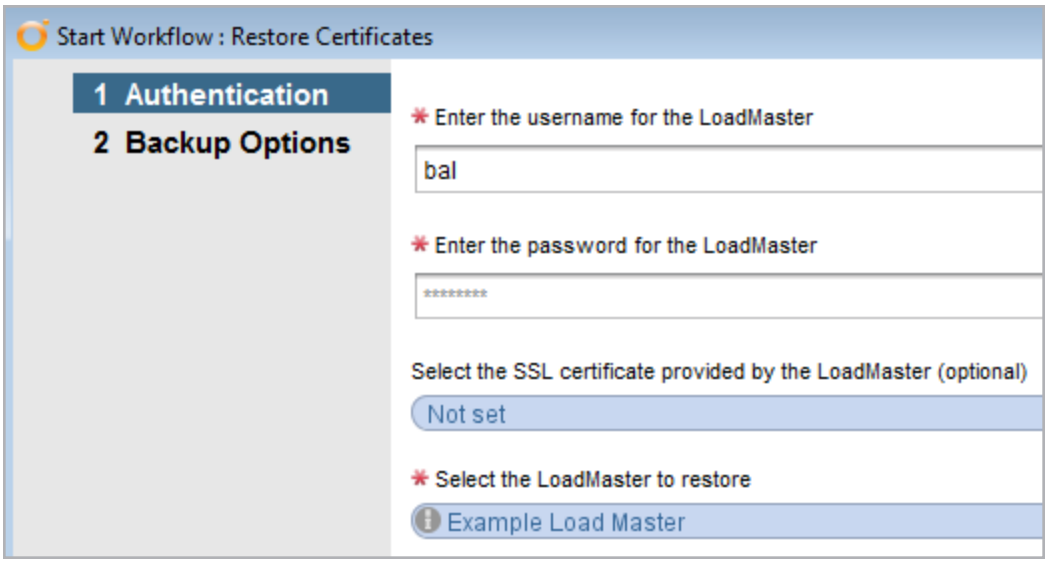
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

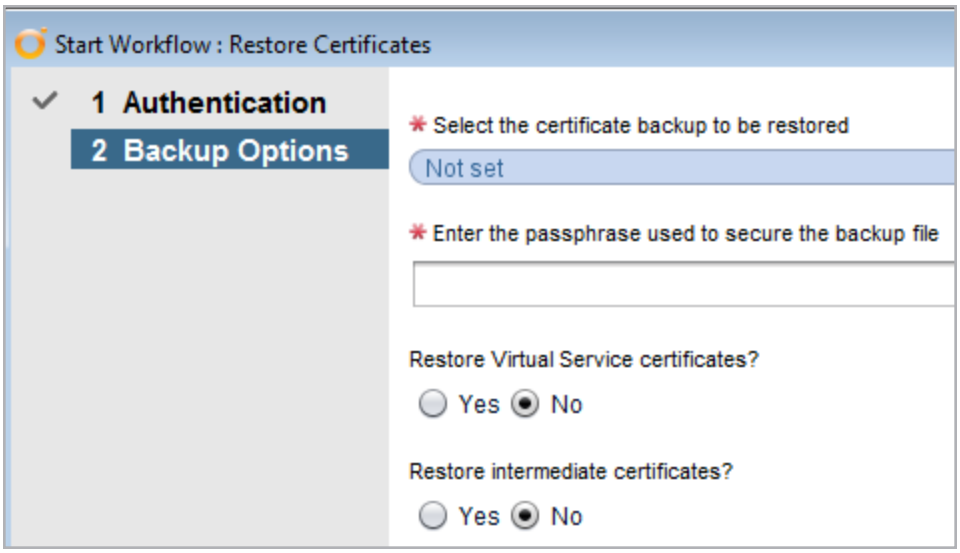
3. Click **Not set**.



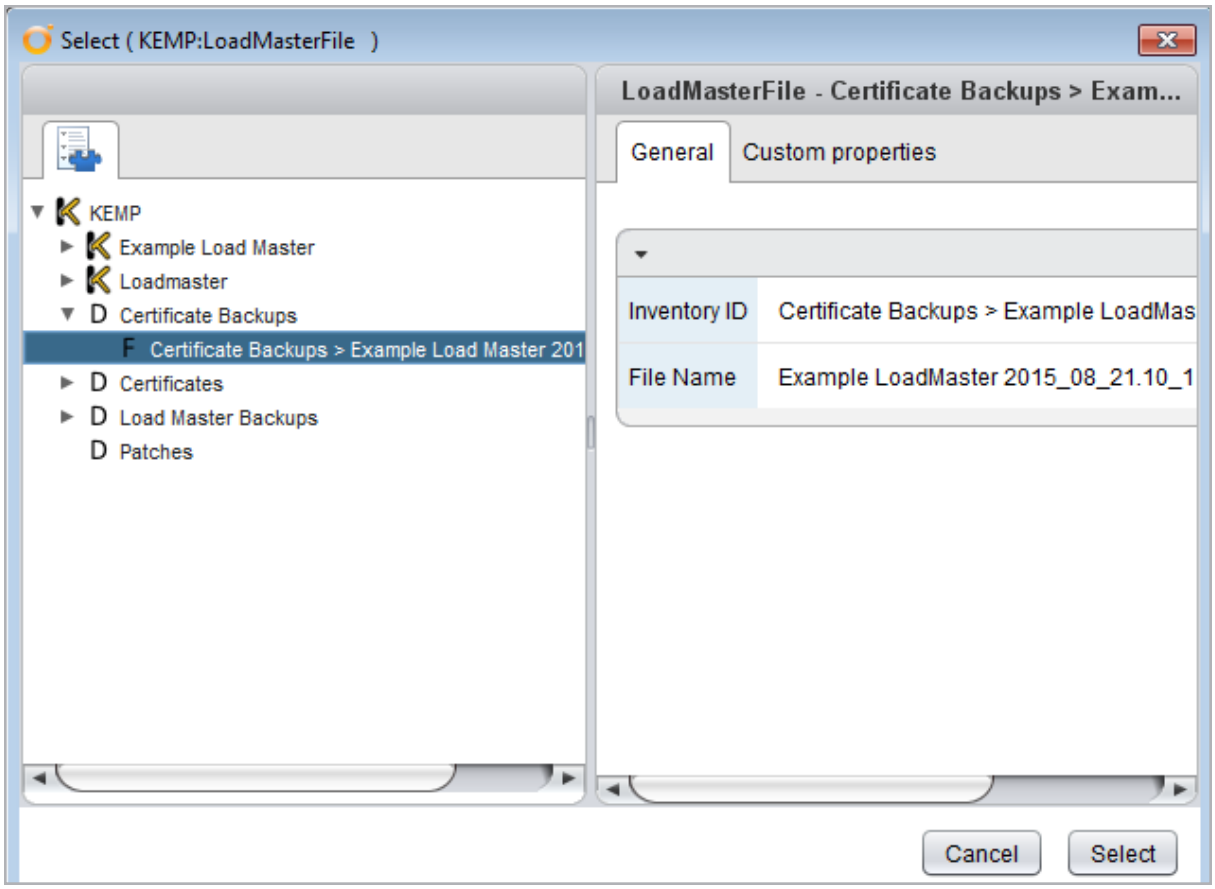
4. Expand the **Kemp** directory.
5. Select the relevant LoadMaster.
6. Click **Select**.



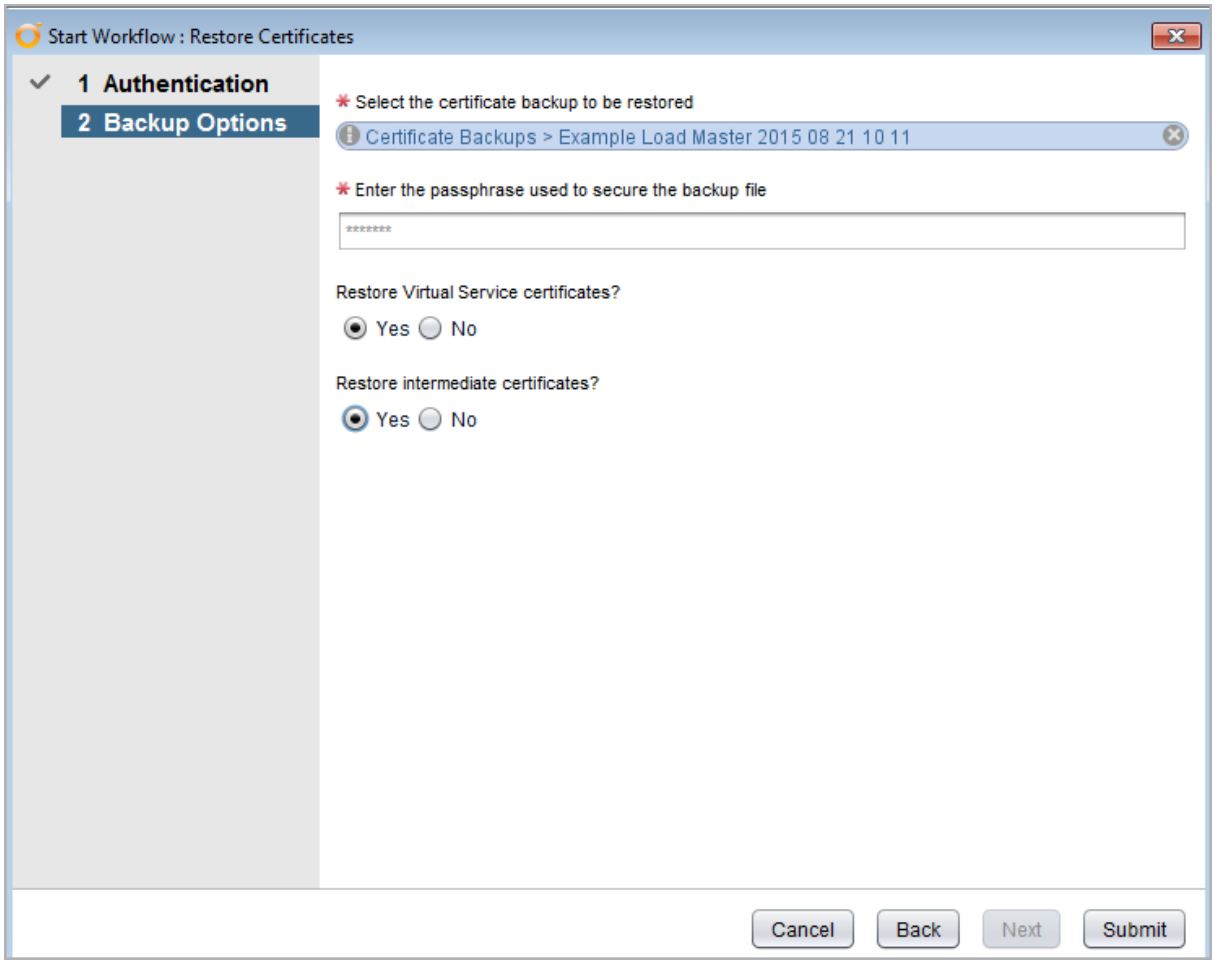
7. Click **Backup Options**.



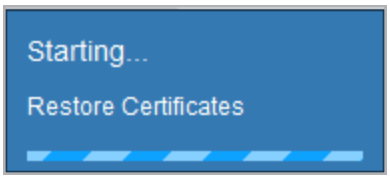
8. Click **Not set**.



9. Expand the **Kemp** directory.
10. Expand the **Certificate Backups** directory.
11. Select the relevant backup.
12. Click **Select**.



13. Enter the passphrase used to secure the backup file.
14. Specify which certificates to restore.
15. Click **Submit**.



16. Wait for the certificates to restore.

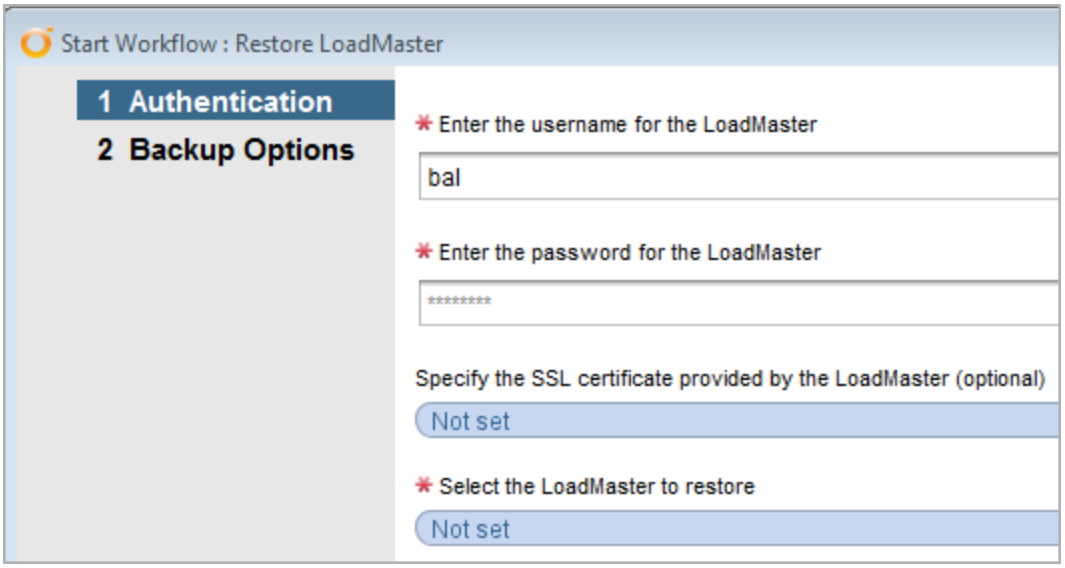
3.4.13 Restore LoadMaster

Before restoring a LoadMaster configuration, a backup configuration must be available in Orchestrator. To back up a LoadMaster configuration in Orchestrator, refer to the **Backup**

LoadMaster section.

When a backup configuration exists in Orchestrator, run the **Restore LoadMaster** workflow to restore the configuration.

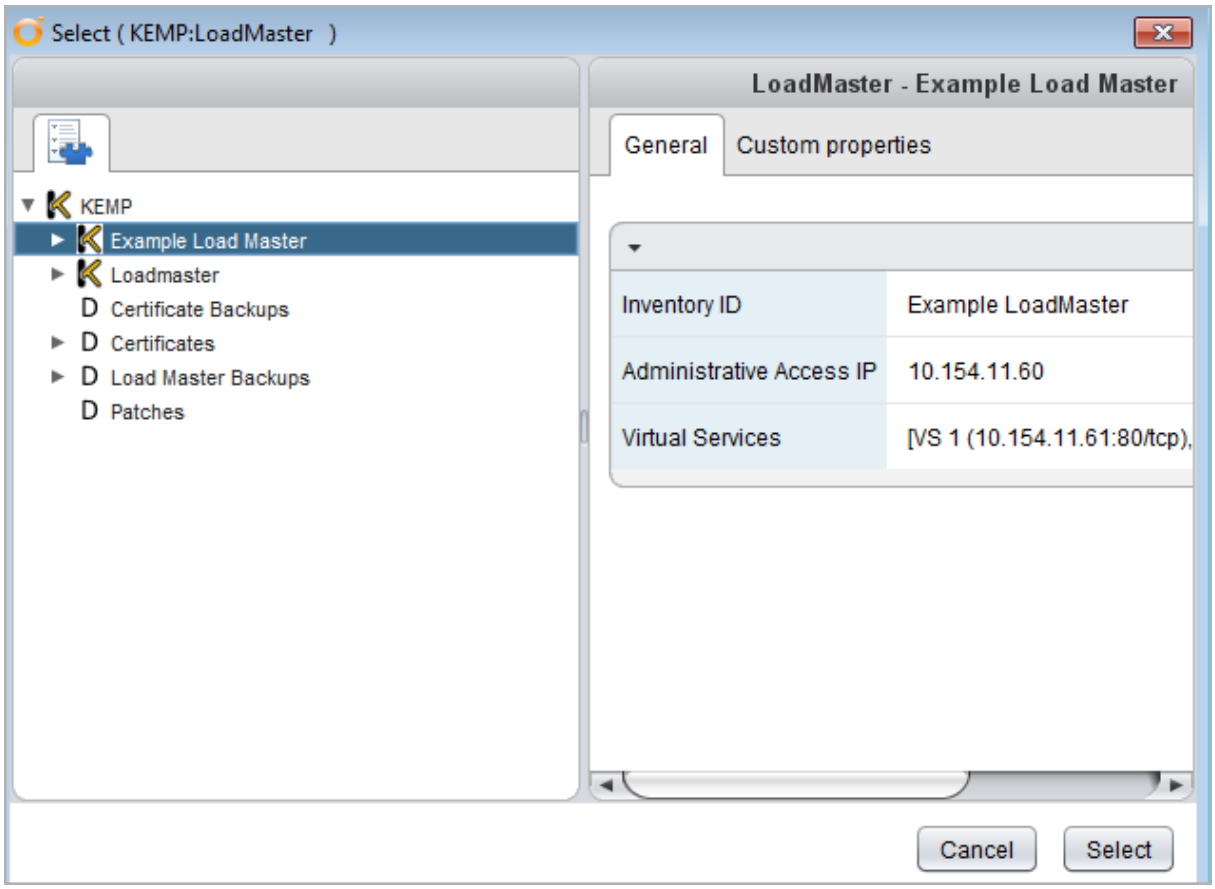
> A GEO LoadMaster backup configuration cannot be restored on a non-GEO LoadMaster configuration



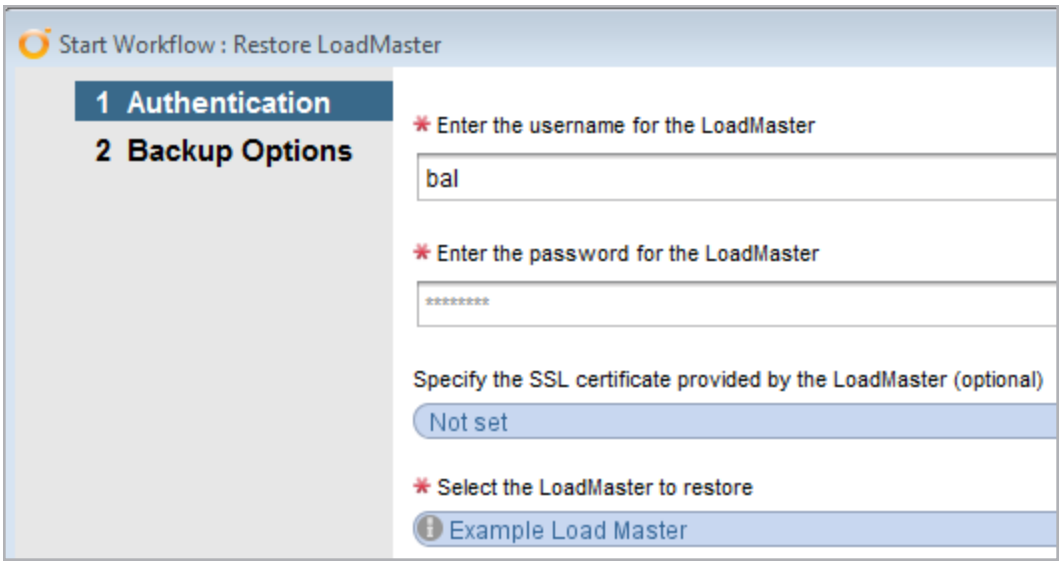
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

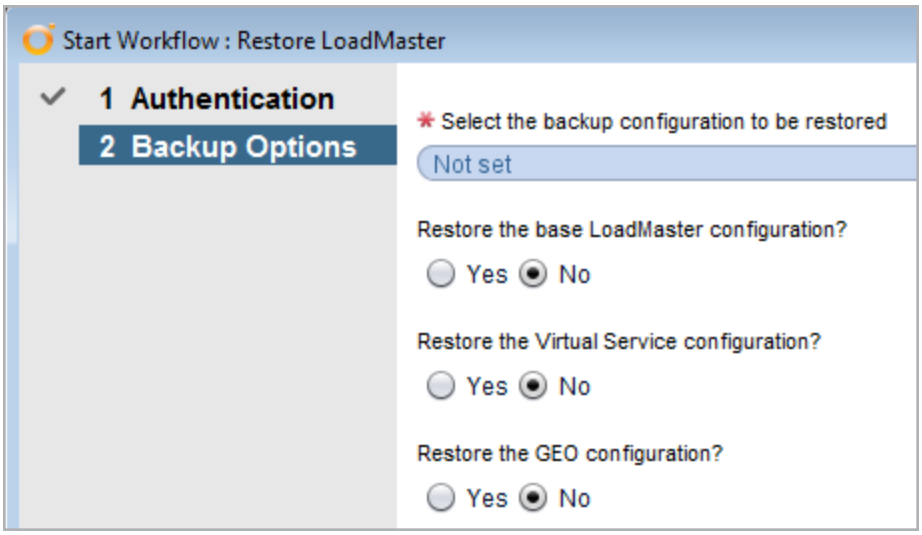
3. Click **Not set** in the **Select the LoadMaster to restore** field.



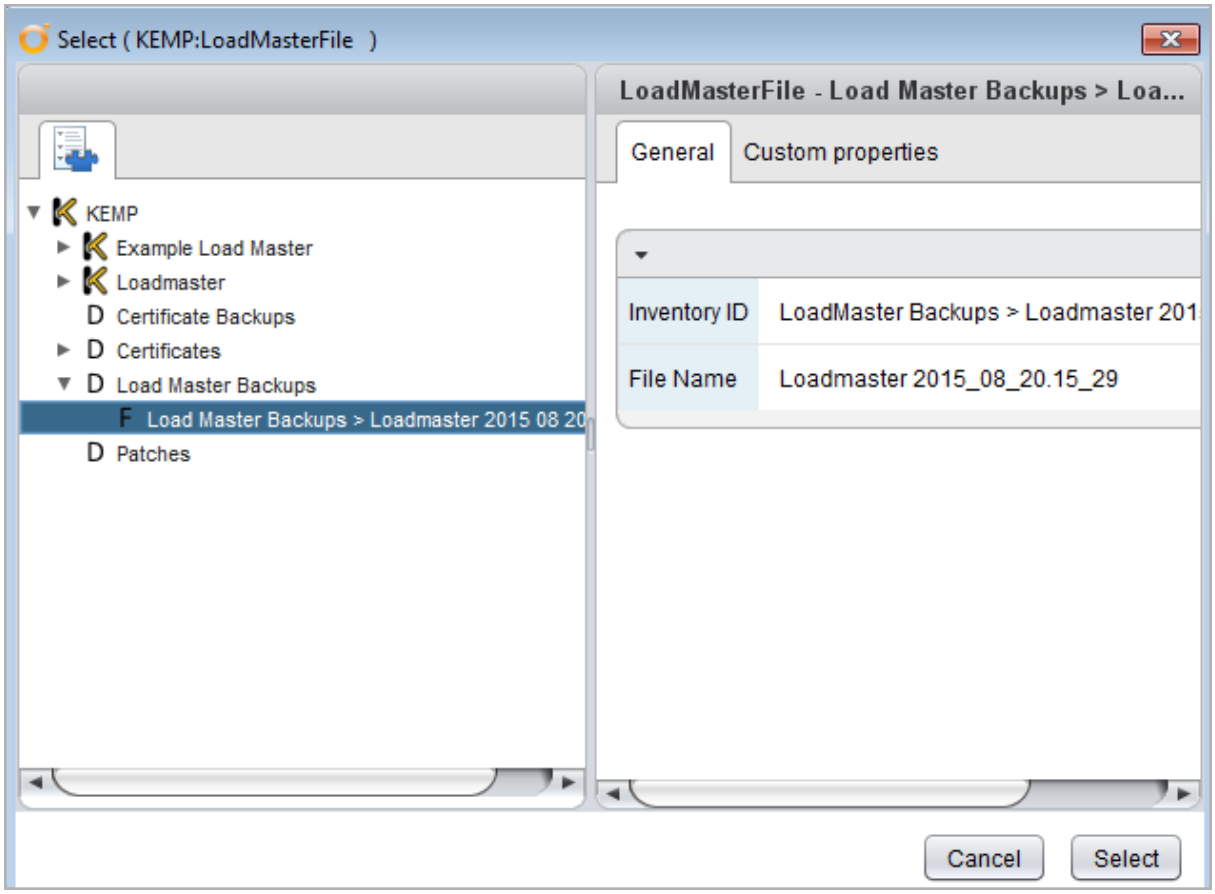
4. Expand the **Kemp** directory.
5. Select the relevant LoadMaster.
6. Click **Select**.



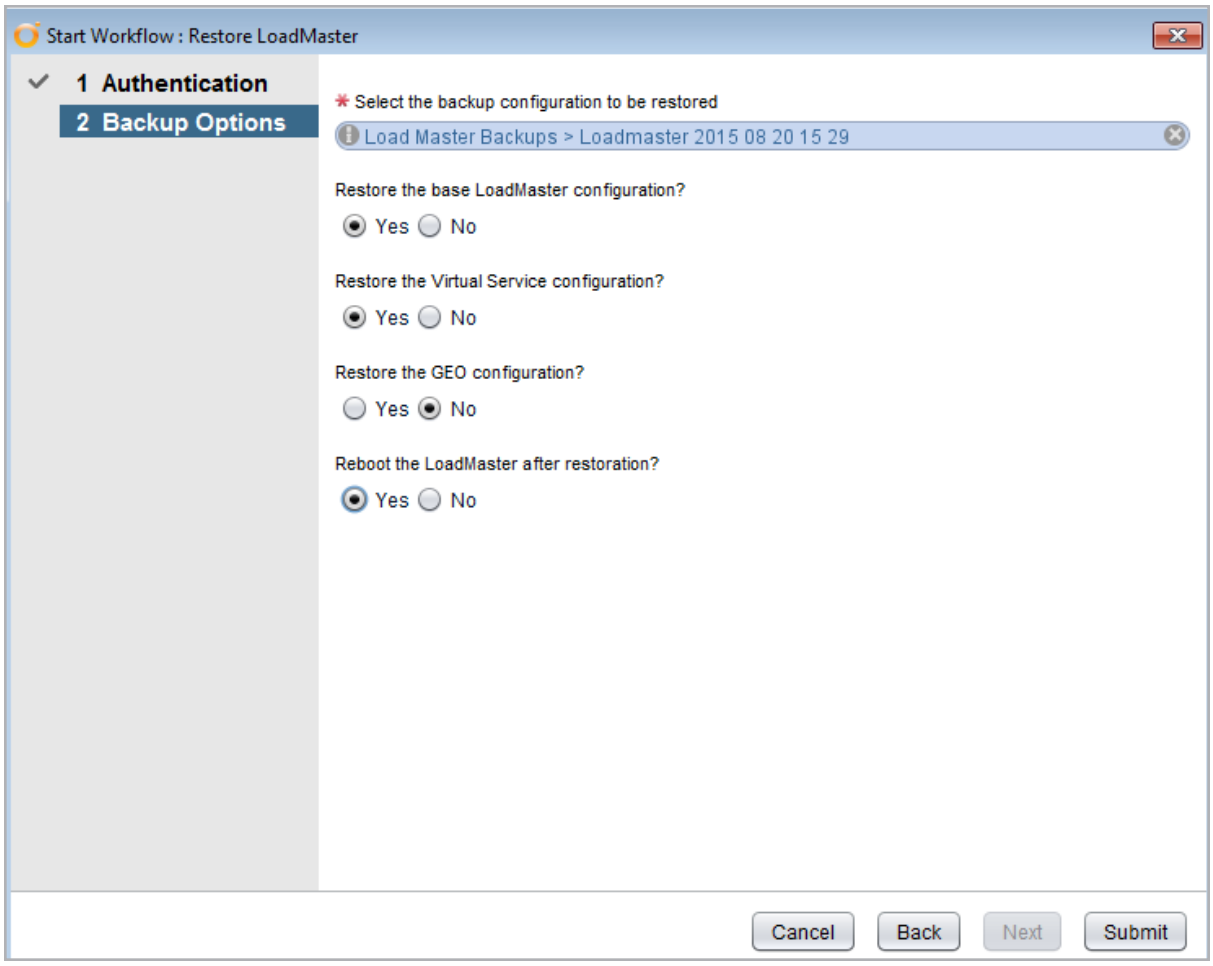
7. Click **Backup Options**.



8. Click **Not set**.



9. Expand the **Kemp** directory.
10. Expand the **LoadMaster Backups** directory.
11. Select the relevant backup.
12. Click **Select**.



13. Specify the configurations to be restored by selecting **Yes** for the relevant options.

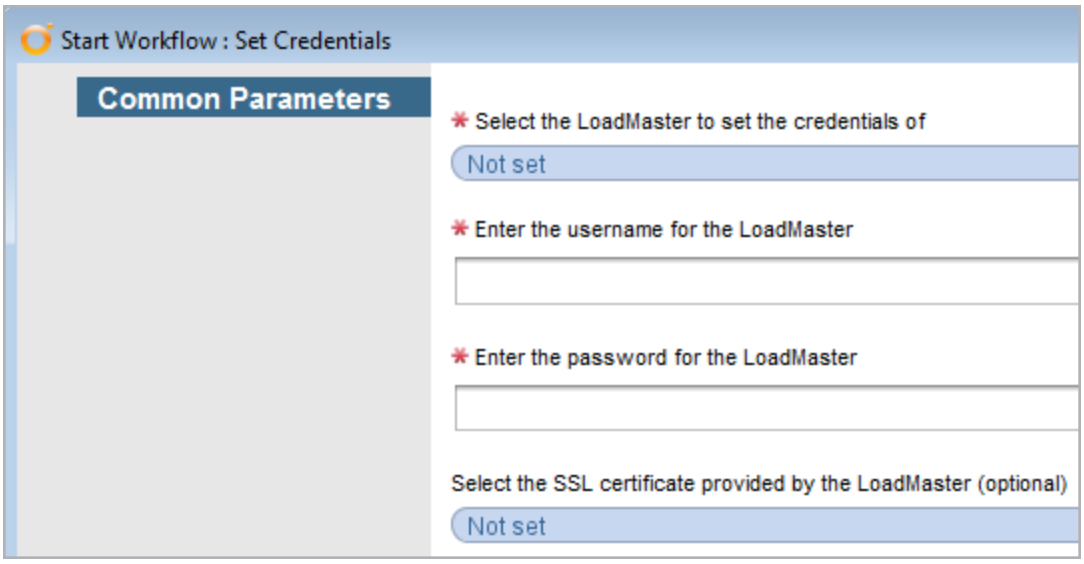
14. If restoring the base LoadMaster configuration, another field will appear asking if the LoadMaster should be rebooted after restoration. If restoring the base configuration, please set this to **Yes** as the LoadMaster needs to be rebooted for the changes to be applied.

15. Click **Submit**.

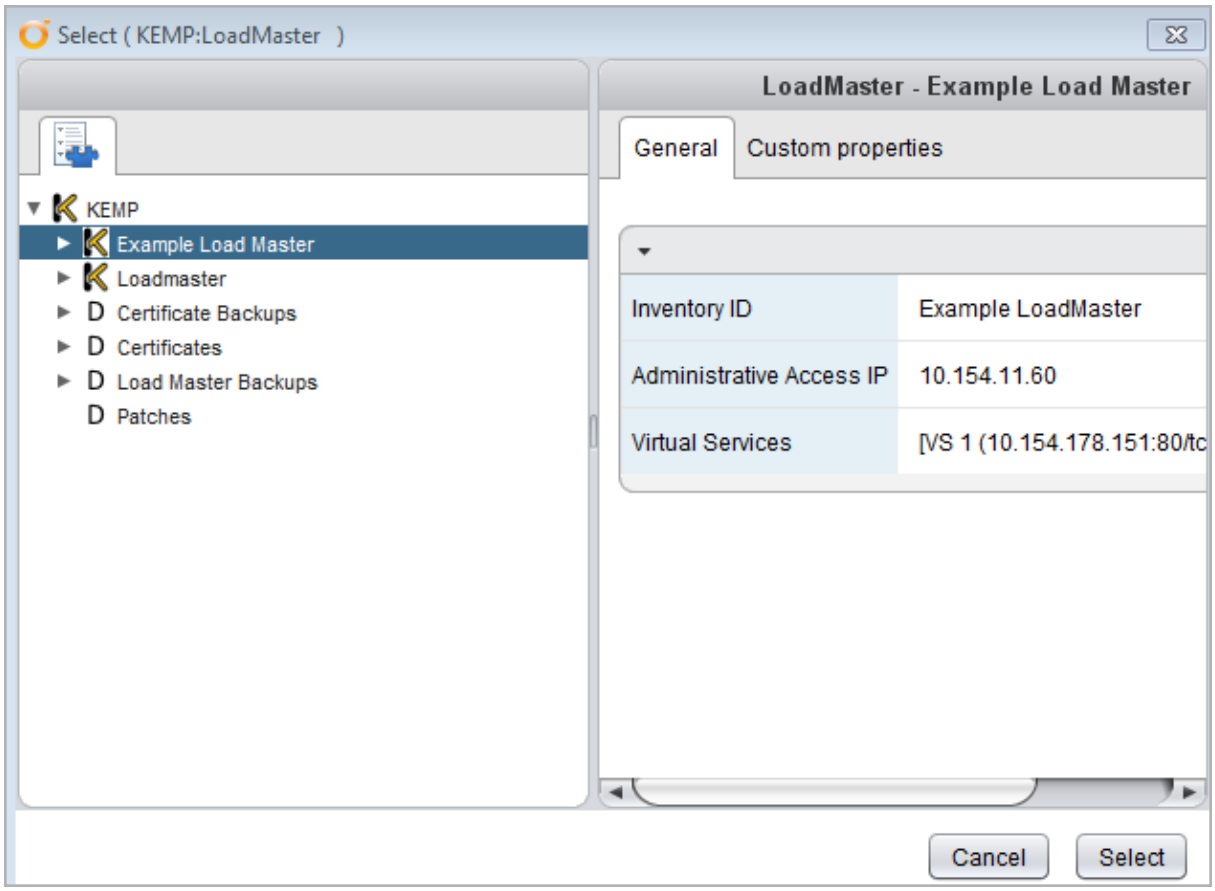
16. Wait for the restoration to complete.

3.4.14 Set Credentials

When a LoadMaster is added to Orchestrator via the **Add LoadMaster** command, the credentials are set. If, for any reason, the LoadMaster credentials which are saved in Orchestrator need to be updated (for example if the credentials have changed), the **Set Credentials** workflow can be run.

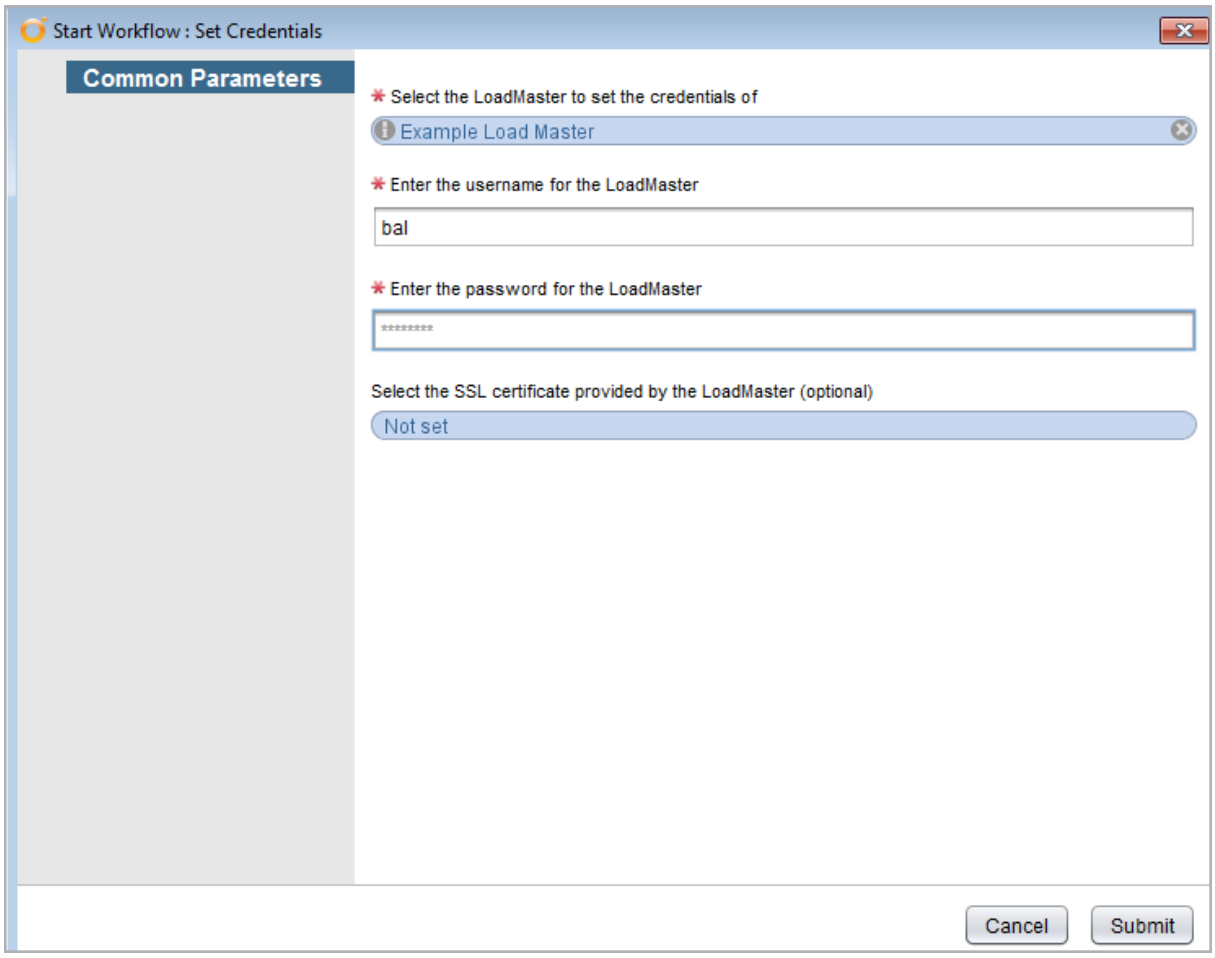


1. Click **Not set** in the **Select the LoadMaster to set the credentials of** field.



2. Expand the **Kemp** directory.

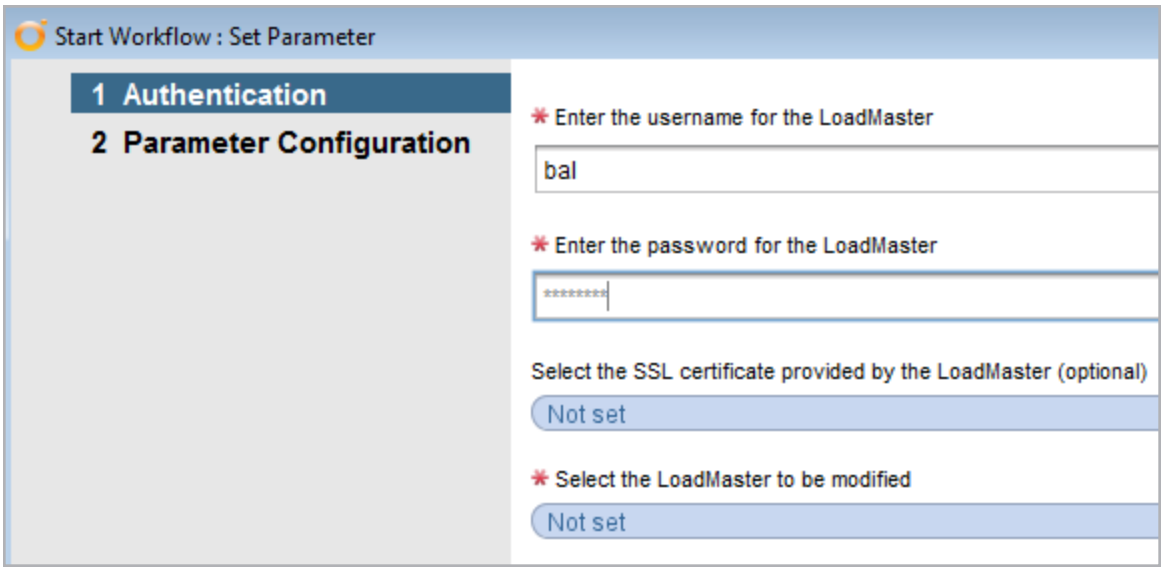
3. Select the relevant LoadMaster.
4. Click **Select**.



5. Enter the updated LoadMaster credentials.
6. Click **Submit**.

3.4.15 Set Parameter

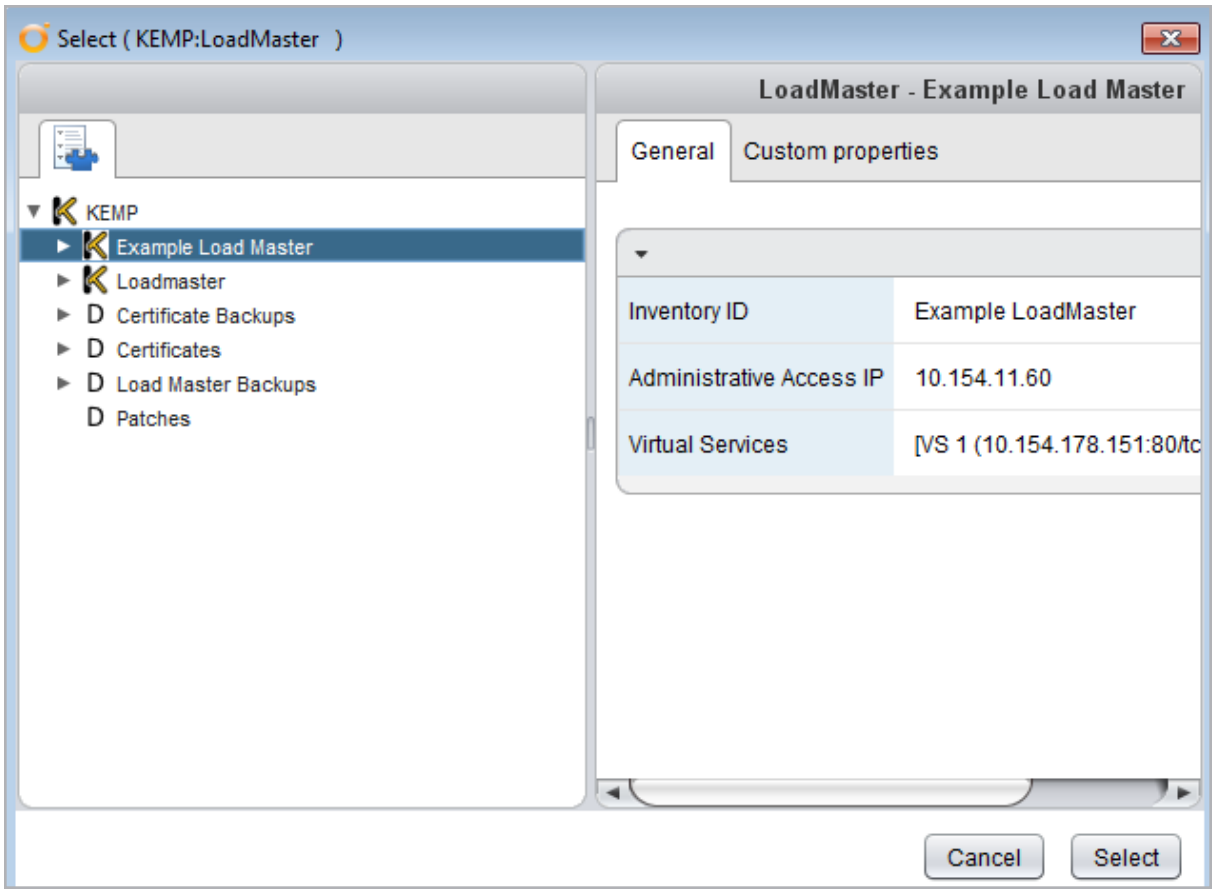
The **Set Parameter** workflow can be used to set a number of LoadMaster field values. For a list of parameter names that can be set, refer to **Appendix A - Get and Set Parameters**.



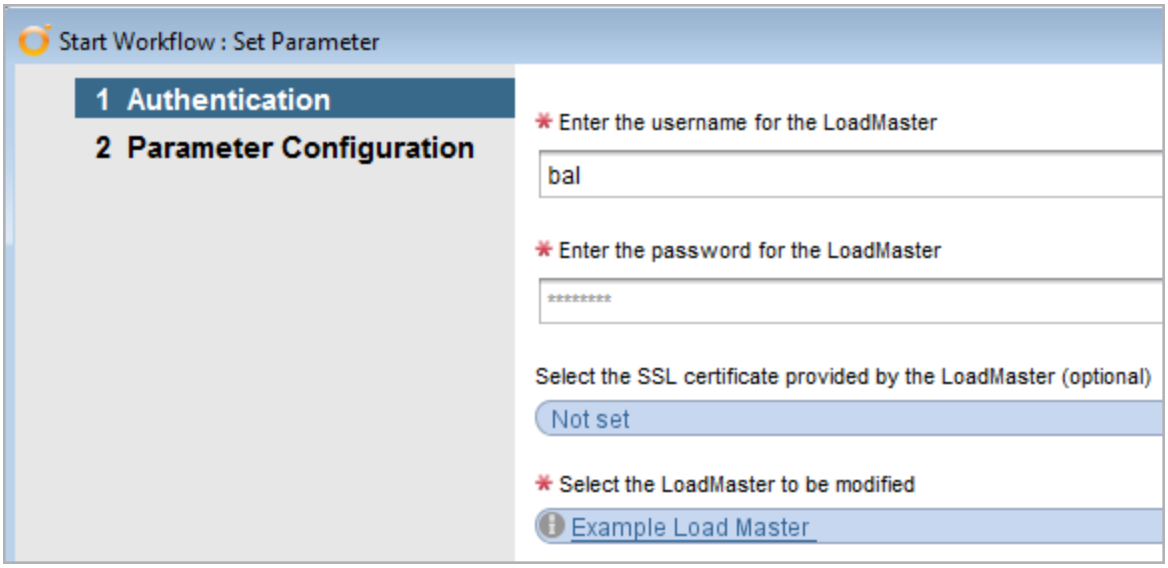
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

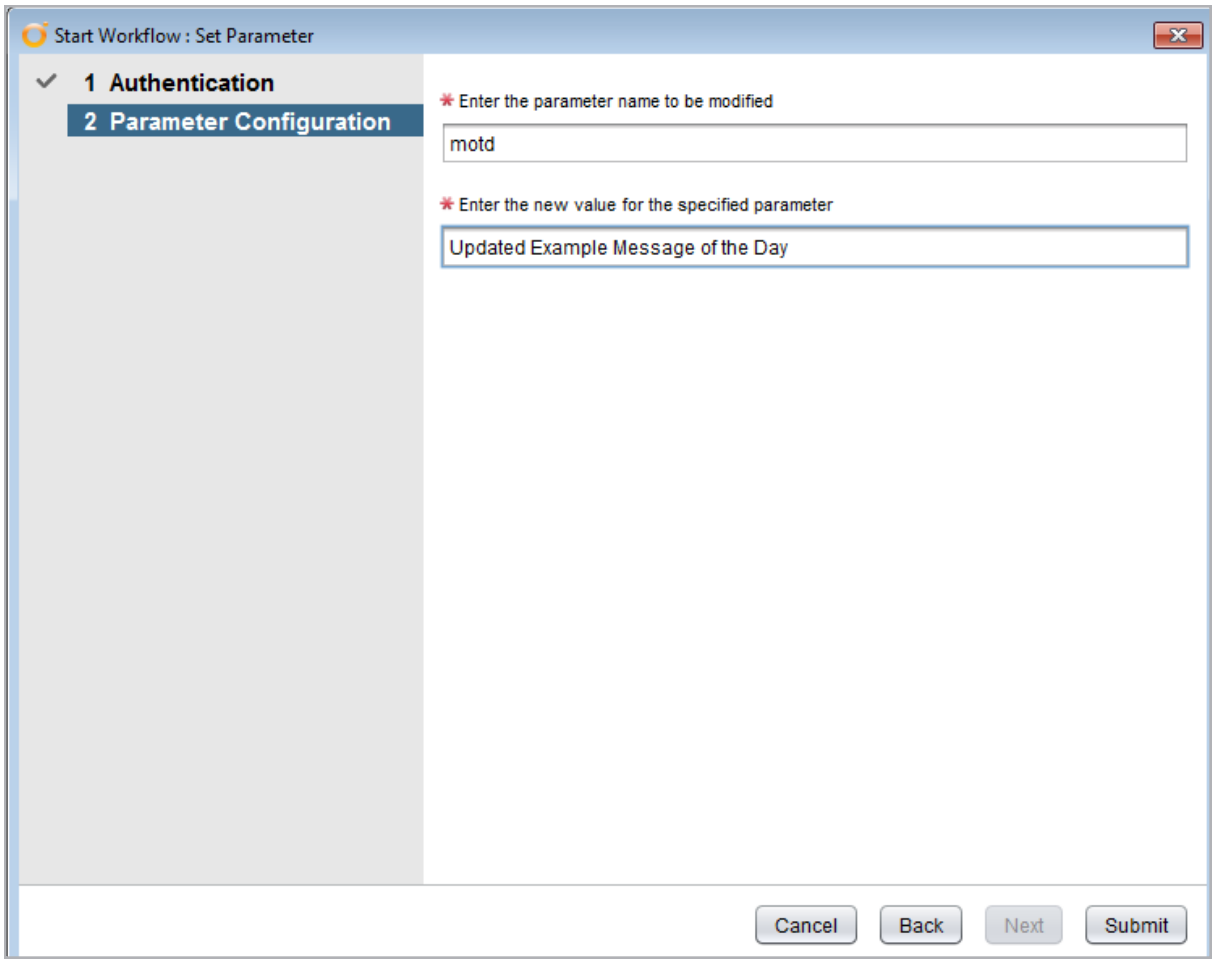
3. Click **Not set** in the **Select the LoadMaster to be modified** field.



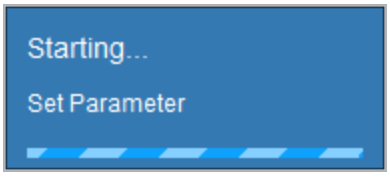
4. Expand the **Kemp** directory.
5. Select the relevant LoadMaster.
6. Click **Select**.



7. Click **Parameter Configuration**.



8. Enter the name of the parameter to be modified.
9. Enter the new value for the specified parameter.
10. Click **Submit**.



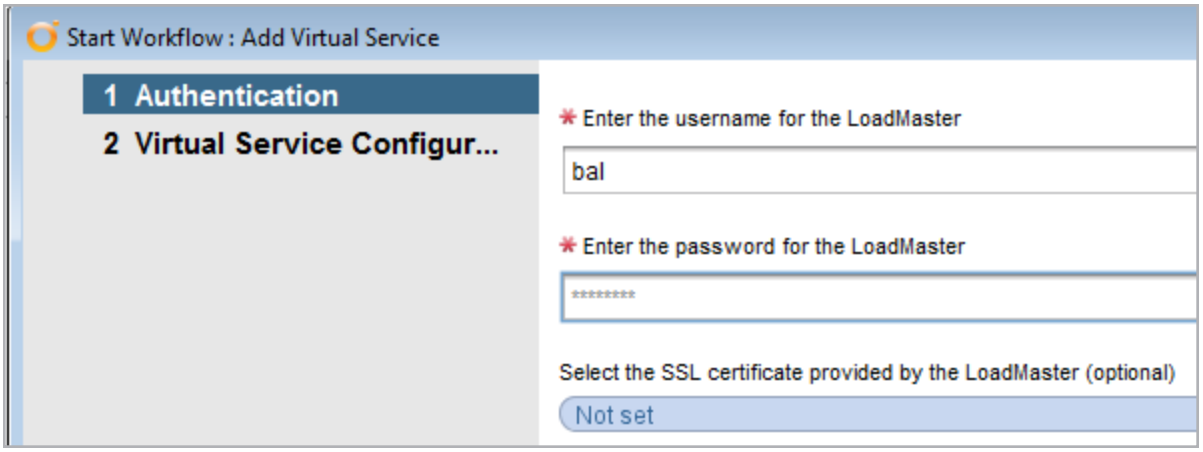
11. Wait for the parameter to be set.

3.5 Virtual Services

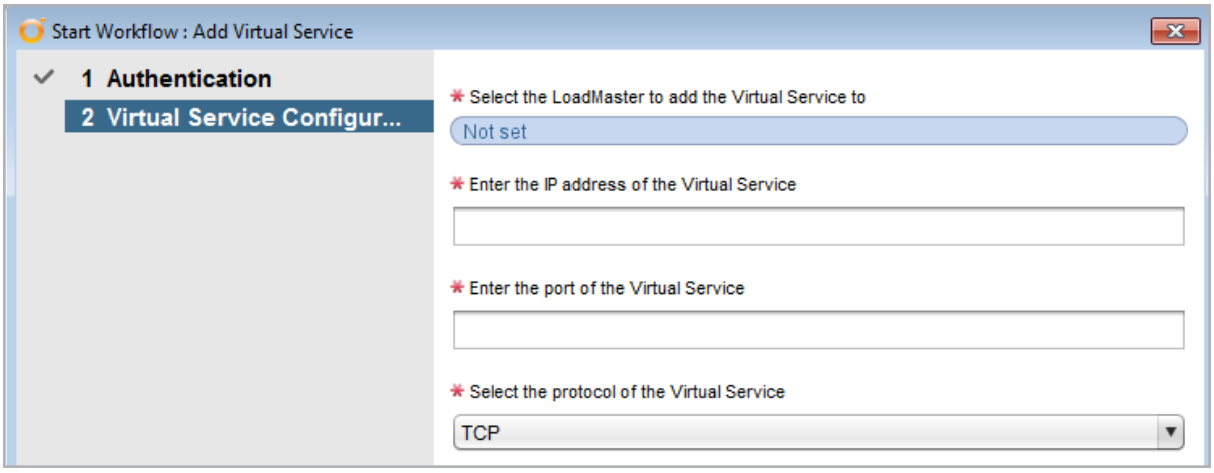
A number of tasks can be performed in relation to Virtual Services, such as adding and removing them. Refer to the sections below for further details.

3.5.1 Add Virtual Service

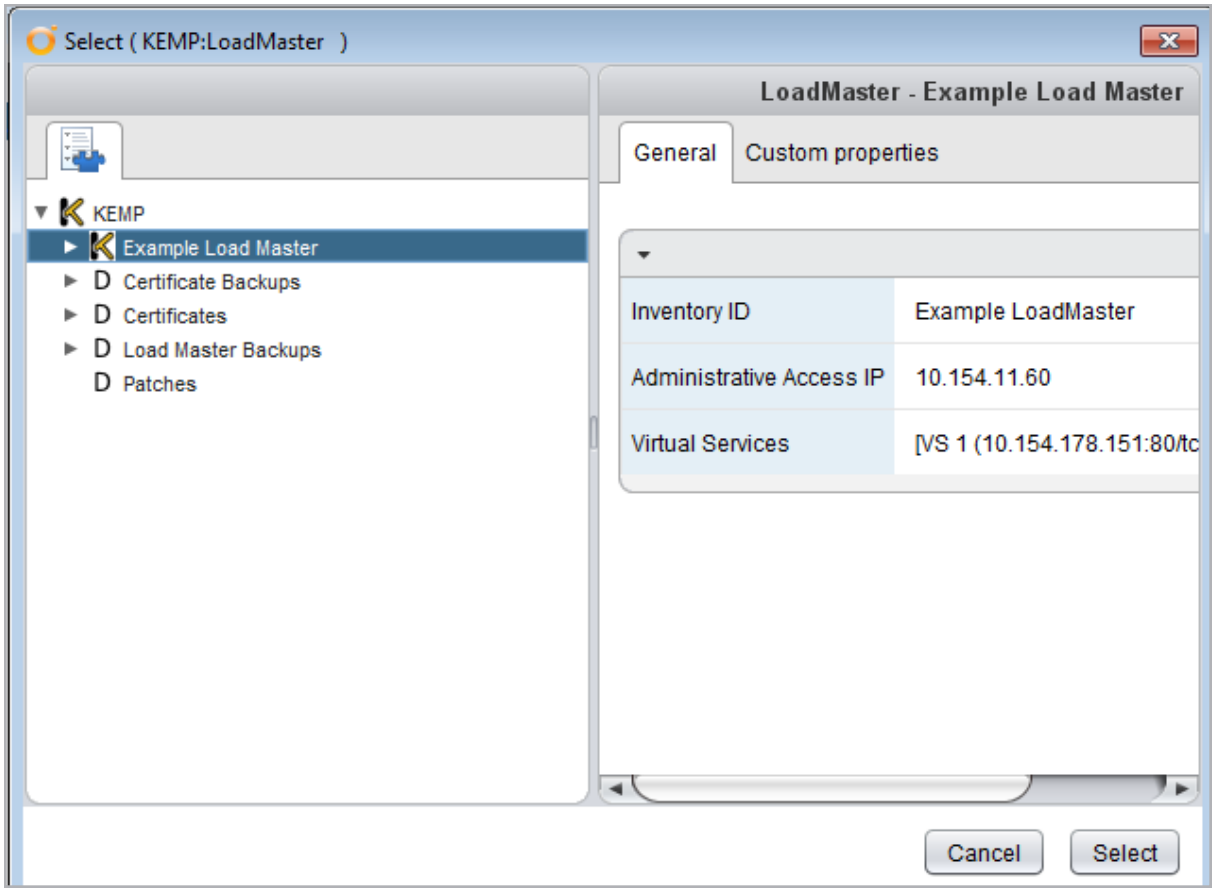
A Virtual Service can be added to a LoadMaster via Orchestrator by running the **Add Virtual Service** command.



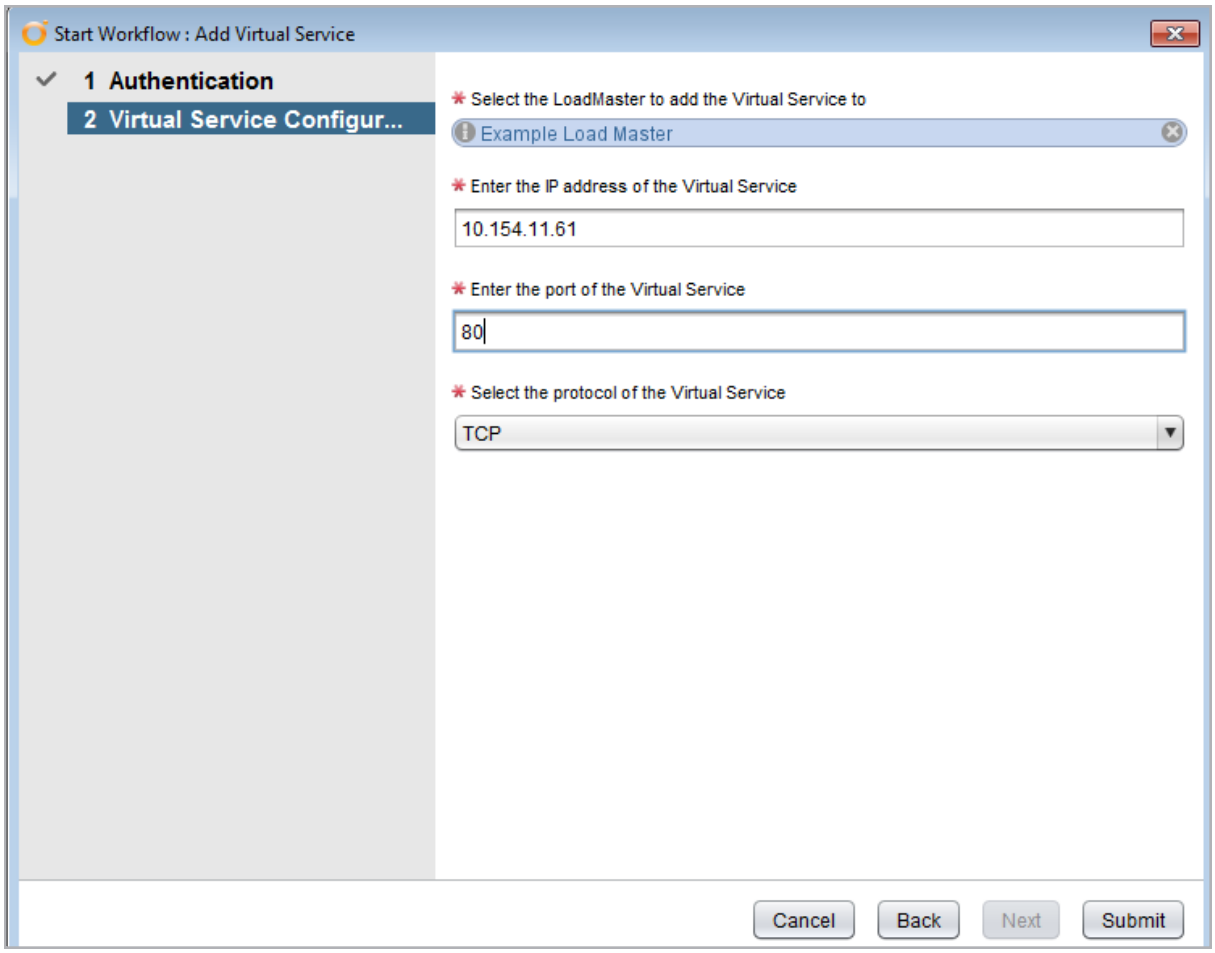
1. Enter the username and password to access the LoadMaster.
2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).
3. Click **Virtual Service Configuration**.



4. Click **Not set**.



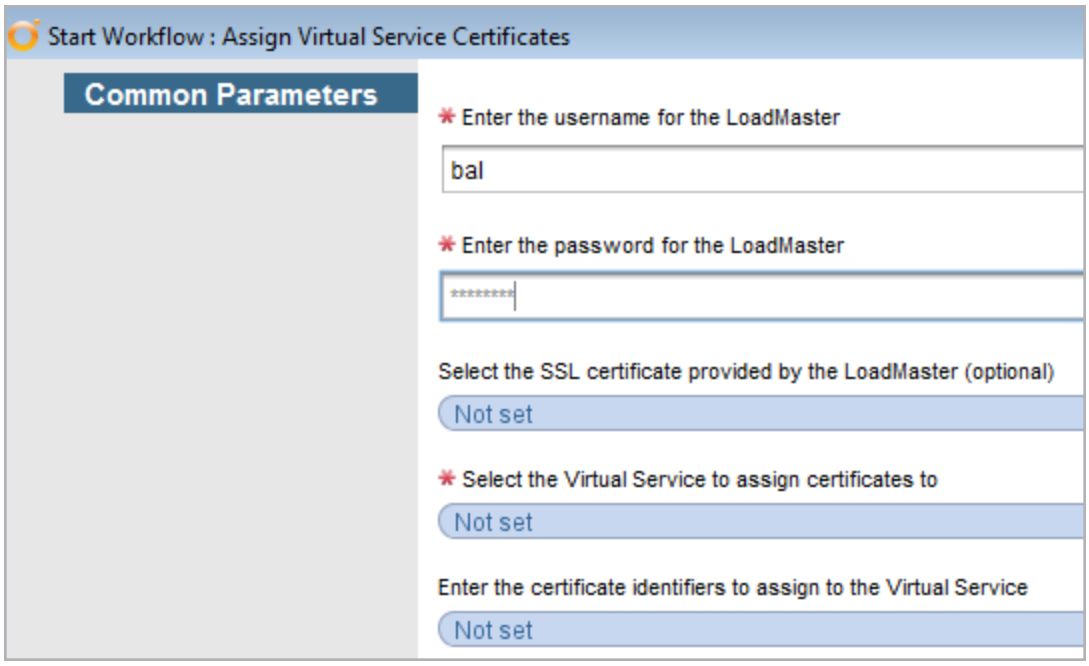
5. Expand the **Kemp** directory.
6. Select the relevant LoadMaster.
7. Click **Select**.



8. Enter a valid IP address in the Enter the IP address of the Virtual Service text box.
9. Enter the desired port in the **Enter the port of the Virtual Service** text box.
10. Select the relevant protocol from the drop-down list.
11. Click **Submit**.

3.5.2 Assign Virtual Service Certificates

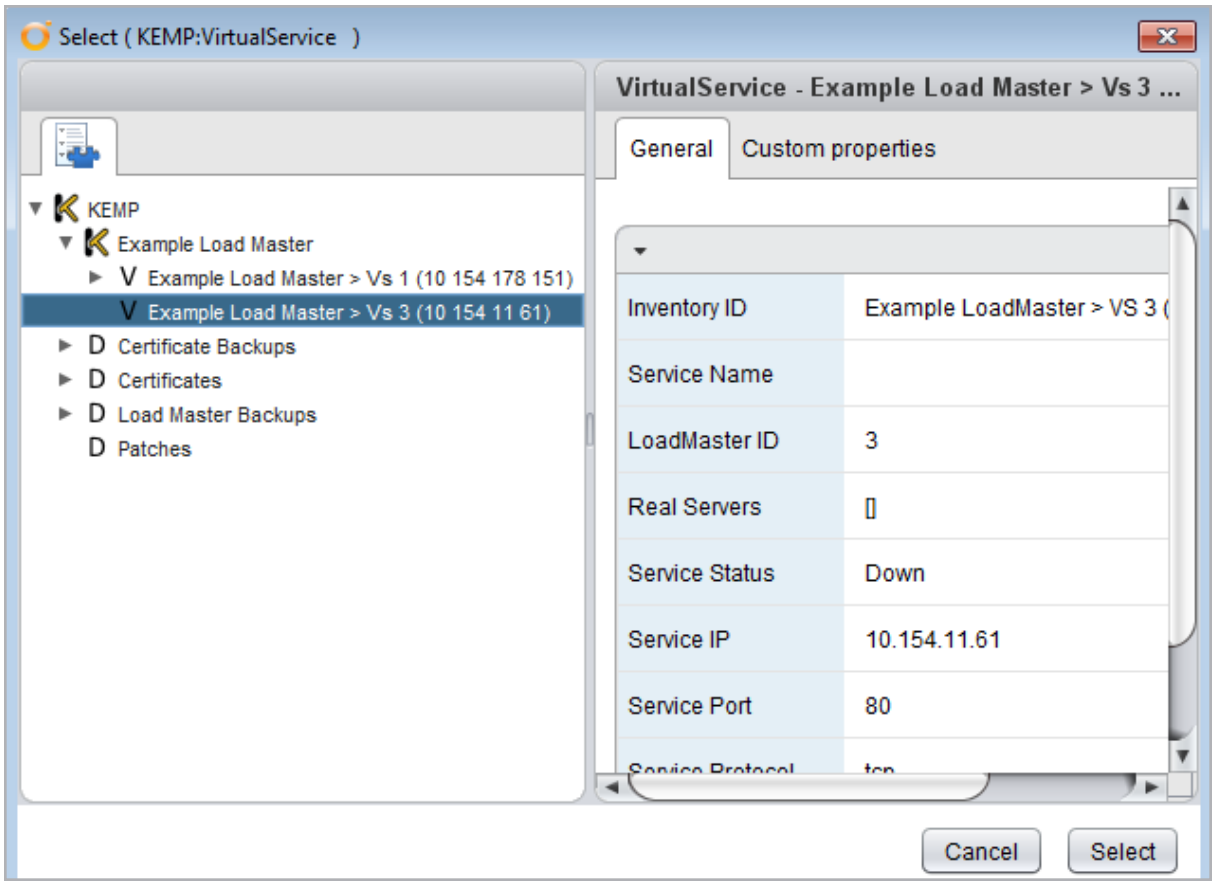
Certificates can be assigned to a Virtual Service via Orchestrator. To do this, run the **Assign Virtual Service Certificates** command.



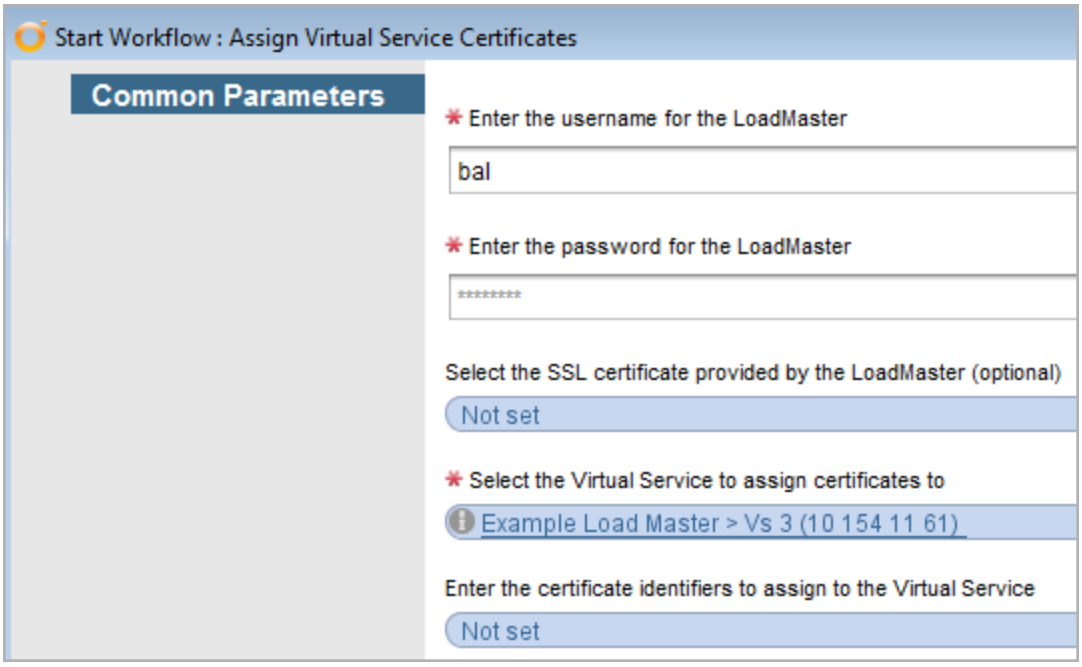
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

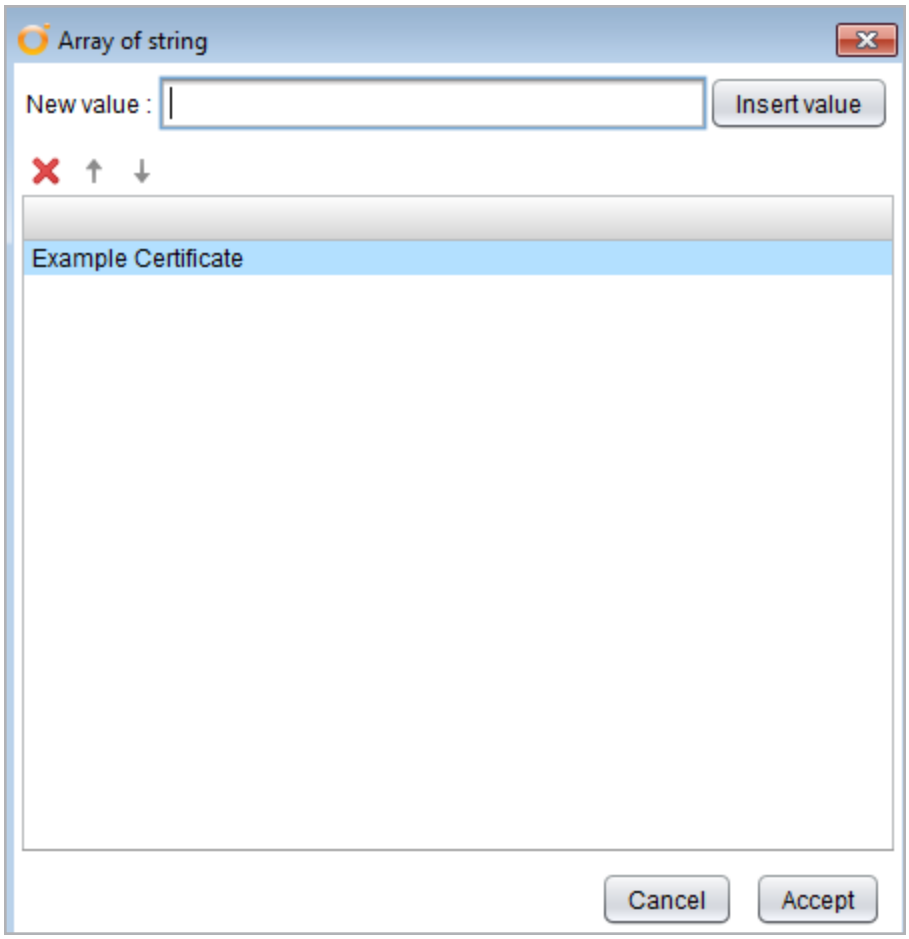
3. Click **Not set** in the Select the **Virtual Service to assign certificates to** field.



4. Expand the **Kemp** directory.
5. Expand the relevant LoadMaster.
6. Select the relevant Virtual Service.
7. Click **Select**.



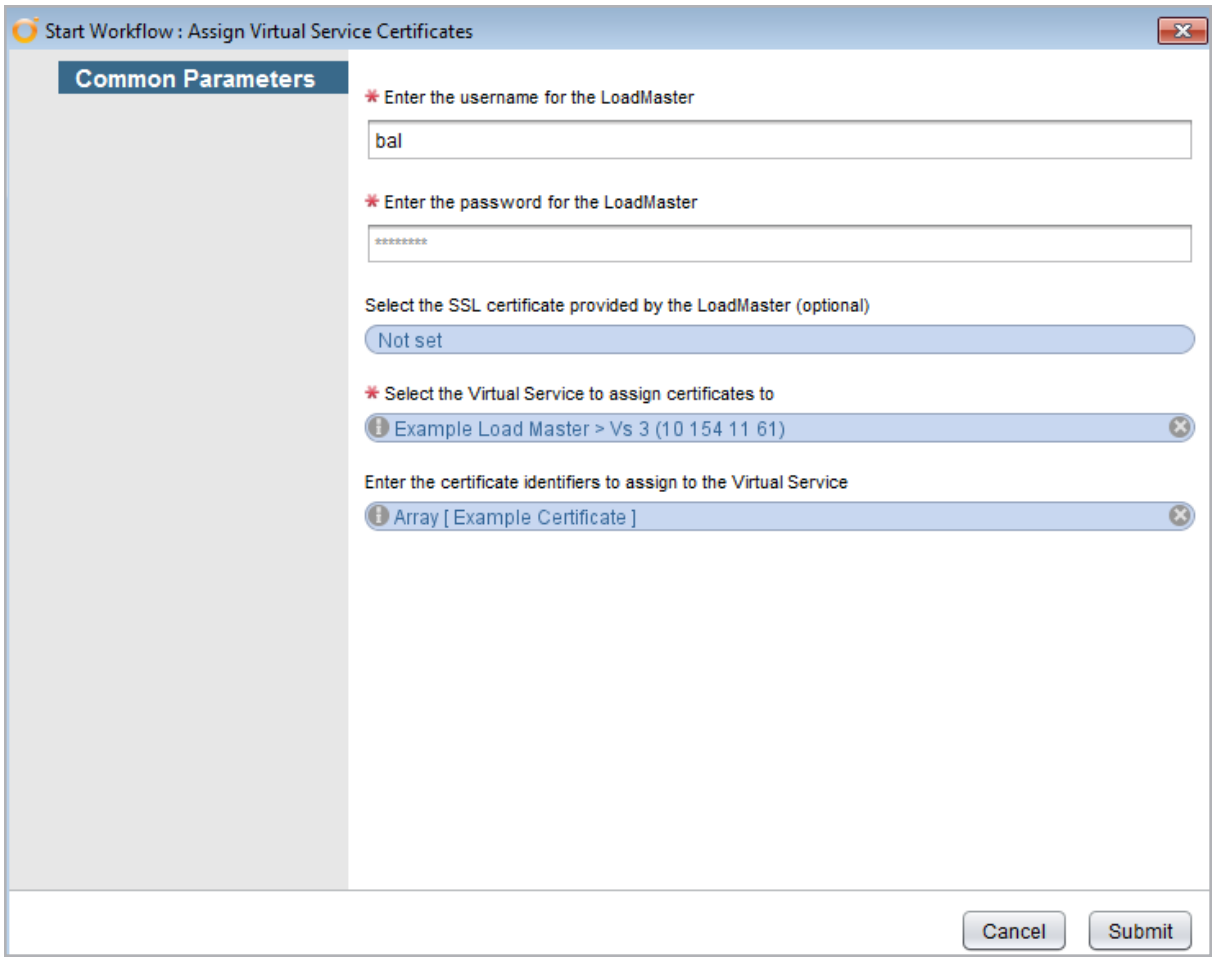
8. Click **Not set** in the **Enter the certificate identifiers to assign to the Virtual Service** field.



9. In the **New value** text box, enter the certificate identifier (friendly name) of the certificate to be assigned.

10. Click **Insert value**.

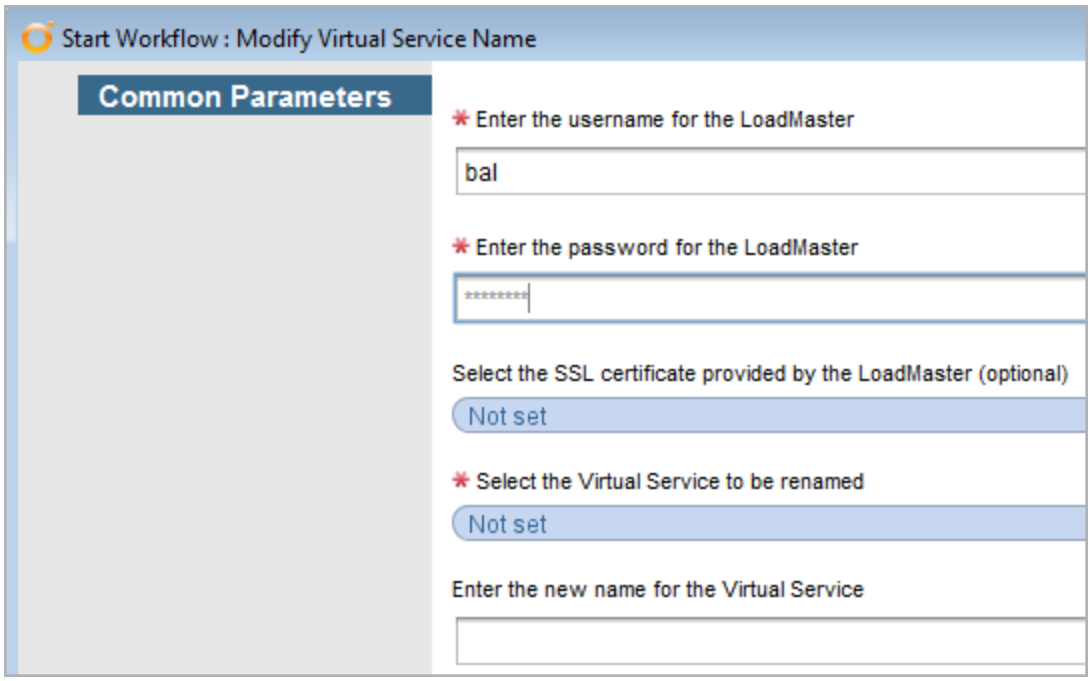
11. Click **Accept**.



12. Click **Submit**.

3.5.3 Modify Virtual Service Name

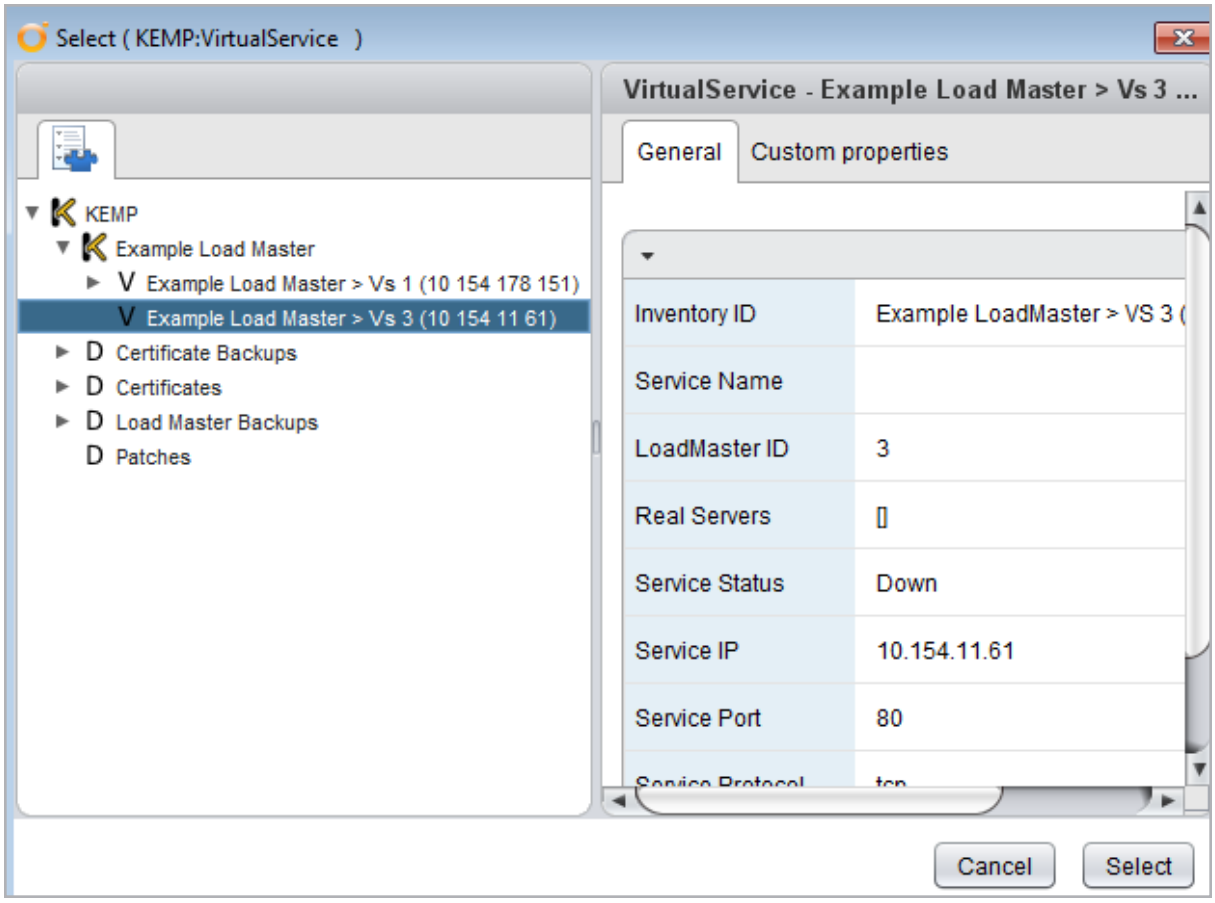
The name of a Virtual Service can be modified using the **Modify Virtual Service Name** workflow.



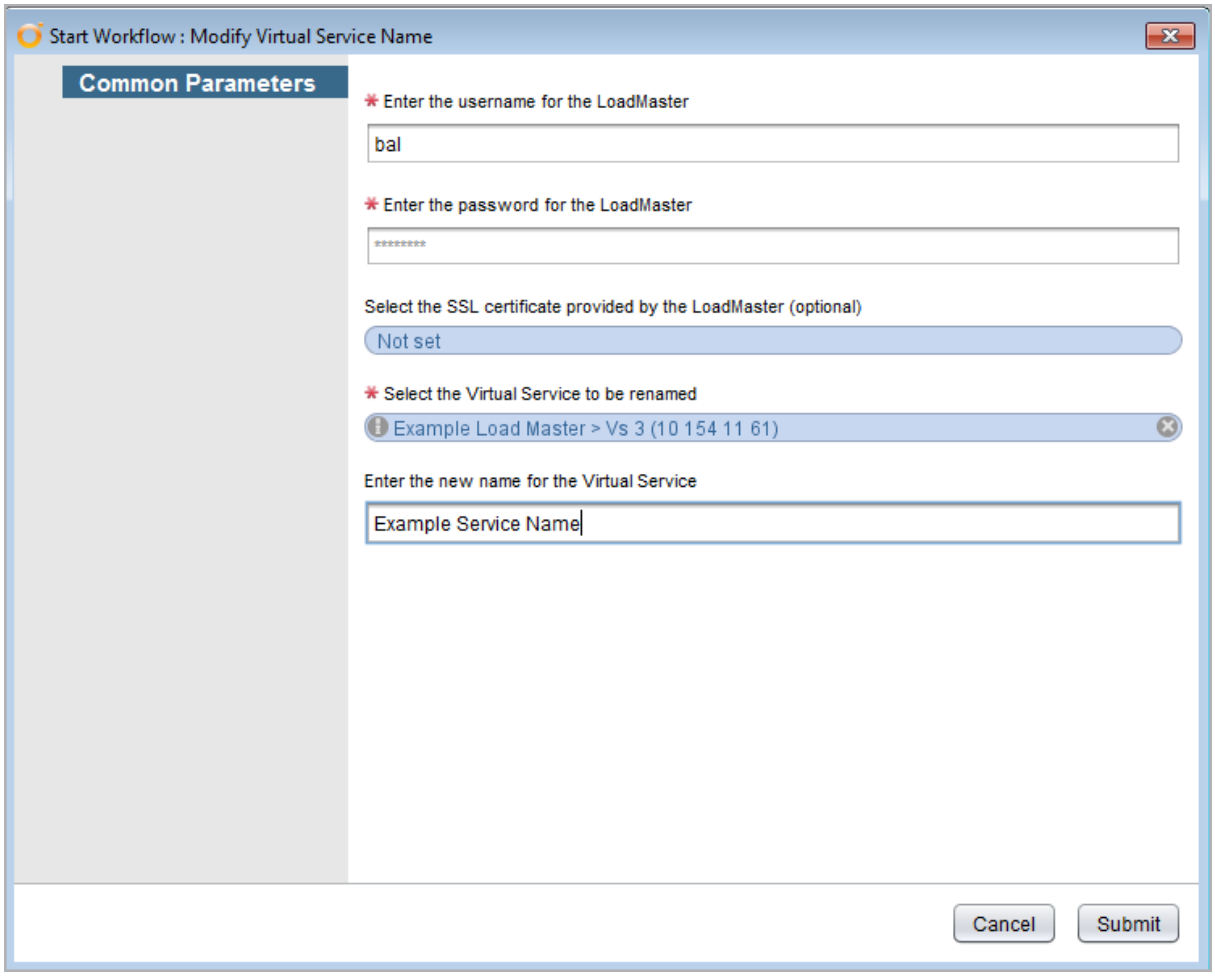
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

3. Click **Not set** in the **Select the Virtual Service to be renamed** field.



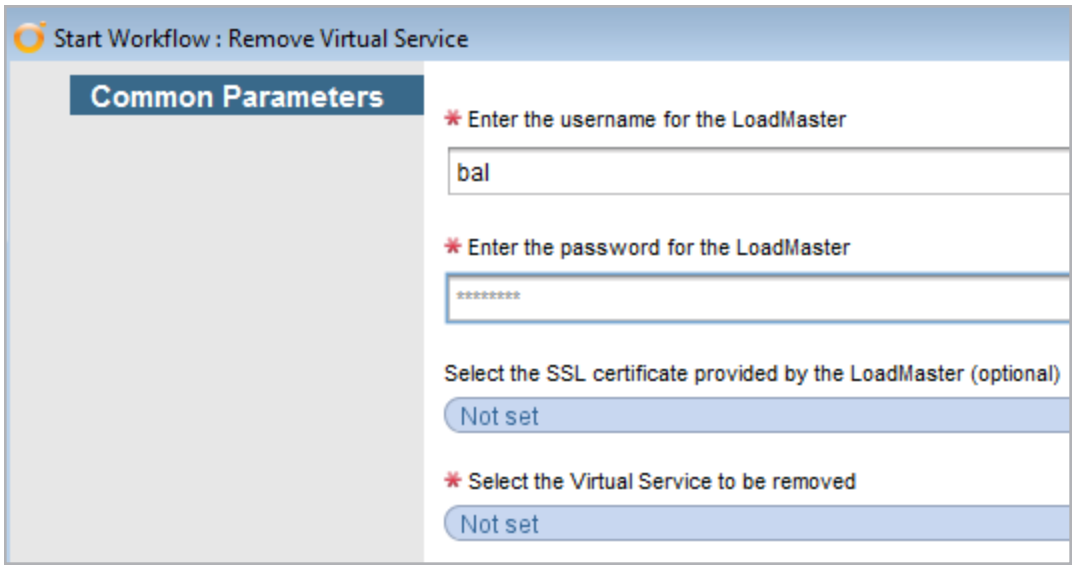
4. Expand the **Kemp** directory.
5. Expand the relevant LoadMaster.
6. Select the relevant Virtual Service.
7. Click **Select**.



8. Enter the new name for the Virtual Service.
9. Click **Submit**.

3.5.4 Remove Virtual Service

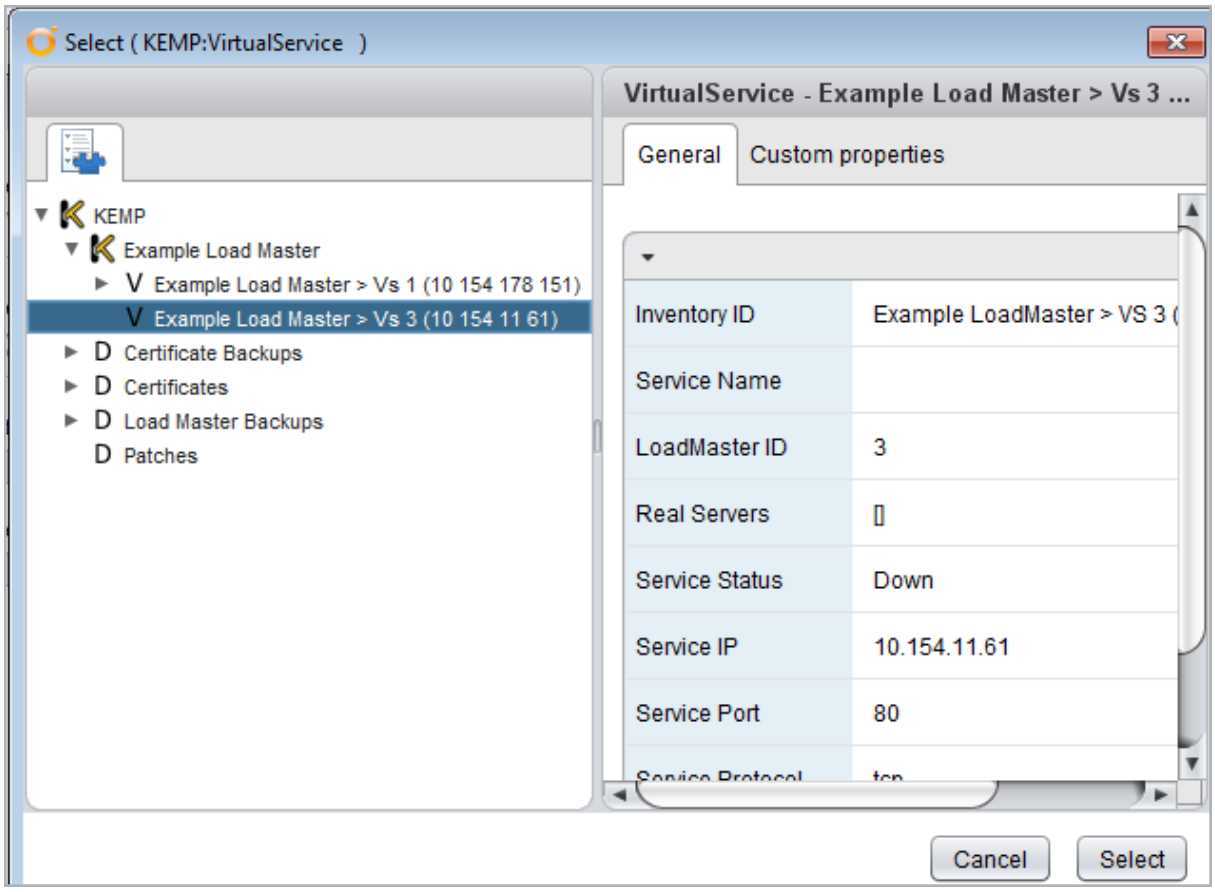
A Virtual Service can be deleted via Orchestrator by running the **Remove Virtual Service** workflow.



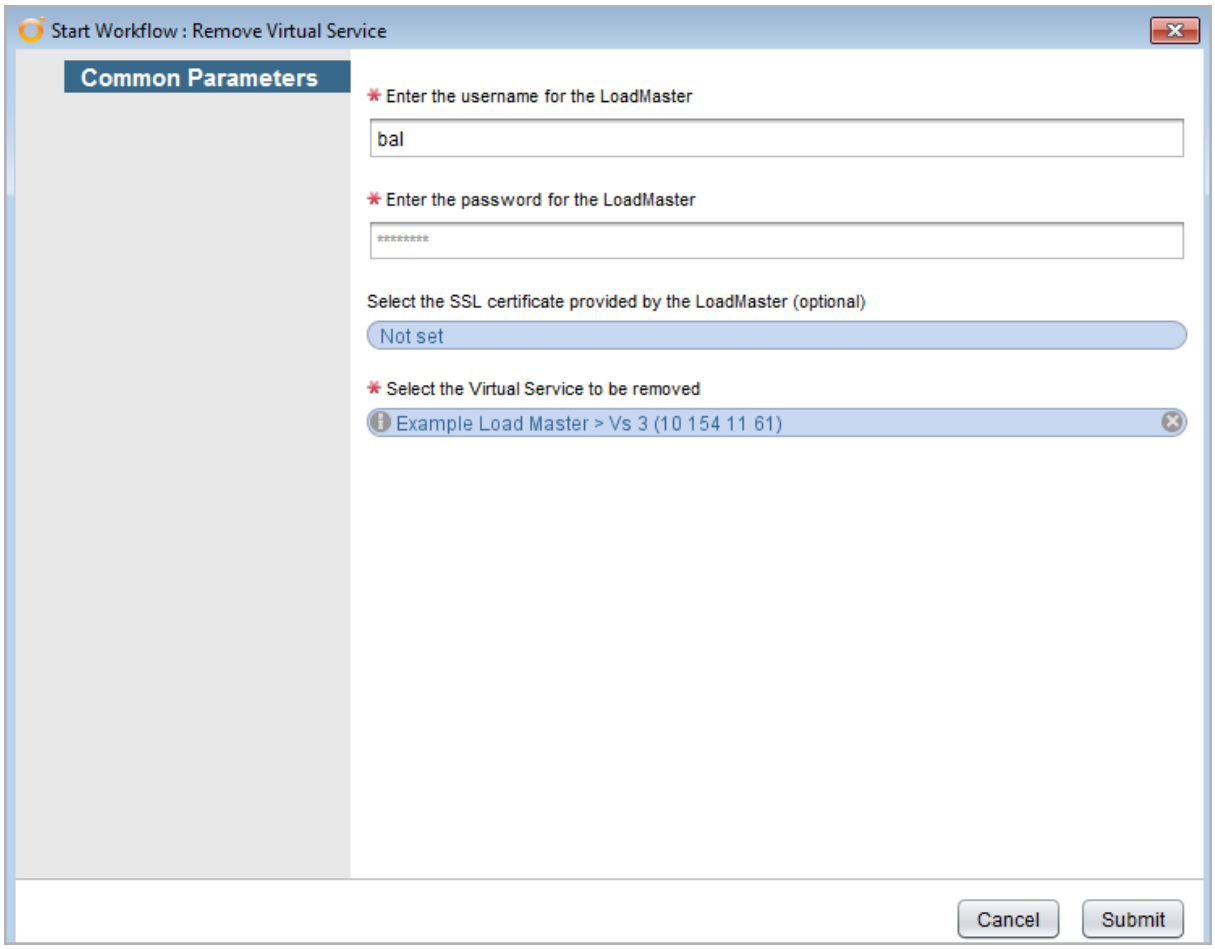
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

3. Click **Not set** in the **Select the Virtual Service to be removed** field.



4. Expand the **Kemp** directory.
5. Expand the relevant LoadMaster.
6. Select the relevant Virtual Service.
7. Click **Select**.



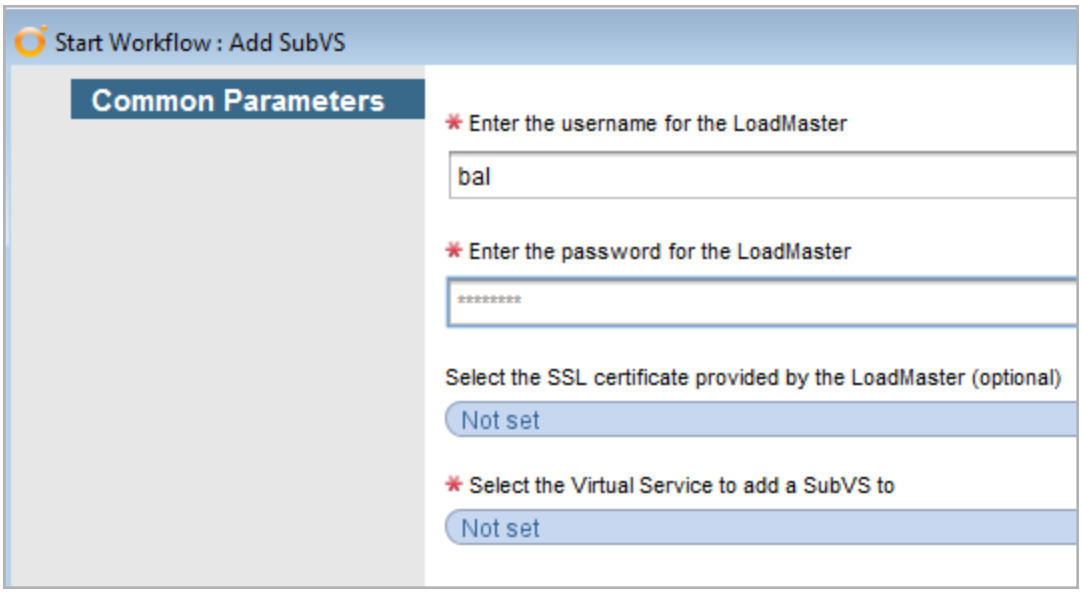
8. Click **Submit**.

3.6 Sub Virtual Services

A number of tasks can be performed in relation to SubVSes, such as adding and removing a SubVS. Refer to the sections below for further details.

3.6.1 Add SubVS

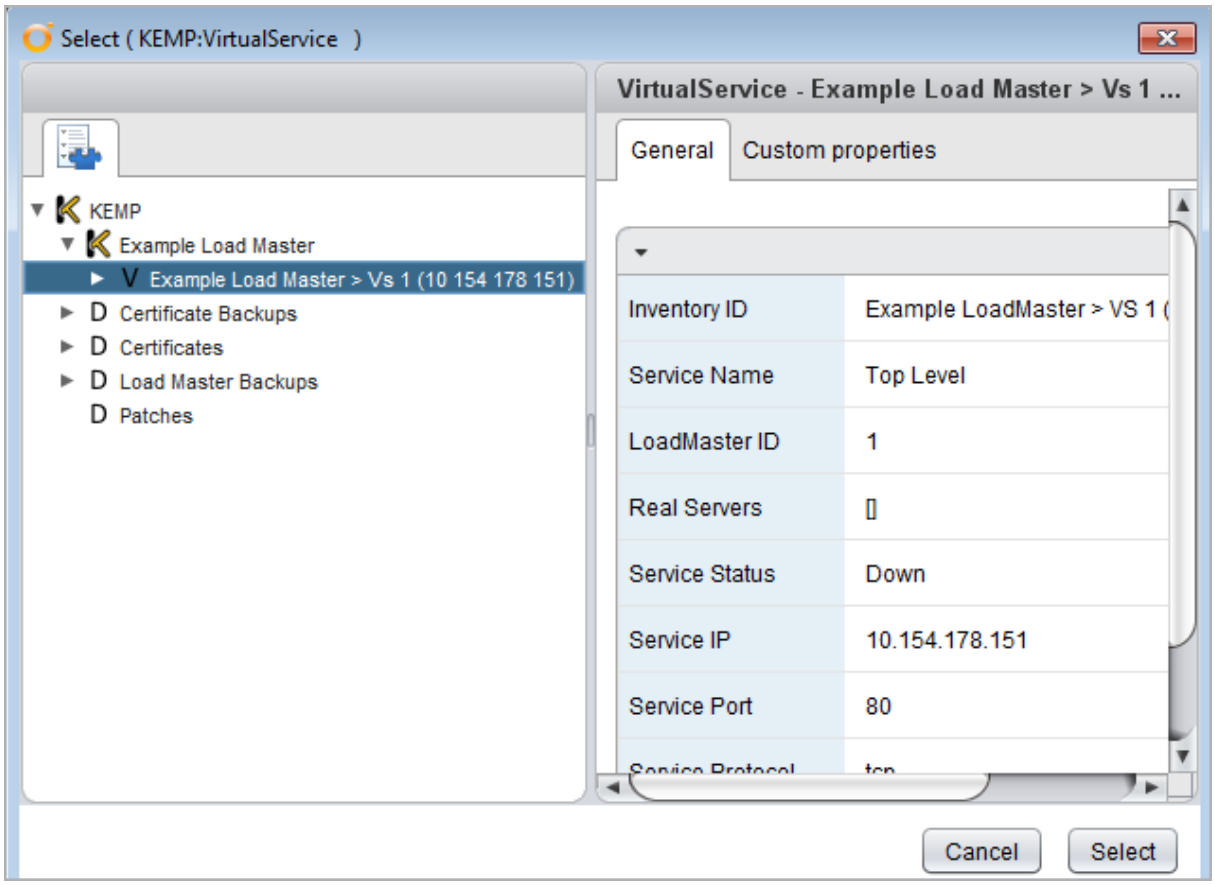
A SubVS can be added by running the **Add SubVS** workflow.



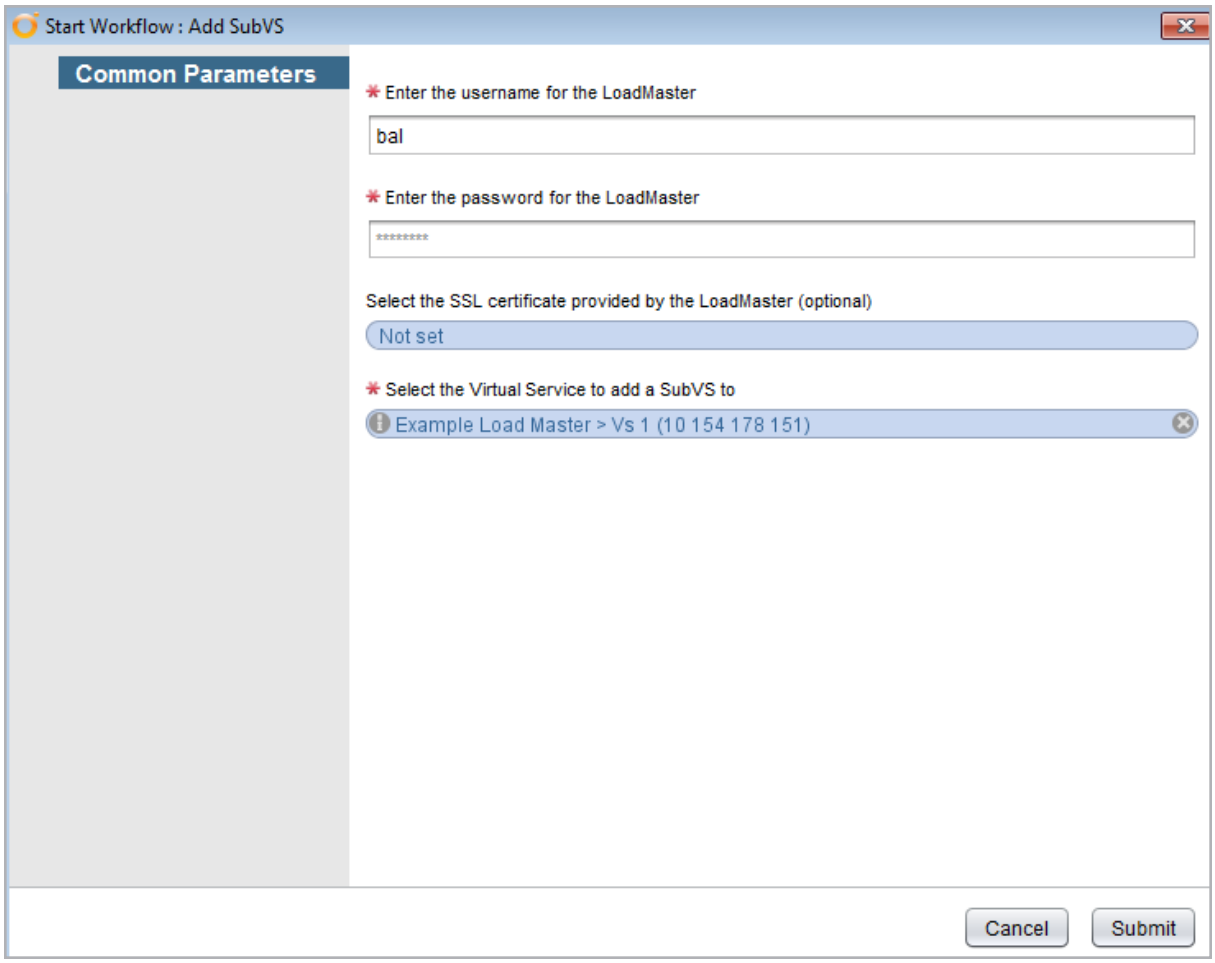
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

3. Click **Not set** in the **Select the Virtual Service to add a SubVS to** field.



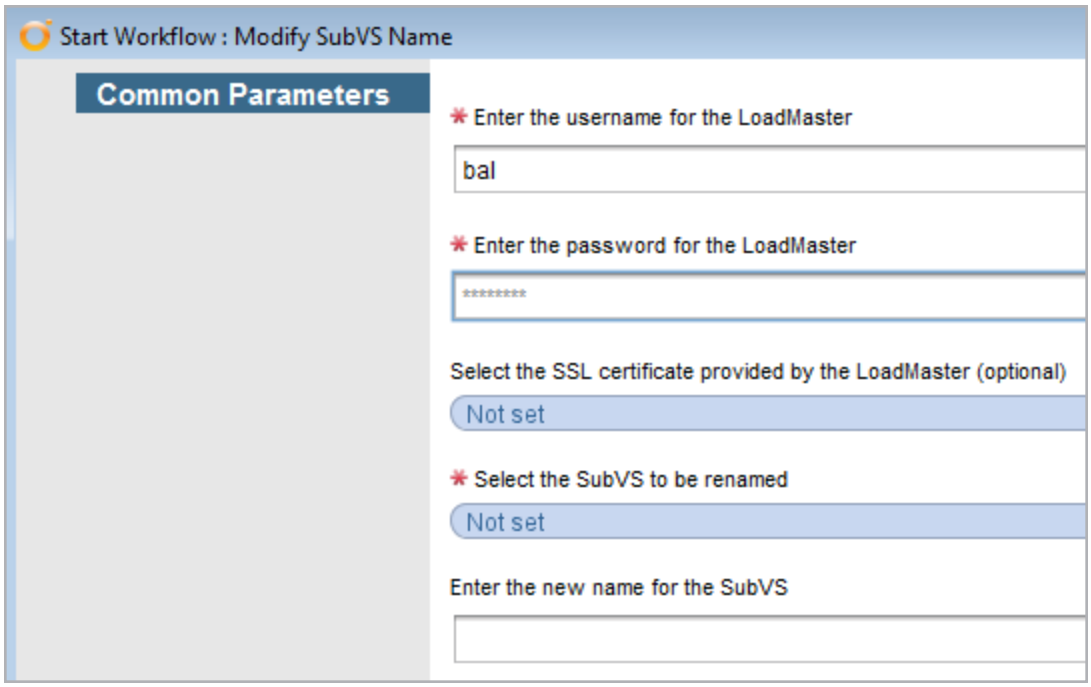
4. Expand the **Kemp** directory.
5. Expand the relevant LoadMaster.
6. Select the relevant Virtual Service.
7. Click **Select**.



8. Click **Submit**.

3.6.2 Modify SubVS Name

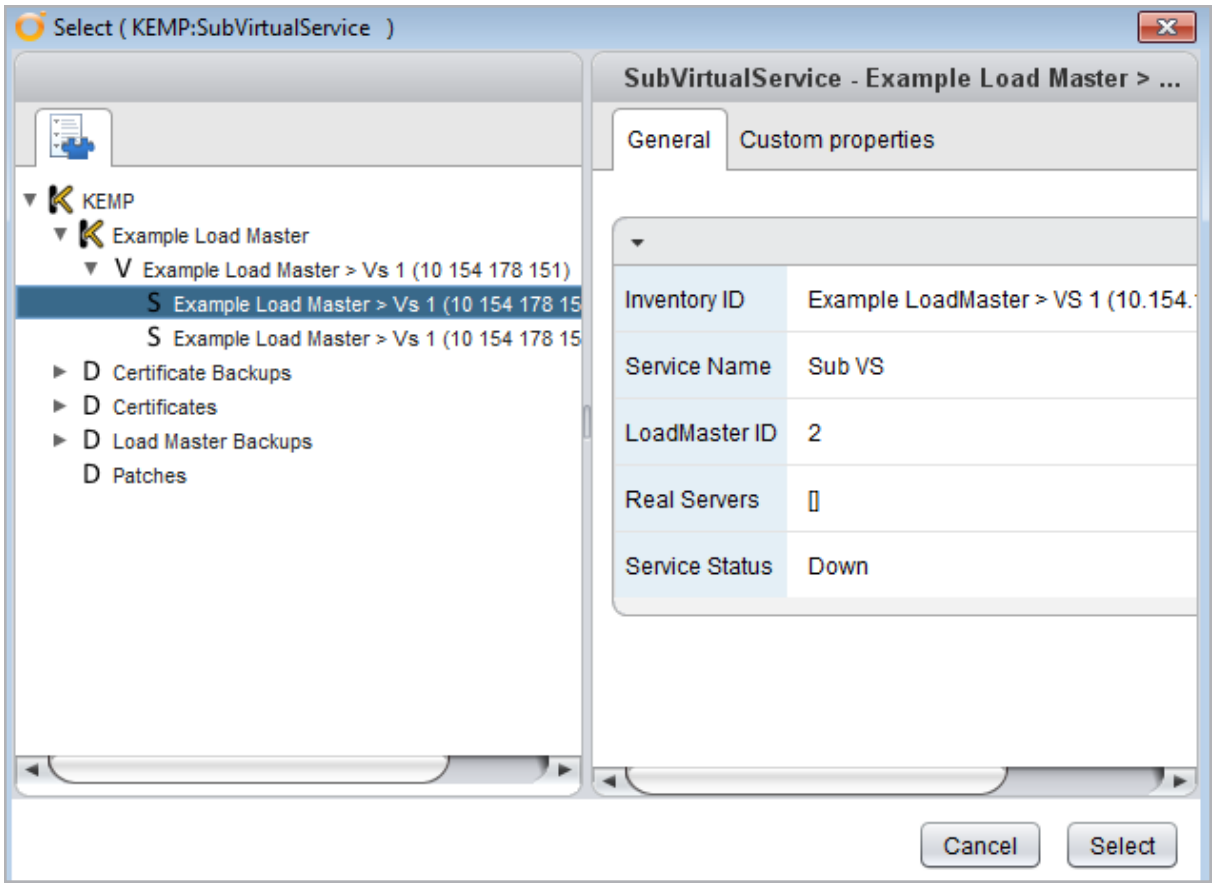
The name of a SubVS can be modified using the **Modify SubVS Name** workflow.



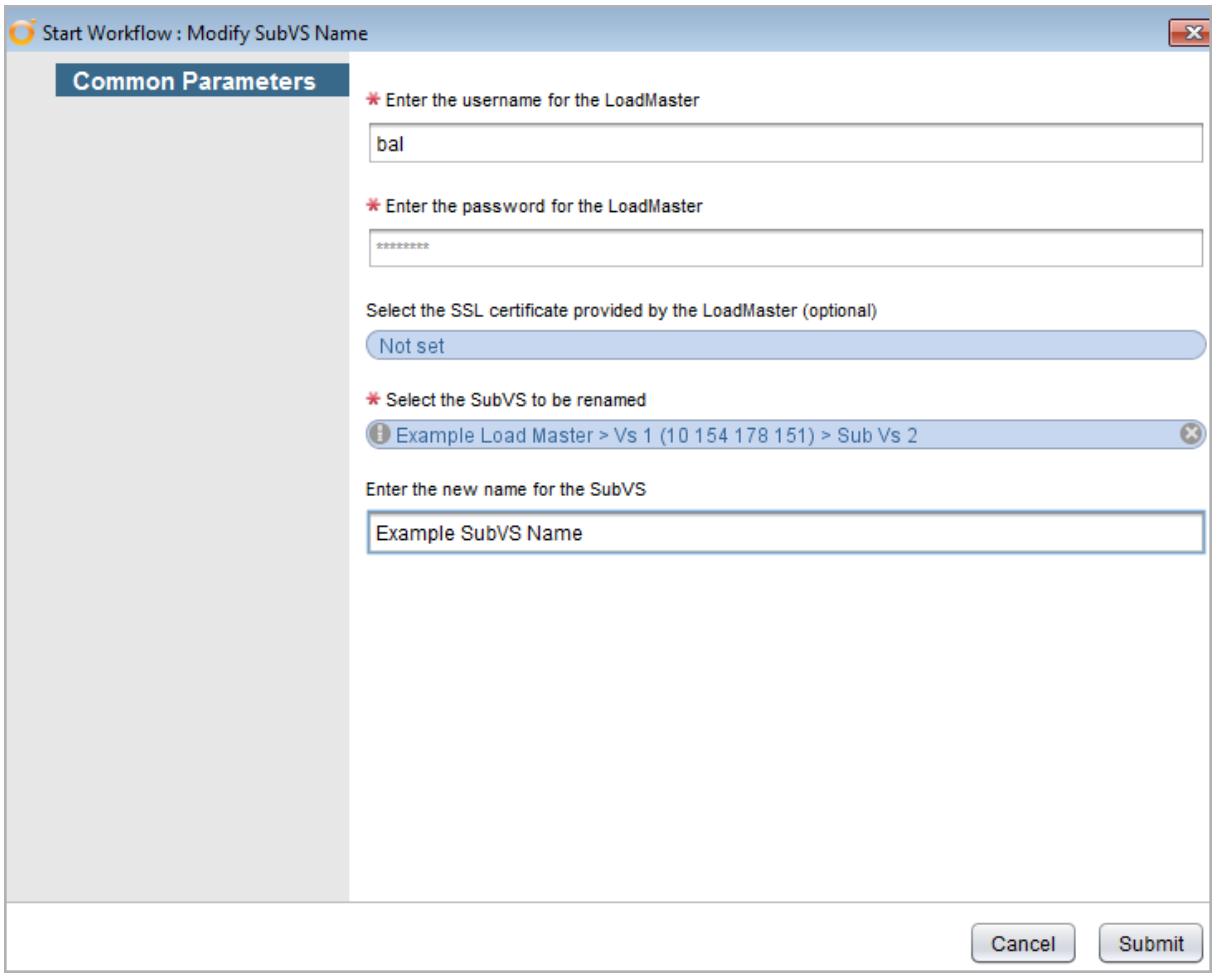
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

3. Click **Not set** in the **Select the SubVS to be renamed** field.



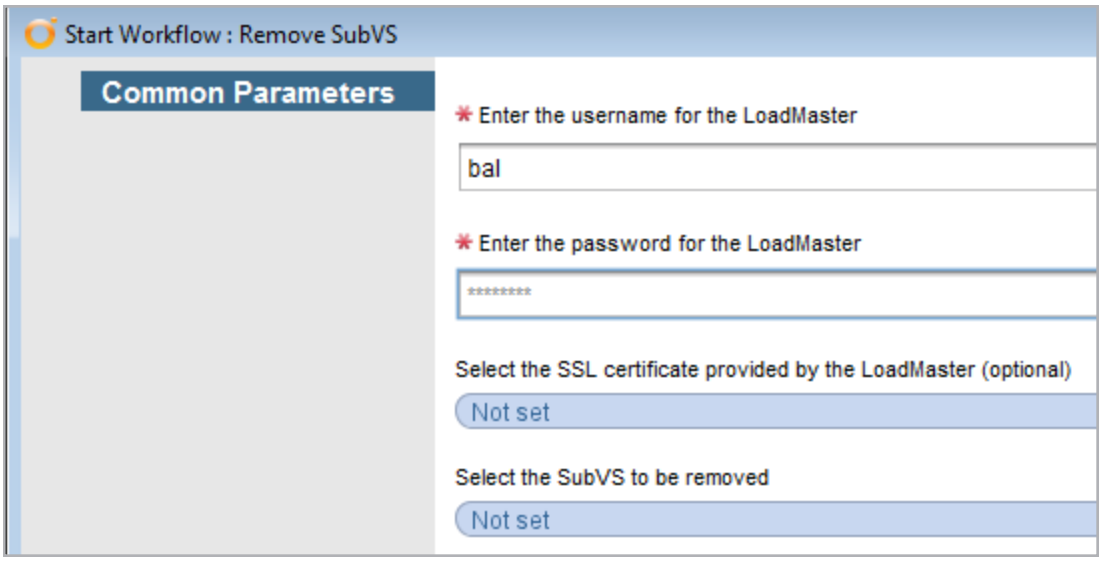
4. Expand the **Kemp** directory.
5. Expand the relevant LoadMaster.
6. Select the relevant SubVS.
7. Click **Select**.



8. Enter the new name for the SubVS.
9. Click **Submit**.

3.6.3 Remove SubVS

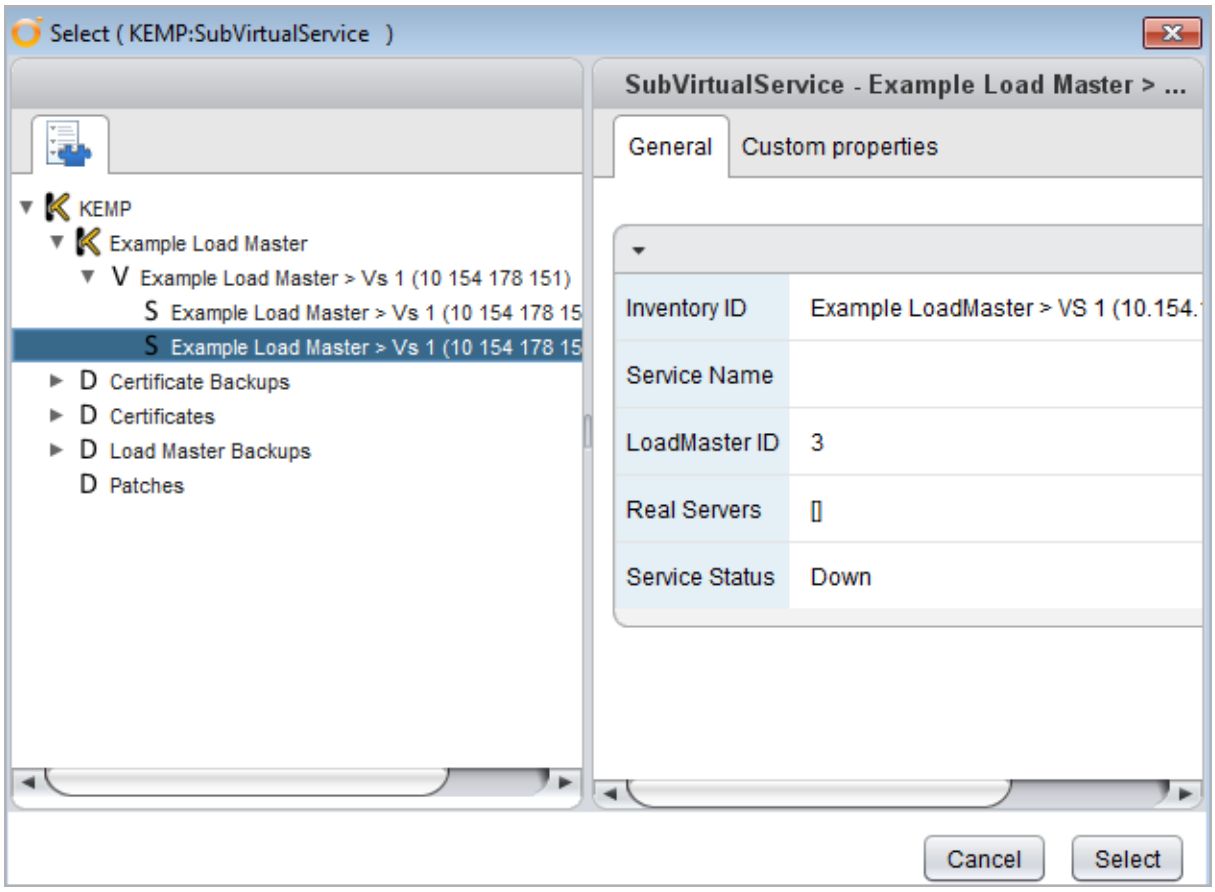
A SubVS can be deleted via Orchestrator by running the **Remove SubVS** command.



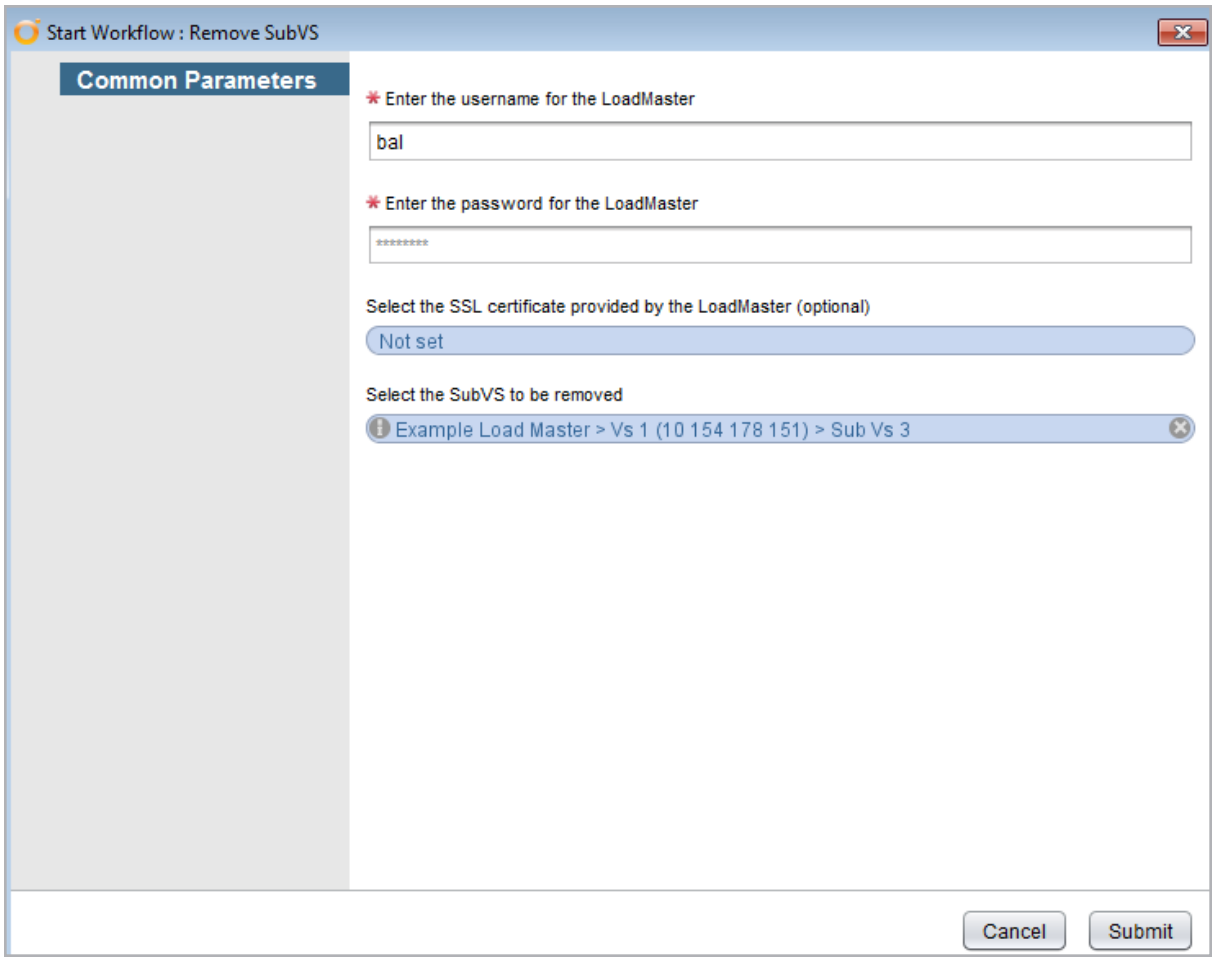
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

3. Click **Not set** in the **Select the SubVS to be removed** field.



4. Expand the **Kemp** directory.
5. Expand the relevant LoadMaster.
6. Expand the relevant Virtual Service.
7. Select the relevant SubVS.
8. Click **Select**.



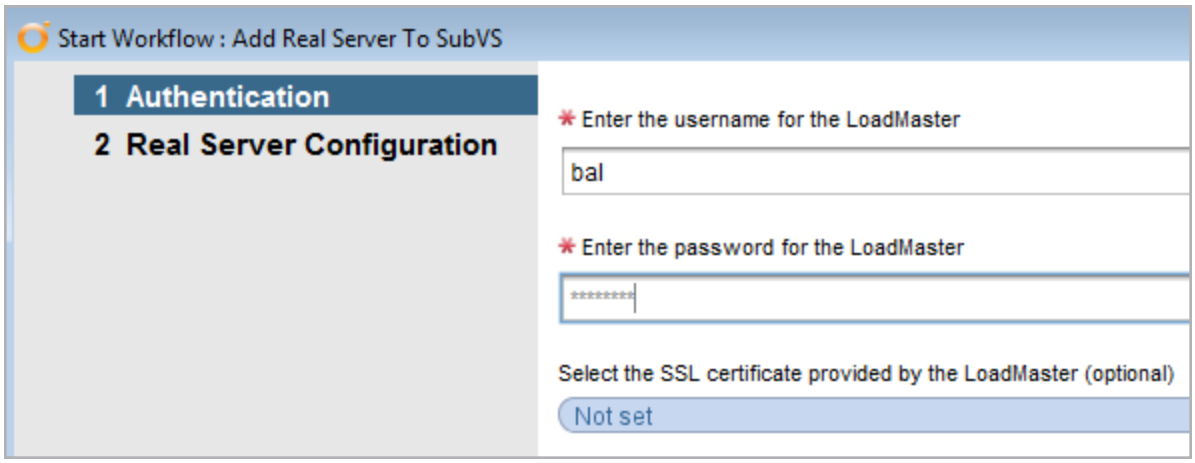
9. Click **Submit**.

3.7 Real Servers

A number of tasks can be performed in relation to Real Servers, such as adding a Real Server to a Virtual Service or removing a Real Server. Refer to the sections below for further details.

3.7.1 Add Real Server to Sub Virtual Service

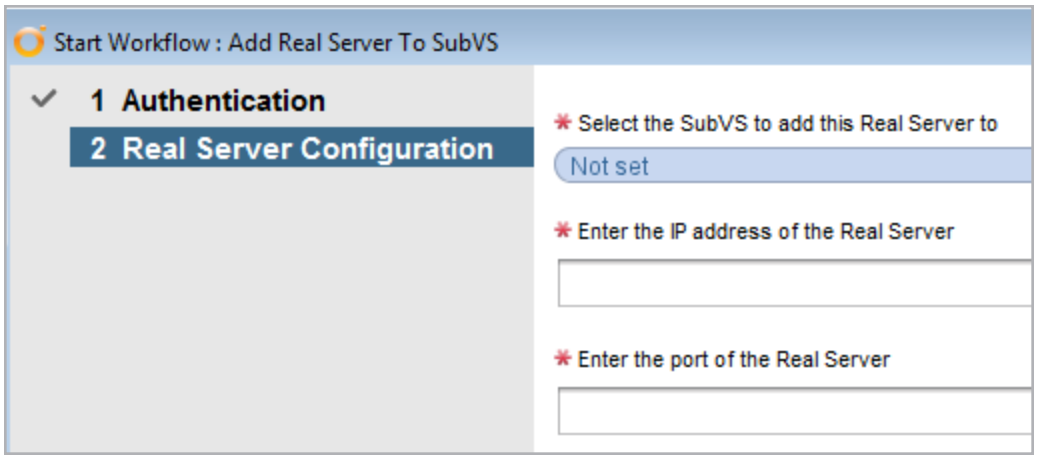
A Real Server can be added to a SubVS by running the **Add Real Server to Sub Virtual Service** workflow.



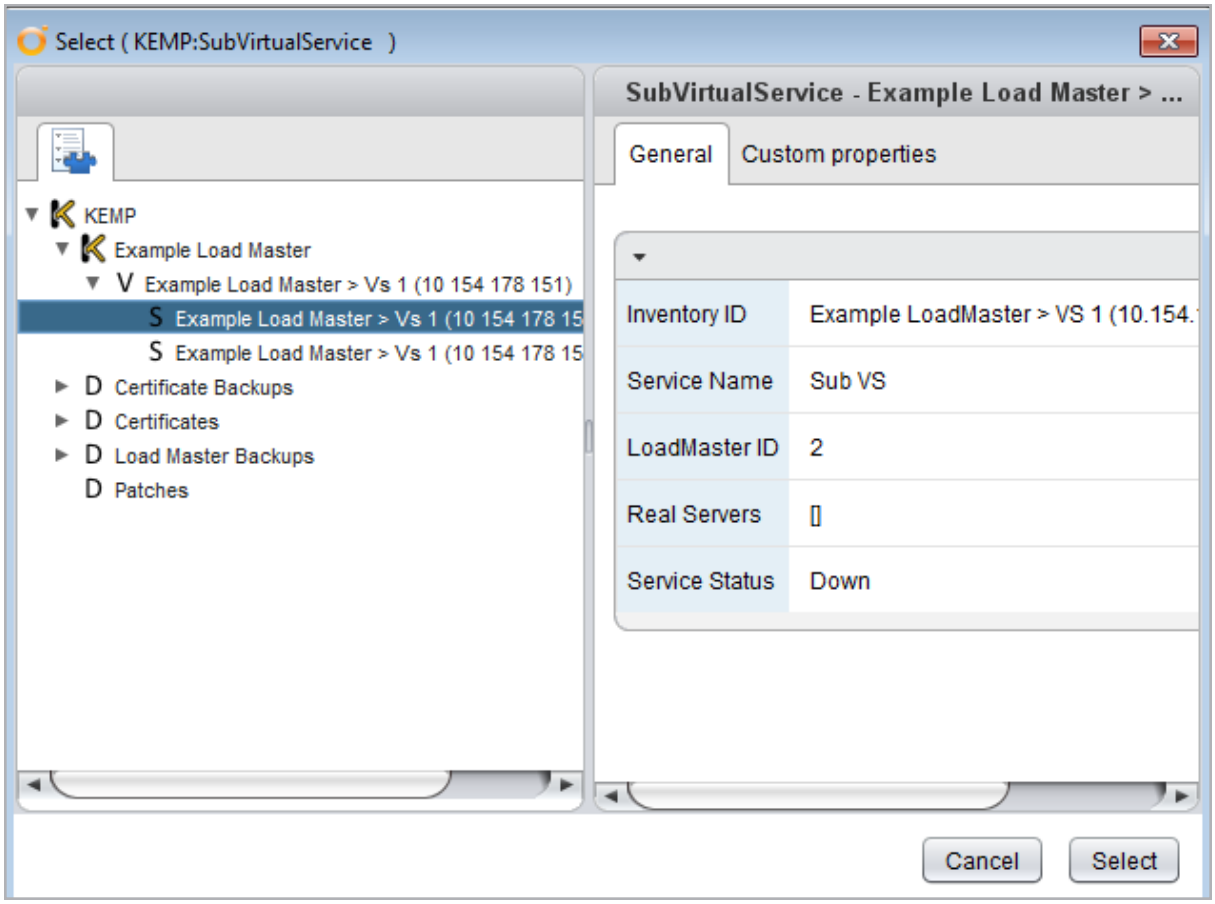
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

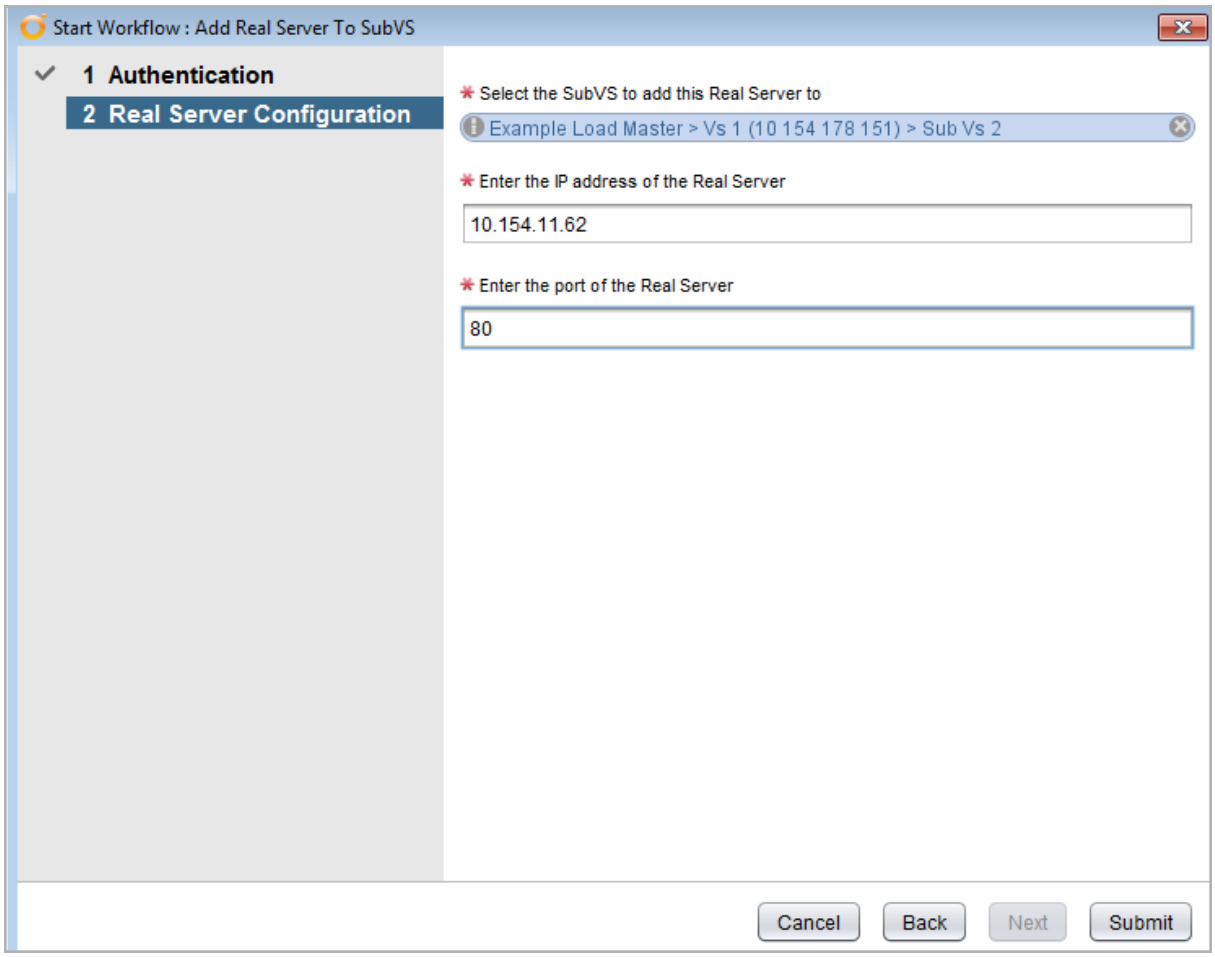
3. Click **Real Server Configuration**.



4. Click **Not set**.



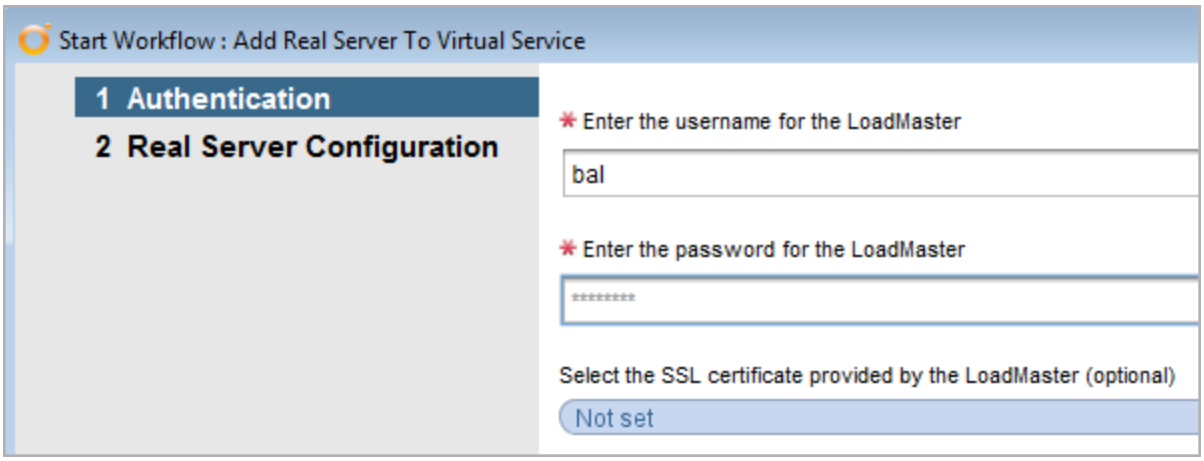
5. Expand the **Kemp** directory.
6. Expand the relevant LoadMaster.
7. Expand the relevant Virtual Service.
8. Select the relevant **SubVS**.
9. Click **Select**.



10. Enter the IP address of the Real Server to be added.
11. Enter the port of the Real Server.
12. Click **Submit**.

3.7.2 Add Real Server to Virtual Service

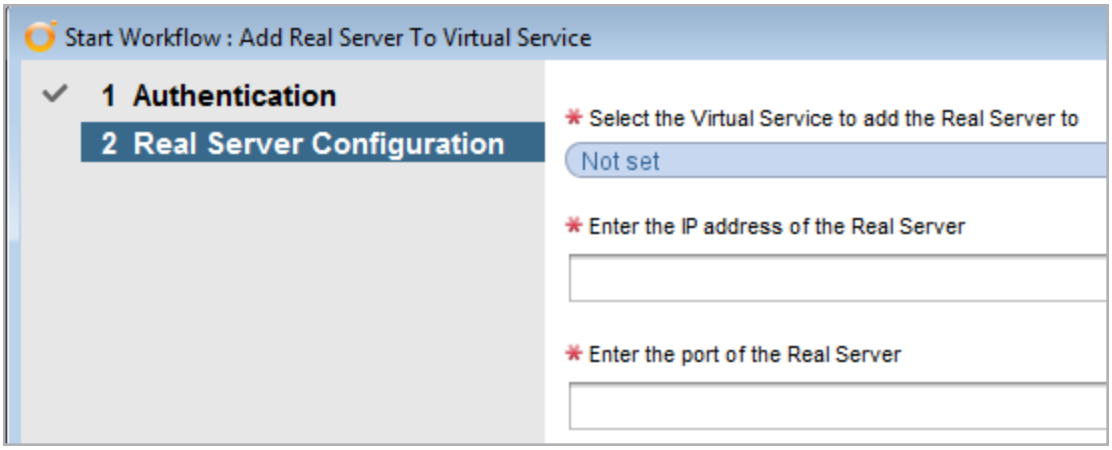
A Real Server can be added to a Virtual Service via Orchestrator by running the **Add Real Server to Virtual Service** workflow.



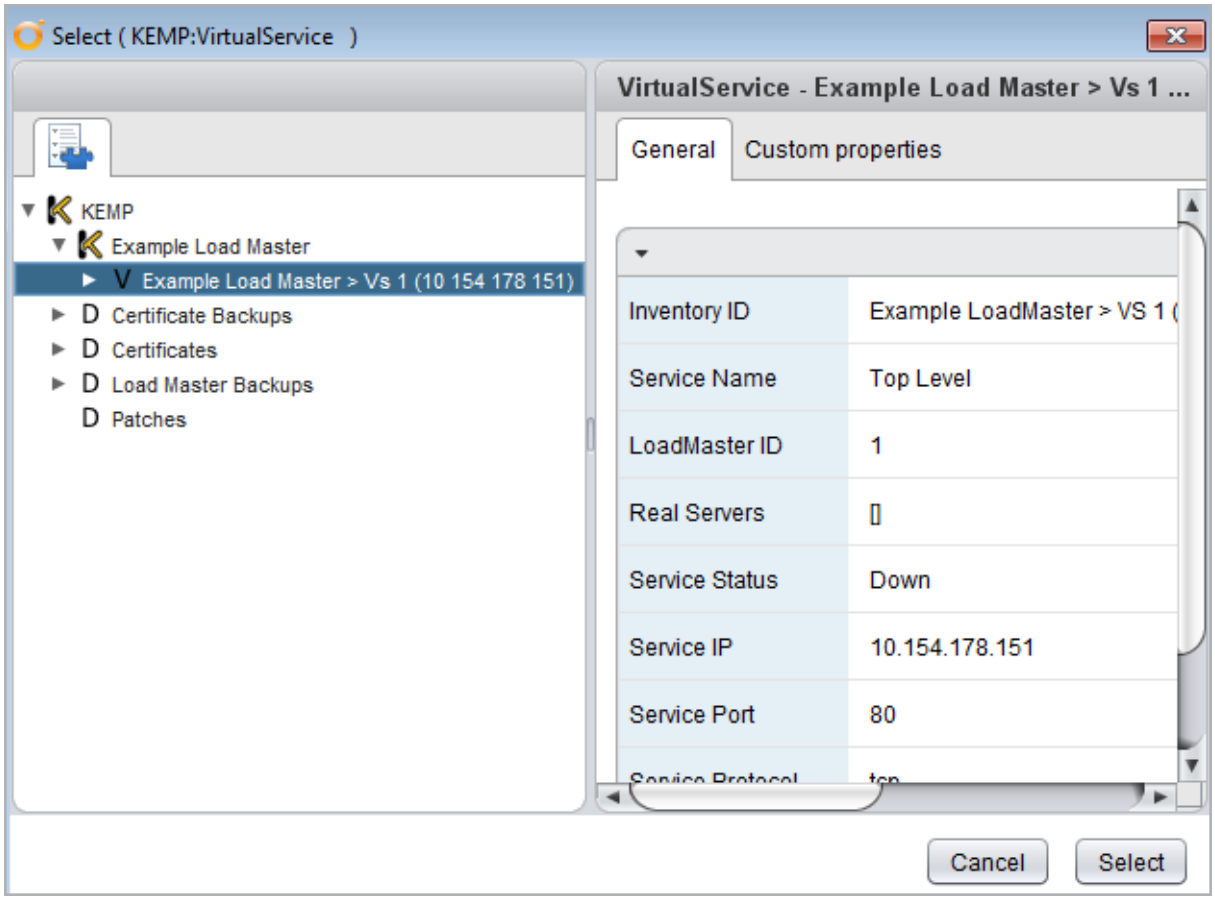
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

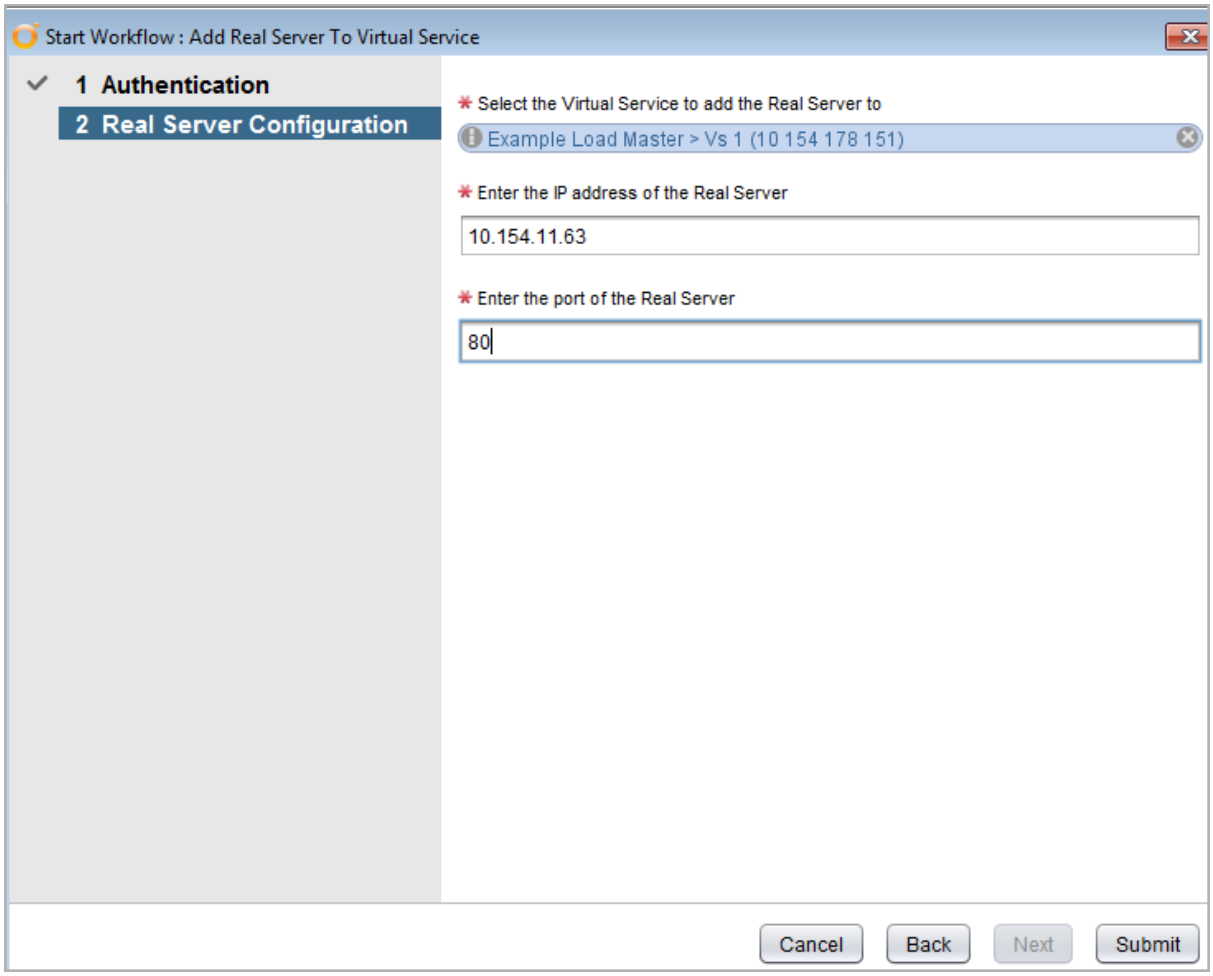
3. Click **Real Server Configuration**.



4. Click **Not set**.



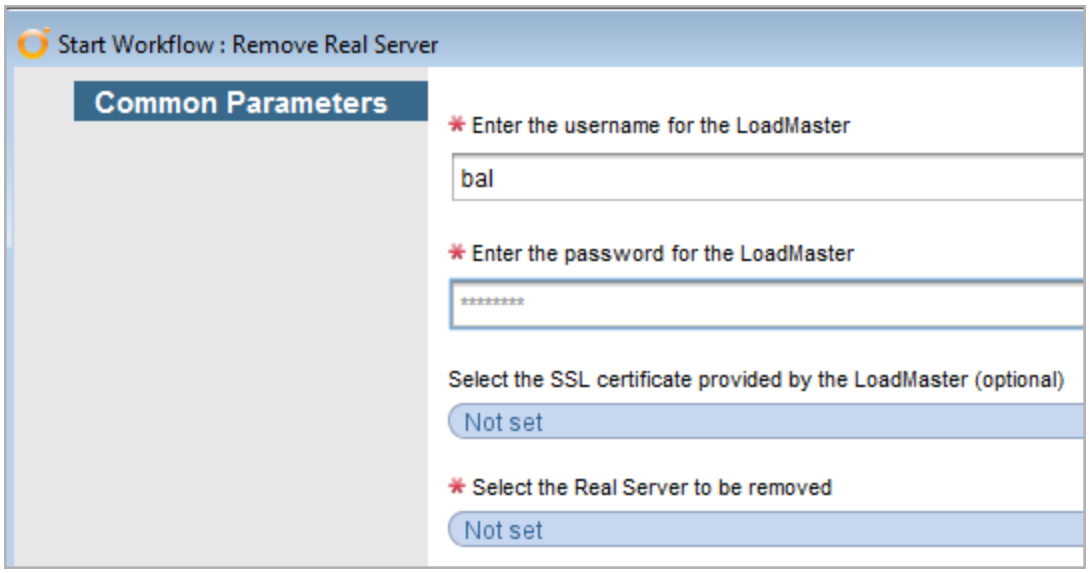
5. Expand the **Kemp** directory.
6. Expand the relevant LoadMaster.
7. Select the relevant Virtual Service.
8. Click **Select**.



9. Enter the IP address of the Real Server.
10. Enter the port of the Real Server.
11. Click **Submit**.

3.7.3 Remove Real Server

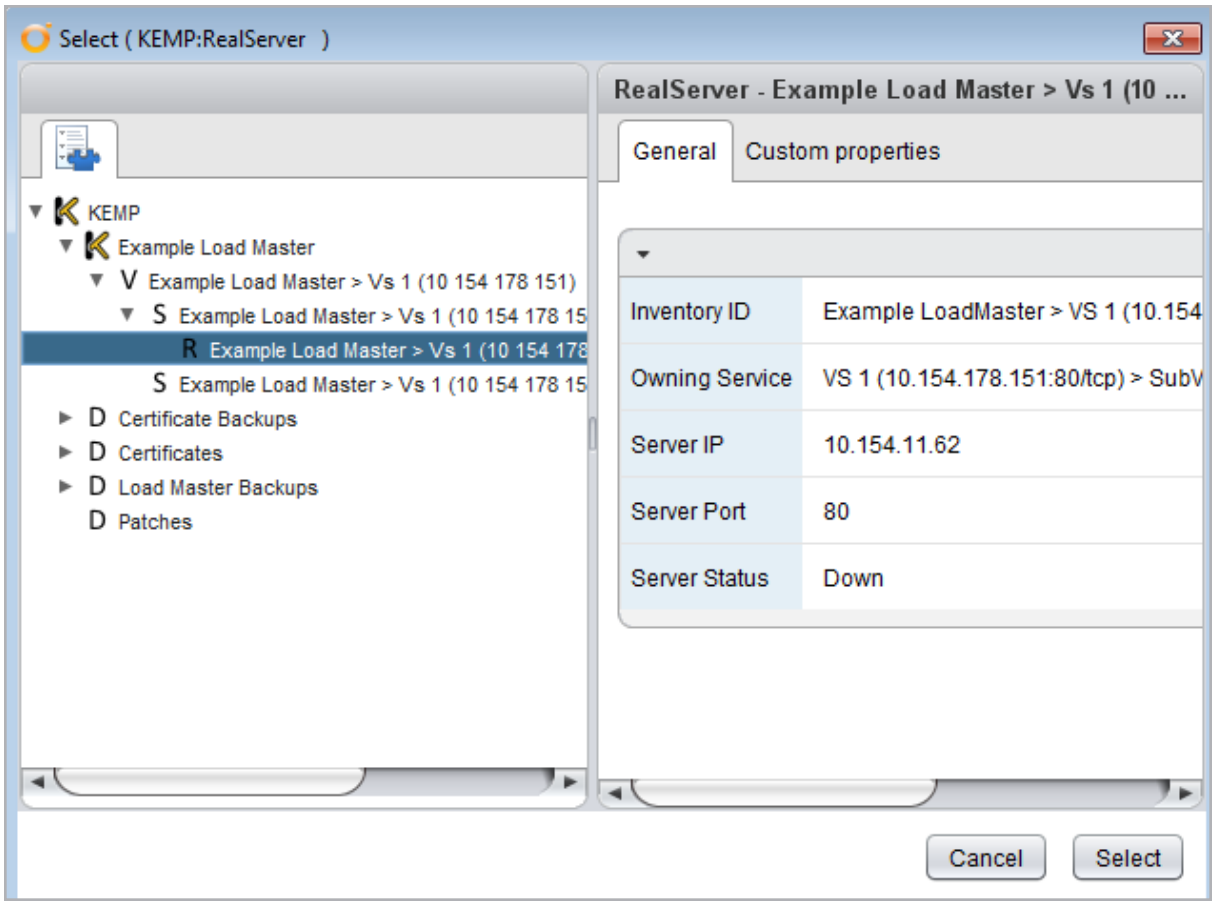
A Real Server can be removed by running the **Remove Real Server** workflow.



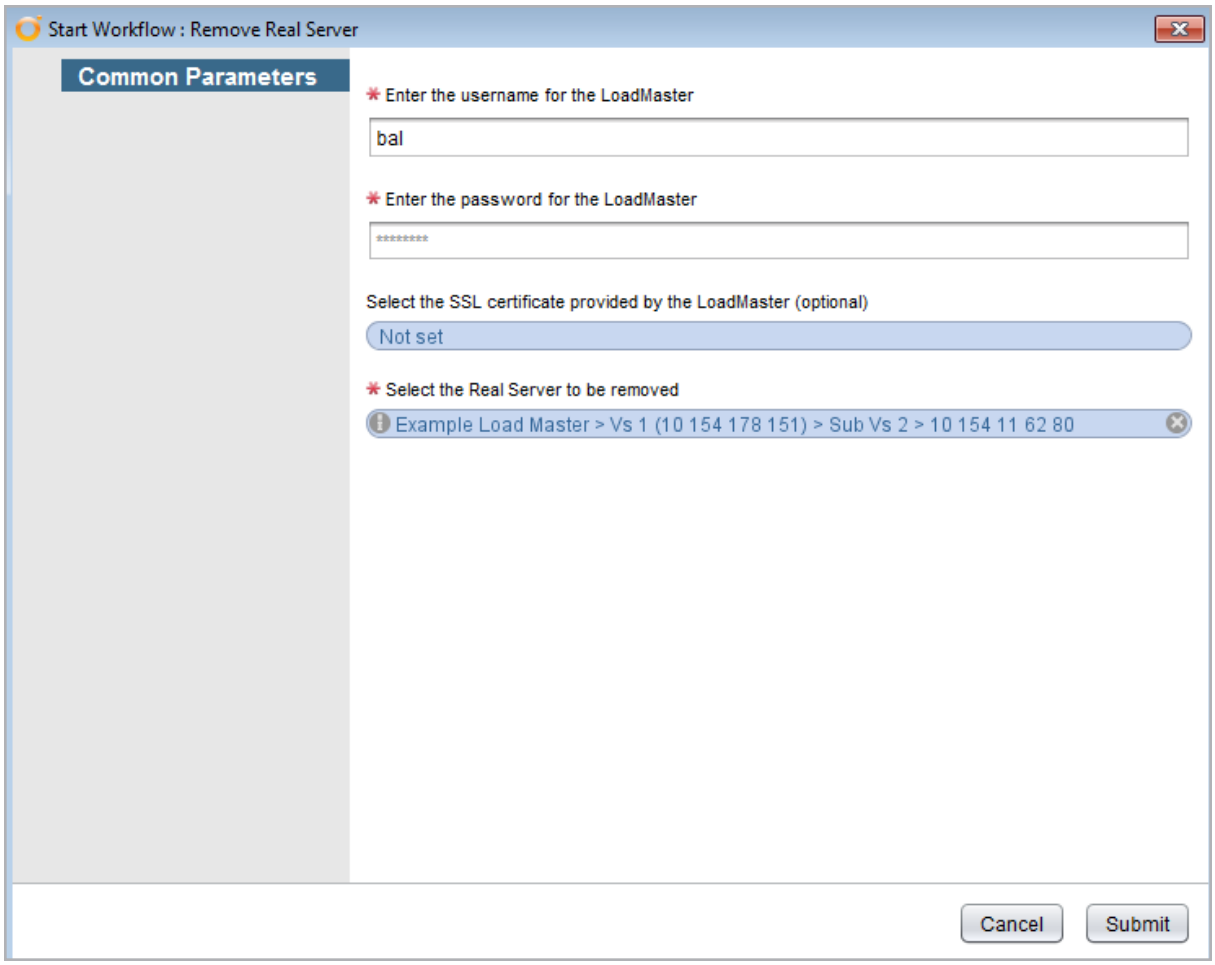
1. Enter the username and password to access the LoadMaster.

2. Specifying the SSL certificate is optional - this is the certificate file used to authenticate to the LoadMaster (the root LoadMaster certificate).

3. Click **Not set** in the **Select the Real Server to be removed** field.



4. Expand the **Kemp** directory.
5. Expand the relevant LoadMaster.
6. Expand the Virtual Service and/or SubVS.
7. Select the relevant Real Server.
8. Click **Select**.



9. Click **Submit**.

4 Uninstall the Kemp Orchestrator Plugin

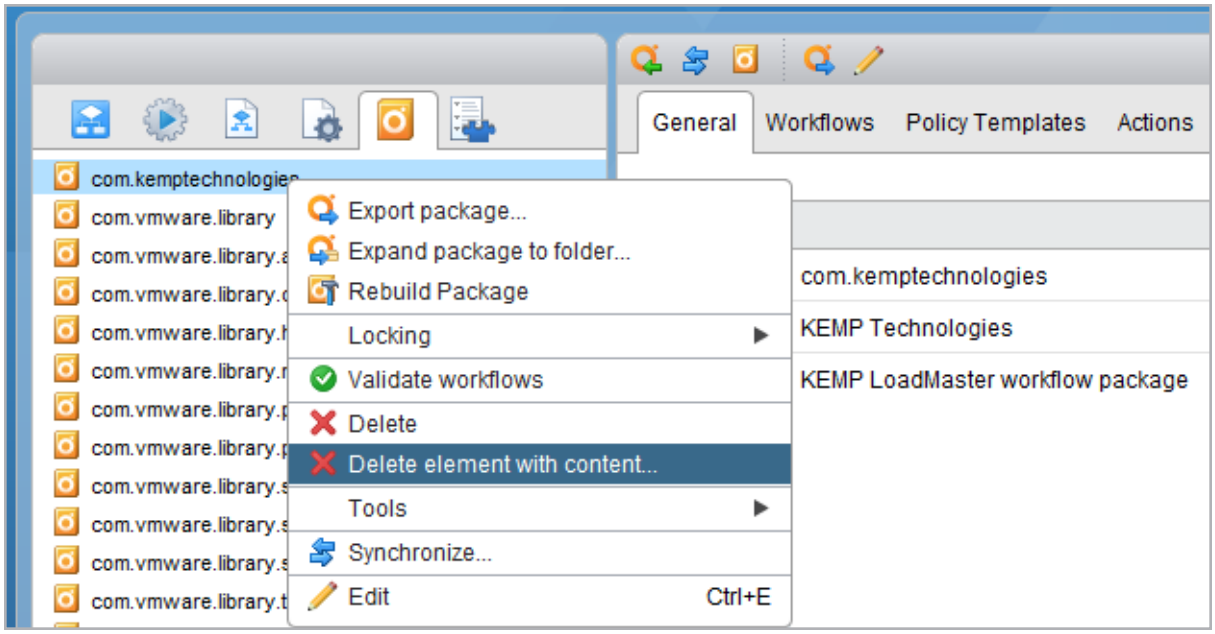
There are three steps that need to be completed in order to uninstall the Kemp Orchestrator plugin. Refer to the sections below for step-by-step instructions.

4.1 Uninstall the Workflows

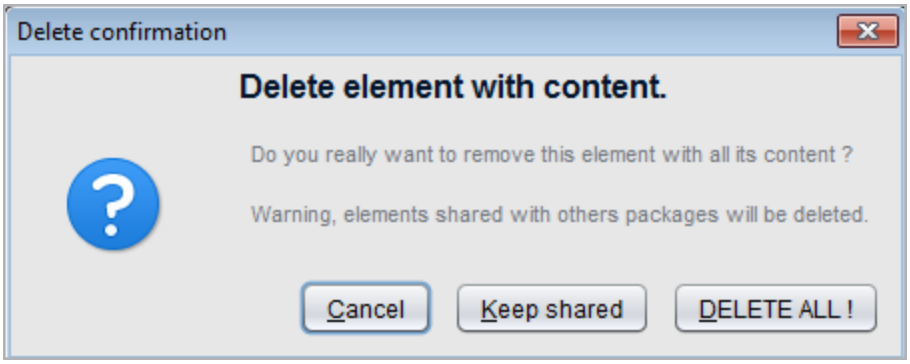
The first step is to uninstall the workflows. To do this, follow the steps below:

1. Select **Design** from the drop-down menu in the top-left of the screen.

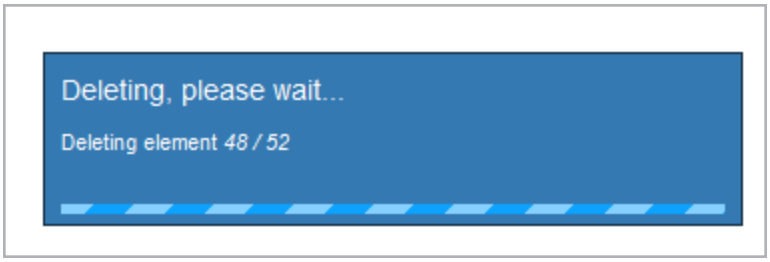
2. Select the packages tab (orange icon).



3. Right-click **com.kemptechnologies** and select **Delete element with content**.



4. Click **DELETE ALL**.



5. Wait for the deletion to complete.

Now that the workflows have been uninstalled, the Kemp plugin can be uninstalled. Follow the steps in the next section to do this.

4.2 Remove the Kemp Orchestrator Plugin

Then, after uninstalling the workflows - follow these steps:

1. Remotely connect to the Orchestrator server.
2. Navigate to the Orchestrator plugins folder:

   cd /var/lib/vco/app-server/plugins

3. Remove the Kemp Orchestrator plugin by running the following command:

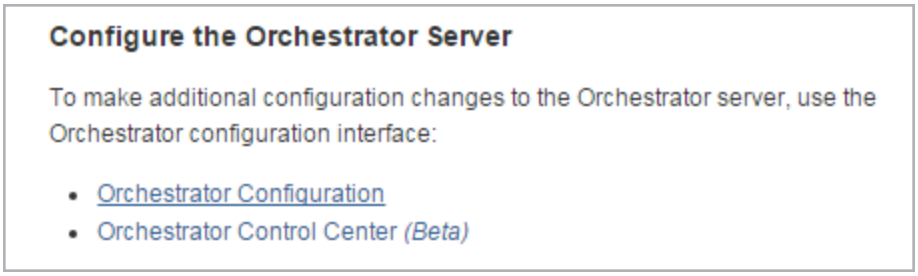
   rm <KempPluginFilename>.dar

Now that the Kemp Orchestrator plugin has been removed, the service needs to be restarted for the changes to be applied.

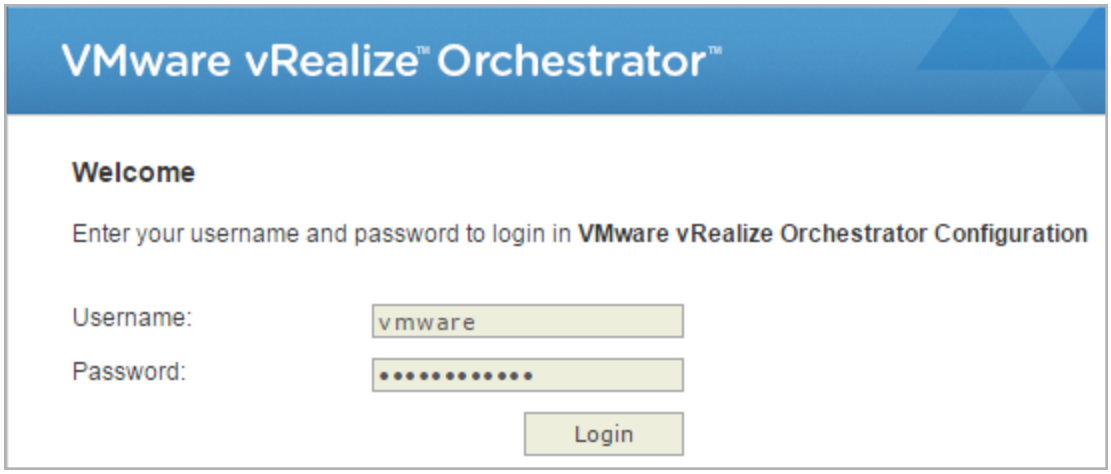
4.3 Restart the Service

After uninstalling, restart the service to complete the uninstallation. To do that, follow the steps below:

1. In a web browser, navigate to the IP address of the Orchestrator server followed by the :8281 port.



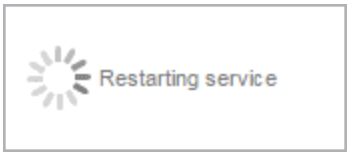
2. Click the **Orchestrator Configuration** link.



3. Enter the Orchestrator credentials and click **Login**.

4. Click **Startup Options** on the left.

5. Click **Restart service**.



6. Wait for the service to restart.

A message will appear when the service has been restarted.

5 Appendix A - Get and Set Parameters

A number of LoadMaster fields can be retrieved and set using the **Get Parameter** and **Set Parameter** workflows. The fields are retrieved and set using API parameters. The list of API parameters that can be used are listed below. For descriptions of what each of the parameters correspond to, please refer to the **Java API, Interface Description** or the **RESTful API, Interface Description**.

- dfltgw
- dfltgwv6
- admingw
- snat
- hatimeout
- hawait
- haprefered
- hamode
- haif
- havhid
- hastyle
- hainitial
- tcpfailover
- cookieupdate
- vmac
- sshaccess
- sshport
- sshv1prot

- wuiaccess
- mcast
- wuiiface
- wuiport
- sshiface
- hoverhelp
- routefilter
- transparent
- alwayspersist
- expect100
- localbind
- addcookieport
- subnetoriginating
- nonlocalrs
- multigw
- addforwardheader
- conntimeout
- authtimeout
- finalpersist
- tcptimestamp
- paranoia
- cachesize
- hostcache
- resetclose
- rfcconform
- keepalive

- backupday
- backupenable
- backuphost
- backuphour
- backupminute
- backuppassword
- backuppath
- backupuser
- backupuser
- emailuser
- emaildomain
- emailpassword
- emailserver
- emailsslmode
- emailport
- emailcritical
- emailemergency
- emailerror
- emailinfo
- emailnotice
- emailwarn
- addvia
- allowupload
- dropatdrainend
- droponfail
- closeonerror

- limitinput
- rsarelocal
- slowstart
- subnetorigin
- syslogcritical
- syslogemergency
- syslogerror
- sysloginfo
- syslognotice
- syslogwarn
- sslrenegotiate
- emailenable
- irqbalance
- snmpenable
- snmpV3enable
- snmpv3user
- snmpv3userpasswd
- snmpcontact
- snmpcommunity
- snmplocation
- snmpHaTrap
- snmpv1sink
- snmpv2sink
- snmpclient
- snmptrapenable
- motd

- wuidisplaylines
- linearesplogs
- onlydefaultroutes
- sessionauthmode
- sessionidletime
- sessionmaxfailattempts
- sessioncontrol
- sessionlocalauth
- ntphost
- netconsole
- netconsoleinterface
- namserver
- radiusbackupport
- radiusbackupsecret
- radiusbackupserver
- radiusport
- radiussecret
- radiusserver
- radiusrevalidateinterval
- ldapserver
- ldapbackupserver
- ldapsecurity
- ldaprevalidateinterval
- geoclients
- geopartners
- geosshport

- ha1hostname
- ha2hostname
- hostname
- searchlist
- timezone
- admincert
- localcert
- time
- ntphost
- version
- Tethering
- multihomedwui
- logsplitinterval
- allowemptyposts
- OCSPPort
- OCSPUseSSL
- OCSPOnServerFail
- OCSPServer
- OCSPUrl
- SSLStapling
- SSLRefreshInterval
- L7LimitInput
- sdnstatsmode

6 Appendix B - Memory and CPU Usage Details

The memory and CPU utilization details relating to the Kemp Orchestrator plugin are summarized in the tables below.

The below table shows the specifications of the Orchestrator server that was used when running the tests.

Specification	Type
Hypervisor	VMware vSphere
Memory	3GB
CPU	Dual-core @ 2.0GHz

The below table shows the approximate range of memory usage when the plugin is and is not installed.

Plugin Installed?	Memory Usage
Without plugin installed	381MB -> 395MB
With plugin installed	394MB -> 410MB
With plugin installed (load: ~600 objects)	454MB -> 463MB

The below table shows the CPU usage percentages in various states.

State	CPU Usage
Without plugin installed	~1%
With plugin installed	~1%
Expanding tree view (load: ~100 objects)	~8%
Expanding tree view (load: ~500 objects)	~19%
Empty workflow	~13%

Configure Server Availability workflow	~17%
Add LoadMaster workflow (load: 0 objects)	~17%
Add LoadMaster workflow (load: ~500 objects)	~40%
Remove LoadMaster workflow (load: 0 objects)	~17%
Remove LoadMaster workflow (load: ~500 objects)	~28%

References

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

Java API, Interface Description

RESTful API, Interface Description

Last Updated Date

This document was last updated on 22 March 2021.