



INSTALLATION GUIDE

Campaign Manager 6.0



VERSION CONTROL

| Version | Date | Author | Changes |
|---------|---------------|----------|-------------------------------------|
| 1.2 | 24 July 2017 | D Cooper | Prepare SQL Server section updated. |
| 1.1 | 22 May 2017 | D Cooper | Re-order of Chapter 2 Sub Sections |
| 1.0 | 25 April 2017 | D Cooper | Release |

RELATED DOCUMENTS

The related documents are located in the [Alterian product help](#).

| Name |
|--|
| Campaign Manager 6.0 Upgrade Guide |
| Campaign Manager 6.0 Architecture Guide |
| Campaign Manager 6.0 Backup Guide |
| Campaign Manager 6.0 Data Flow and Structure |
| Campaign Manager 6.0 Load Process Guide |
| Campaign Manager 6.0 Release Note |

TABLE OF CONTENTS

| | |
|---|-----------|
| 1. INTRODUCTION | 4 |
| 1.1. SUPPORTED ENGINE VERSION | 4 |
| 2. SUPPORTED PLATFORMS | 5 |
| 2.1. VIRTUAL MACHINES | 6 |
| 3. INSTALLATION PREREQUISITES | 8 |
| 3.1. COMMON DOMAIN USER ACCOUNT | 8 |
| 3.2. COMMON PREREQUISITES (ALL SERVERS) | 8 |
| 3.3. CONFIGURE WINDOWS 2012 APP SERVER WITH IIS WEB SERVER PREREQUISITES | 9 |
| 3.4. CONFIGURE WINDOWS 2008 APP SERVER WITH IIS WEB SERVER PREREQUISITES | 10 |
| 3.5. PREPARE APP SERVER | 11 |
| 3.6. PREPARE ENGINE SERVER | 11 |
| 3.7. PREPARE SQL SERVER | 11 |
| 4. CAMPAIGN MANAGER INSTALLER | 14 |
| 4.1. RUN CM.DEPLOYER.EXE | 14 |
| 4.2. LAUNCHING CAMPAIGN MANAGER | 24 |
| 5. POST INSTALLATION CONFIGURATION | 25 |
| 5.1. CONFIGURE APP SERVER | 25 |
| 5.2. CONFIGURE ENGINE SERVER | 25 |
| 5.3. CONFIGURE SQL SERVER | 26 |
| 5.4. CONFIGURE CLIENT MACHINES | 26 |
| 6. ADVANCED CONFIGURATION | 27 |
| 6.1. IDENTITY PROVIDERS | 27 |
| 7. INSTALLING KETTLE | 28 |
| 8. UNINSTALLING CAMPAIGN MANAGER | 29 |
| 9. TROUBLESHOOTING | 30 |
| 9.1. ERROR MESSAGES | 30 |
| 9.2. ENGINE TROUBLESHOOTING | 33 |
| 10. APPENDICES | 35 |
| 10.1. APPENDIX A – ADDING EM URLS | 35 |

1. INTRODUCTION

This document provides an overview of considerations that must be given to the existing environment prior to an installation of Campaign Manager 6.0 along with step-by-step guidance for the installation.

For an overview of common Campaign Manager Architecture configurations and guidelines for planning a system, refer to the **Campaign Manager 6.0 Architecture Guide**.

If you require further assistance, contact your Alterian account representative.

The following sections are included in this document:

- Installation
- Uninstall
- Troubleshooting

1.1. SUPPORTED ENGINE VERSION

Campaign Manager 6.0 is deployed with the latest version of Engine.

2. SUPPORTED PLATFORMS

This section details the Operating Systems and other requirements for:

- Application Server
- SQL Server
- Engine Server
- Client

APPLICATION SERVER

- Windows Server 2008 R2 SP2 (x64)
 - English language version
 - Standard Edition or above
 - Includes .net 4.5.2
- Windows Server 2012 R2 (x64) (recommended)
 - English Language version
 - Standard Edition or above
 - Includes .net 4.5.2
 - The deployer will do a version check to verify that the minimum requirement of Windows 2012 R2 April 2014 update (2919355) is installed
- IIS
 - IIS 7.5

SQL SERVER

- SQL Server 2008 R2 SP3
 - English language version
 - Standard Edition or above
- SQL Server 2012 SP3
 - English language version
 - Standard Edition or above
- SQL Server 2014 SP2
 - English language version
 - Standard Edition or above

Note: Only non-clustered environments will be tested

ENGINE SERVER

- Office (if required for Excel export)
 - Microsoft Office 2010 (x86)
 - Microsoft Office 2013 (x86)

CLIENT

- Windows
 - Windows 7
 - Windows 8.1
 - Windows 10
 - Silverlight 5.1
 - Browsers
 - Microsoft Internet Explorer 11
 - Current version of Google Chrome (HTML elements only)
 - Microsoft Edge (HTML elements only) - Supported but not tested.
- macOS
 - Sierra (Version 10.12)
 - Browsers
 - Current version of Google Chrome (HTML elements only)
 - Not Safari
- Microsoft Office 2010 (x86)
 - Microsoft Office 2013 (x86)
 - Client Support for Office 365 (x86)

TABLET SUPPORT

There is no support for tablets in this release

2.1. VIRTUAL MACHINES

Alterian makes significant use of VMWare and Hyper-V virtualization technologies for internal product testing and hosting of production instances in our data centers. Alterian supports virtualized installations of Campaign Manager for on-premise production environments with the following caveats:

If a user reports an issue to Alterian Support that is performance or network related, the user may be required to reproduce the issue in a non-virtualized environment.



If a user requests help from Alterian Support for virtualization software installation, configuration, or optimization, the user will be advised to find another source of qualified technical staff for these activities.

3. INSTALLATION PREREQUISITES

All machines must have the Universal C runtime installed. You can get the appropriate download for your operating system from: <https://support.microsoft.com/en-gb/help/3118401/update-for-universal-c-runtime-in-windows>.

3.1. COMMON DOMAIN USER ACCOUNT

Regardless of the installation approach, on a single machine, or spread across multiple machines, a common user account must be created. We strongly recommend a domain service account that is accessible from each of the server roles. This account is established as the owner for all related Windows services, the IIS app pool, and SQL Server database connections. This account must be a local admin for each machine that Campaign Manager is used on. It is NOT necessary for it to be a domain admin. Grant this account the "Log on as a service" right on each machine.

The actual account can have any name, but is referred to as the Common Domain User Account in this document.

3.2. COMMON PREREQUISITES (ALL SERVERS)

NOTE: The following prerequisites apply to all servers.

1. All servers must be running English-language versions of Windows Server 2008 R2 SP1 64 bit Standard or Enterprise Edition, or Windows 2012 R2 Standard Edition. For Windows 2012, servers must be updated with the April 2014 roll up (2919355).
 - Windows 2008 R2 Web Server edition can be used for a dedicated Web Server
 - NTFS is required
2. Disable Windows firewall service.

NOTE: On a single box install you can leave the windows firewall on, however you must allow http(s) traffic through.

Windows firewall can be enabled after the installation is complete. See the Campaign Manager 6.0 R1 Architecture Guide for a list of ports that need to be opened.

3. Change the User Account Control (UAC) settings to Never Notify. (Server restart is usually required.)
4. Ensure Data Execution Prevention (DEP) is turned on for essential Windows programs and services only. (Sever restart is usually required). Navigate to:

- Computer > System properties > Advanced system settings > Advanced tab > Performance > Settings > Data Execution Prevention tab.
5. The Deployer makes extensive use of Windows Management Instrumentation (WMI) to communicate between servers during the installation. If there are non-Windows firewalls between servers then, for a period while the Deployer runs, all ports must be open.
 6. All machines must be able to ping each other by name. ICMP needs to have access to all the machines through any firewall.
 7. All machines must have the Universal C runtime installed. Get the appropriate download for your operating system from: <https://support.microsoft.com/en-gb/help/3118401/update-for-universal-c-runtime-in-windows>.

3.3. CONFIGURE WINDOWS 2012 APP SERVER WITH IIS WEB SERVER PREREQUISITES

Log in to the App Server using the Common Domain User Account. It must be a local machine administrator.

1. Open **Server Manager (Start > Administrative Tools > Server Manager)**.
2. Click the **Manage** menu option and select **Add Roles and Features**.

In the wizard that opens:

1. Select **Next** on the **Before you Begin** tab.
2. On the Installation Type tab, select the **Role-based or feature-based installation** option.
3. On the **Server Selection** tab, select the current server.
4. On the **Server Roles** tab, select the **Web Server (IIS)** option.
5. If prompted to add Management tool features for the Web Server (IIS) role, make sure the **Include management tools (if applicable)** option is selected and click **Add Features**.
6. Click **Next**.
7. On the **Features** tab, in the tree expand **.NET Framework 4.5 Features** and then **WCF Services**. Select the **HTTP Activation** option.
8. If prompted to add features required for HTTP Activation, make sure the **Include management tools (if applicable)** option is selected.
9. Click **Next**.
10. At the **Web Server Role (IIS)** tab, click **Next**.
11. At the **Role Services** tab for **Web Server (IIS)**, select the following under each heading:

- Application Development - select all options.
 - Common HTTP Features – select Static Content, Default Document, Directory Browsing, and HTTP Errors.
 - Health and Diagnostics - select HTTP Logging and Request Monitor.
 - Management Tools – select 'IIS Management Console' and 'IIS 6 Management Compatibility', and all child settings. If prompted with an option to 'Include management tools' ensure the option is checked and click [Add Features]. (IIS 6 is necessary for the Deployer tool).
 - Performance - select all options.
 - Security – select 'Basic', 'Windows Authentication' and leave 'Request Filtering' checked.
12. Click **Next**.
 13. At the **Confirmation** tab, click **Install**.
 14. Select **Close** when the installation has completed.

3.4. CONFIGURE WINDOWS 2008 APP SERVER WITH IIS WEB SERVER PREREQUISITES

Login to the App Server using the Common Domain User Account. It must be a local machine administrator.

1. Open Server Manager (Start > Administrative Tools > Server Manager). Right-click Roles and select Add Roles. In the wizard, select Web Server (IIS) and make the following selections under each heading:
 - Common HTTP Features – Select Static Content, Default Document, Directory Browsing, and HTTP Errors.
 - Application Development - select all options
 - Health and Diagnostics - select HTTP Logging and Request Monitor
 - Security – select 'Basic', 'Windows Authentication' and leave 'Request Filtering' checked.
 - Performance - select all options
 - Management – select 'IIS Management Console' and 'IIS 6 Management Compatibility', and all child settings. (IIS 6 is necessary for the Deployer tool).
2. Complete the wizard and select Install.
3. When the installation has completed, select Close.
4. If not already present, download and install .NET Framework 4.5.2 or later from Microsoft.

3.5. PREPARE APP SERVER

1. Ensure that the system is up-to-date by performing a Windows update.
2. Configure DCOM as follows. Select Start > Administrative Tools > Component Services – expand the Component Services node > expand the Computers node > right-click My Computer and select Properties.
3. On the COM Security tab, verify that the following accounts have all options allowed for Access Permissions and Launch and Activation Permissions for both Limits and Default: INTERACTIVE, NETWORK, SYSTEM, and the Common Domain User Account.
4. On the Default Protocols tab, select Properties and configure a port range for DCOM usage, typically this is 5500-5700.
5. To test the install on the App server, after running the Deployer, you must install Silverlight 5 (Silverlight 4 is not supported).

3.6. PREPARE ENGINE SERVER

1. Log in to the Engine Server using the Common Domain User Account. It must be a local machine administrator.
2. Ensure the Domain User Account acts as part of the operating system, from the same place as you grant log in as a service rights.
3. Run a Windows update and accept all updates.
4. Configure DCOM as follows. Select Start > Administrative Tools > Component Services – expand the Component Services node > expand the Computers node > right-click My Computer and select Properties.
5. On the Default Protocols tab, select Properties and configure a port range for DCOM usage, typically this is 5500-5700.
6. On the COM Security tab, verify that the following accounts have all options allowed for Access Permissions and Launch and Activation Permissions for both Limits and Default: INTERACTIVE, NETWORK, SYSTEM, and the Common Domain User Account.

3.7. PREPARE SQL SERVER

1. Log in to the SQL Server using the Common Domain User Account. It must be a local machine administrator.
2. Install .NET Framework 3.5 or later.
 - a. On Windows Server 2012 R2: Open Server Manager (Start Icon > Server Manager). Select Add Roles and features. In the wizard, click Next through to Features and select .NET Framework 3.5 Features. Continue through the wizard and select Install on the final step.

- b. On Windows Server 2008 R2: Open Server Manager (Start > Admin Tools > Server Manager). Right-click Features and select Add Features. In the wizard that launches, select .Net framework 3.5 features. When prompted, click [Add Required Role Services]. Continue through the wizard selecting the defaults and select Install on the final step.
 3. Install .NET Framework 4.5.2 or later.
 - a. On Windows Server 2012 R2: Open Server Manager (Start Icon > Server Manager). Select Add Roles and features. In the wizard, click Next through to Features and select .NET Framework 4.5 Features. Continue through the wizard and select Install on the final step.
 - b. On Windows Server 2008 R2: Open Server Manager (Start > Admin Tools > Server Manager). Right-click Features and select Add Features. In the wizard that launches, select .Net framework 4.5 features. When prompted, click [Add Required Role Services]. Continue through the wizard selecting the defaults and select Install on the final step.
4. Run a Windows update and accept all updates.
5. Install SQL Server 2008 R2 SP3, SQL Server 2012 SP2 Enterprise or Standard Edition, or SQL Server 2014 SP1. Note that SQL Clustering is not supported.
6. On the Feature Selection screen select:
 - Database Engine Services
 - Management Tools (Basic and Complete)
7. On the Instance Configuration screen, select the appropriate instance name, for example 'Default Instance'.
8. On the Server Configuration screen on the Service Accounts tab, enter the Common Domain User Account's credentials.
9. On the Database Engine Configuration screen on the Account Provisioning tab, under Authentication Mode, select Mixed Mode Authentication.
10. On the Database Engine Configuration screen on the Account Provisioning tab, specify the SQL Server administrator.
11. On the FILESTREAM tab, select Enable FILESTREAM for Transact-SQL access and select all child options.
12. Finish the install.
13. Run a Windows update and apply the latest SQL Service Pack.
14. Open SQL Server Configuration Manager. Expand the SQL Server Network Configuration node. Double-click Protocols and enable Named Pipes and TCP/IP.
15. Under SQL Server Services, ensure the SQL Server Agent is started and set to Automatic Start mode.

16. Stop and restart the SQL Server Service.
17. Connect to SQL via SQL Server Management Studio (SSMS) and verify you can connect. Select Windows Authentication.
18. In SQL Management Studio, connect to the Server and expand Security->Logins. Ensure the Common Domain User Account has a valid SQL Login with Default Language=English and Server Roles=public, sysadmin
19. The Windows account for the user running the Deployer should have an SQL Login with Server Roles=public,sysadmin. The deployer requires this access to create databases on a new install, and also to create and remove MSDB jobs on upgrade and uninstall.

4. CAMPAIGN MANAGER INSTALLER

STOP: Before running the Campaign Manager Installer, be sure that for each of the server roles, you have addressed all installation prerequisites listed in Section 3.

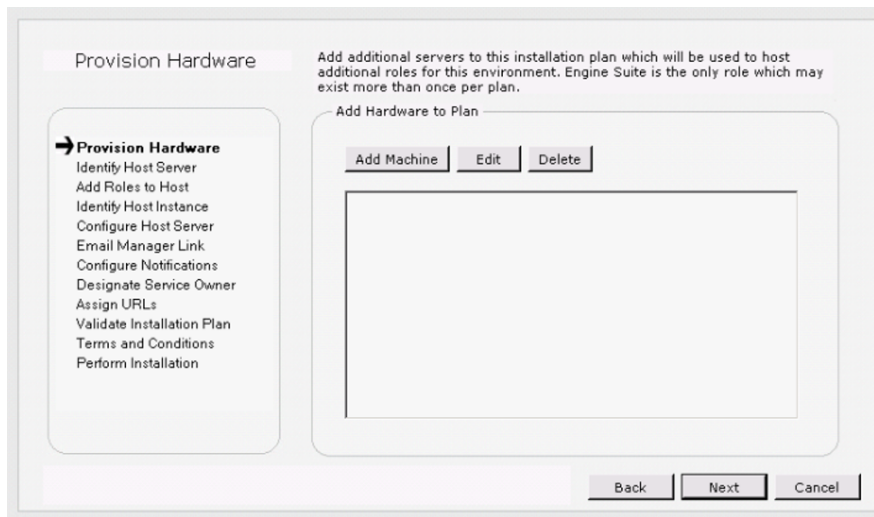
These instructions relate to a new, clean installation of Campaign Manager.

4.1. RUN CM.DEPLOYER.EXE

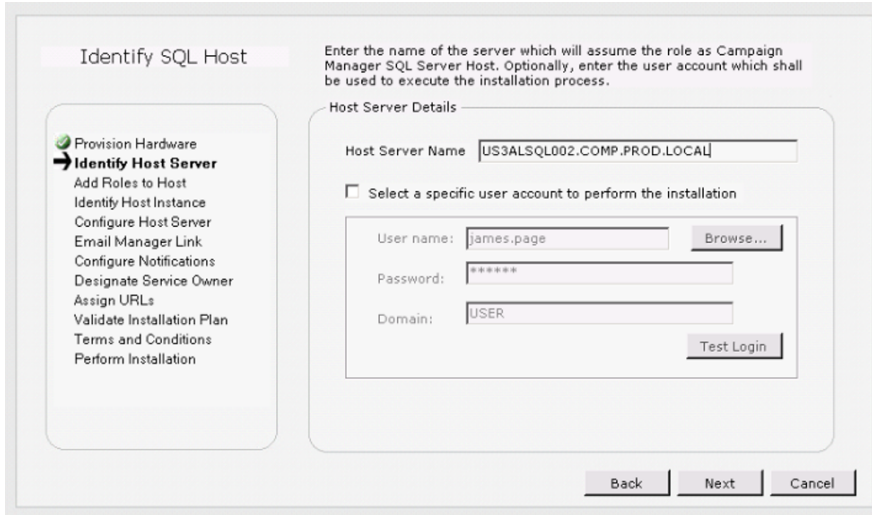
1. Log on to the App Server as the Domain Service Account, save the Deployer package to the App Server and unzip. Run the CM.Deployer.exe file.

NOTE: If installing on Windows Server 2012 R2, right-click CM.Deployer.exe and select Run as Administrator .

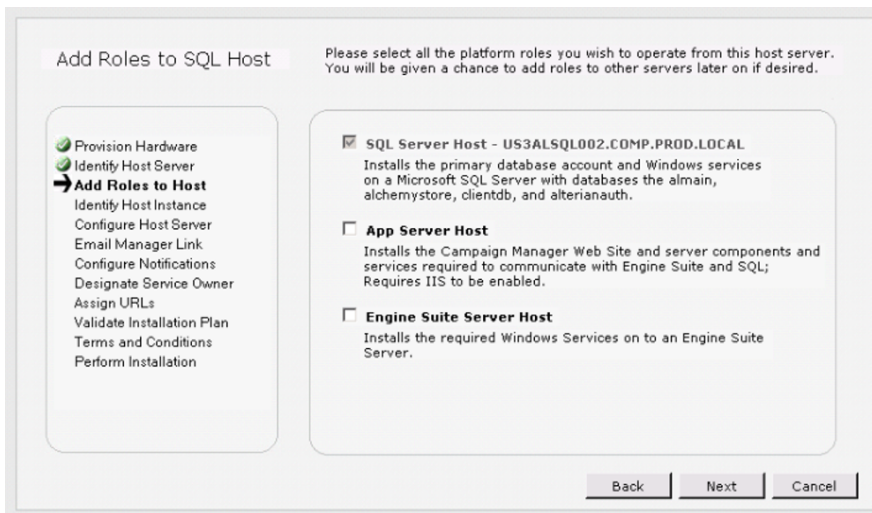
2. On the Welcome Screen, click Next.
3. On the Platform Installer, select New Environment.
4. The number of machines added depends on your planned architecture. For each machine added, there are a number of standard steps that are required. This example details a three-box architecture, so machine configuration steps are repeated for the SQL, App and Engine machines.
5. Click Add Machine to configure the first machine.



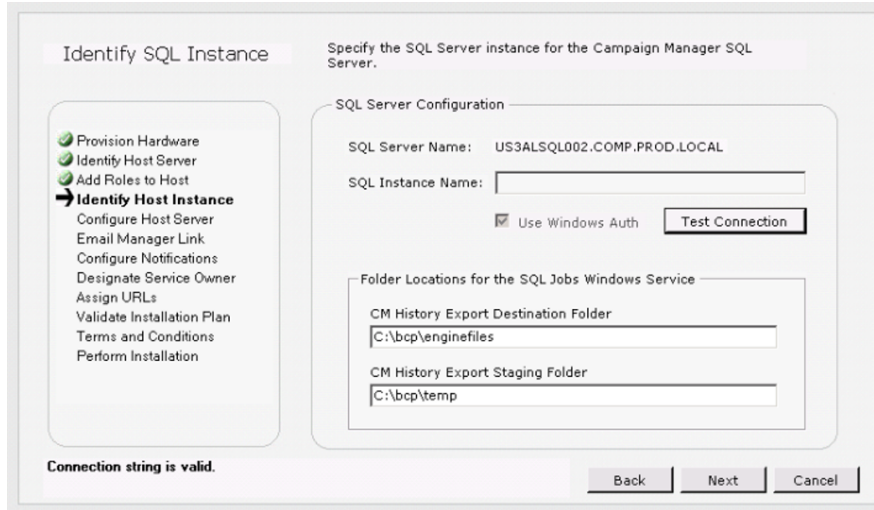
6. Enter the SQL Server name that will host the databases.



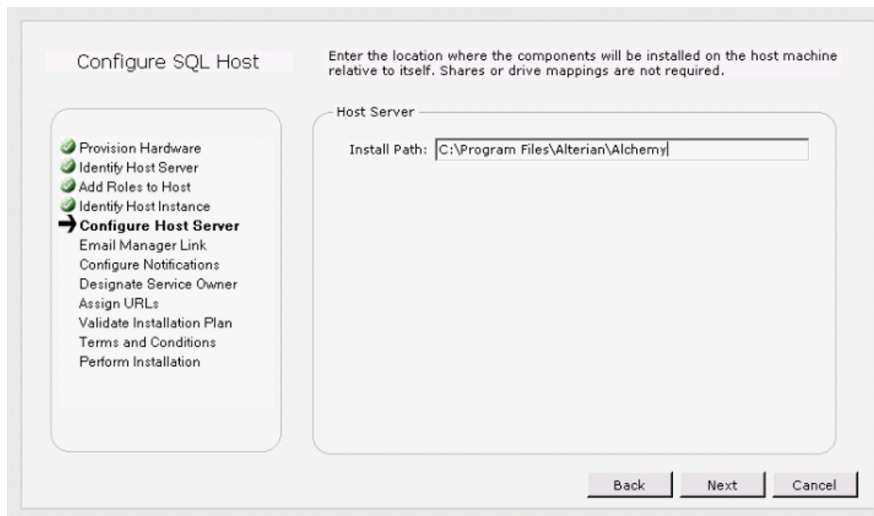
7. Click Next.
8. Add Roles to SQL Host. This server by default is the SQL Server host. You can assign additional roles to this machine here or, as in this example, they can be assigned to different machines later in the process.



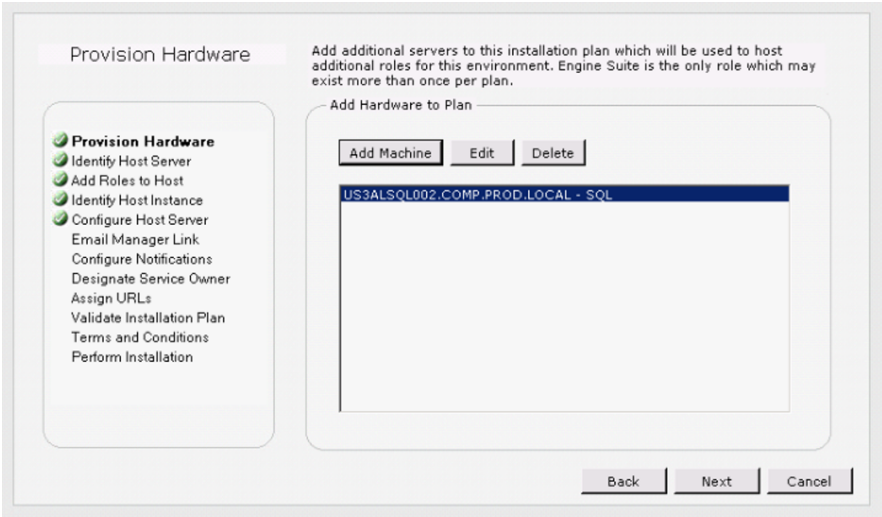
9. Click Next.
10. Use the 'Identify SQL Instance' screen to assign the SQL Server instance where it is not the Default. It is recommended that you use the Test Connection button to confirm that you are able to connect to the configured SQL Server Instance.
 - The Export Destination Folder is where iLoader retrieves history files for import into Engine.
 - The Export Staging Folder is where CM tactic output files are stored prior to FTP.



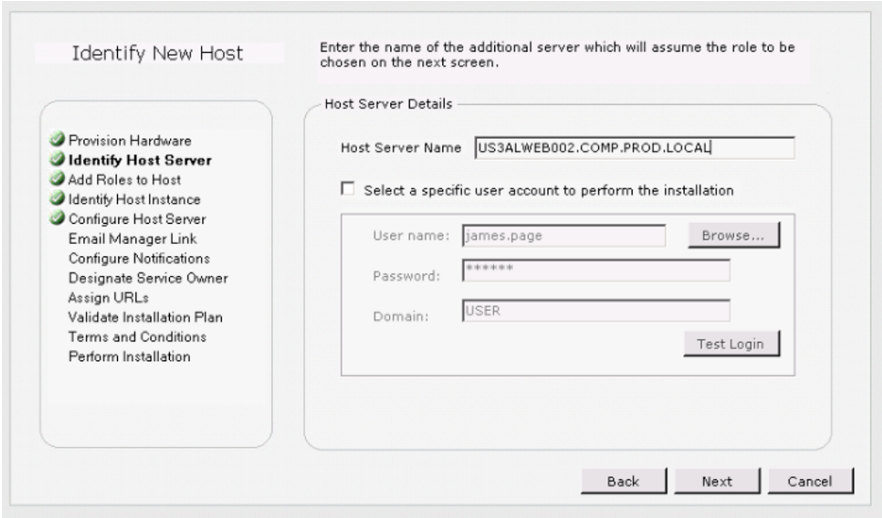
11. Click Next.
12. The 'Configure SQL Host' screen applies to the SQL Server machine only and is used to specify the location of the installation files. If there is any other Alterian software installed on the machine, ensure that the selected folder does not conflict with an existing 'Alterian' folder.



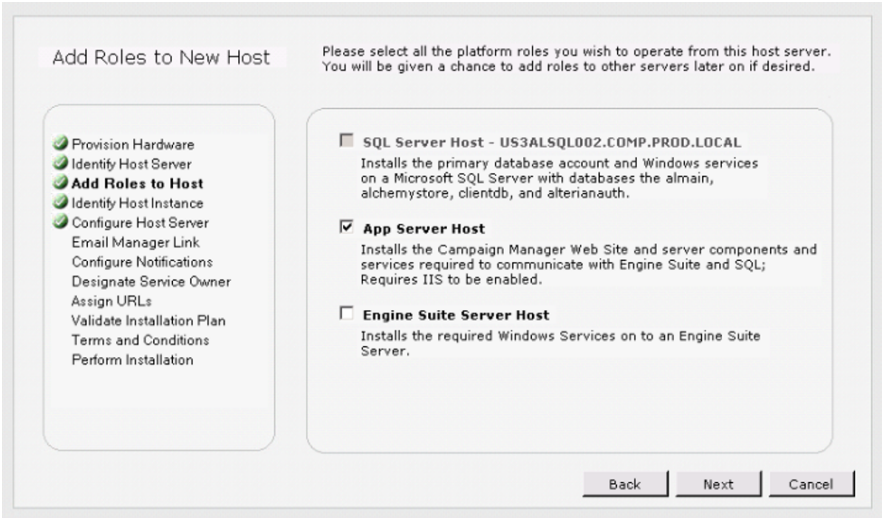
13. You have now added the SQL Host Server and have looped back to the Add Machine step. In the 'Provision Hardware' screen, click Add Machine to add additional machines for the Application Server and Engine.



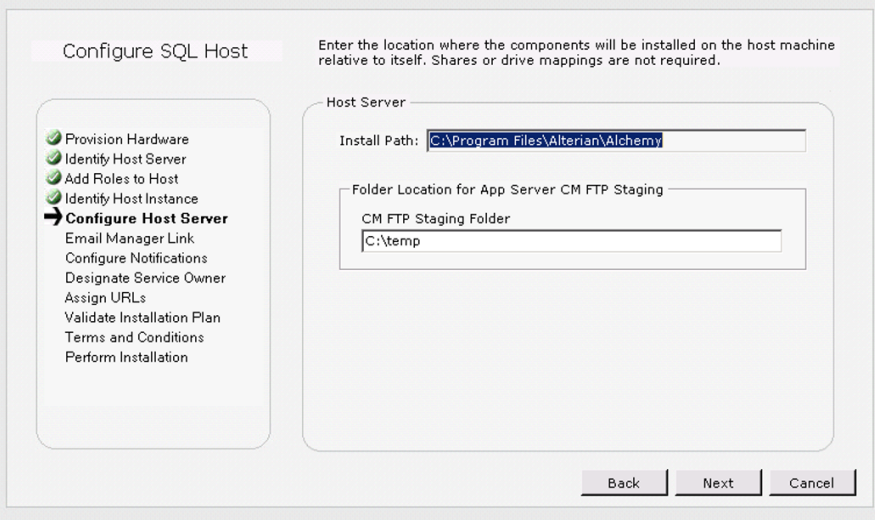
14. In the Host Server Name field, add the details of the App Server.



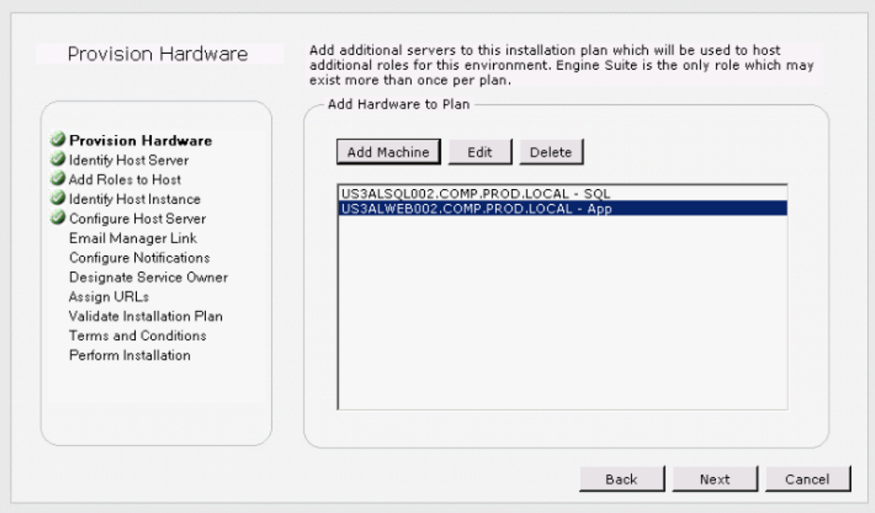
15. Select the App Server Host check box to specify this is the App Server.



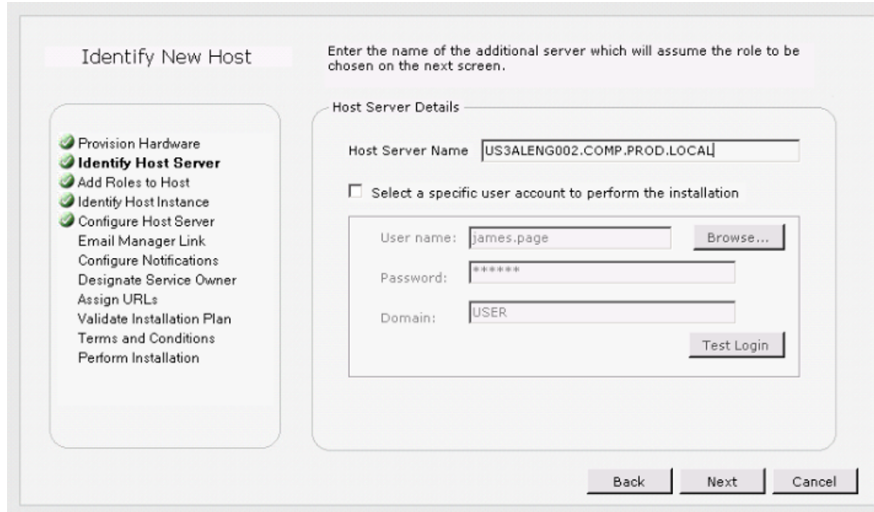
- Specify the install folder for the App Server and the CM FTP Staging folder, used by Campaign Manager for export of full files prior to posting on the FTP location defined within the Admin screens.



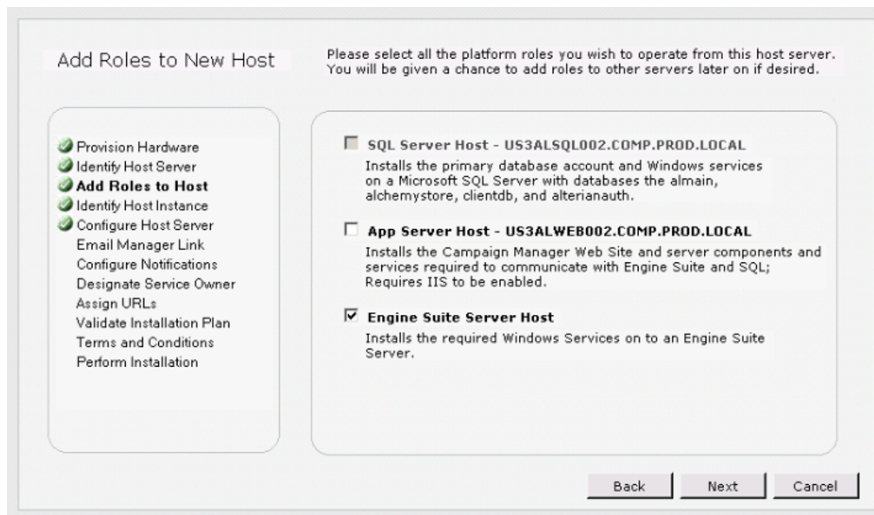
- You have now added the App Server and have looped back to the Add Machine step. We can now add the Engine server details.
- Click Add Machine to add the Engine Server Details.



- In the Host Server Name field, add the details of the Engine Server.

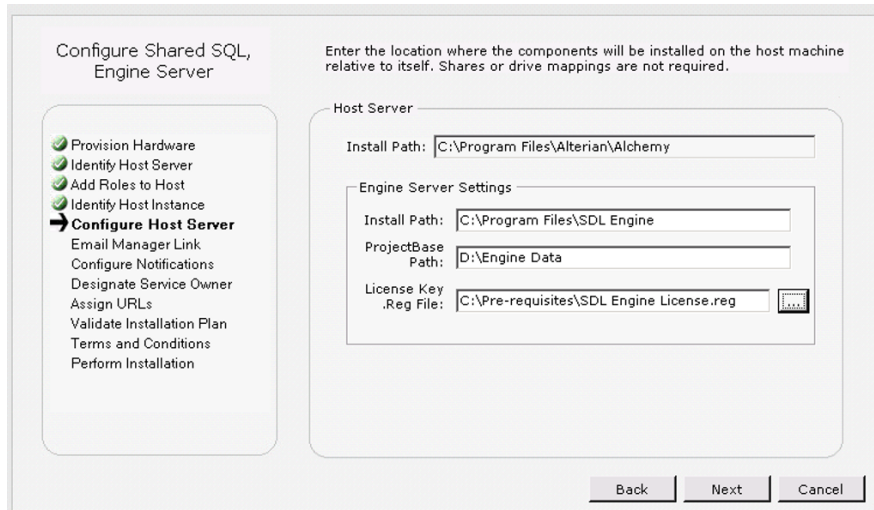


20. Select the Engine Suite Server Host check box to specify this is the Engine server.

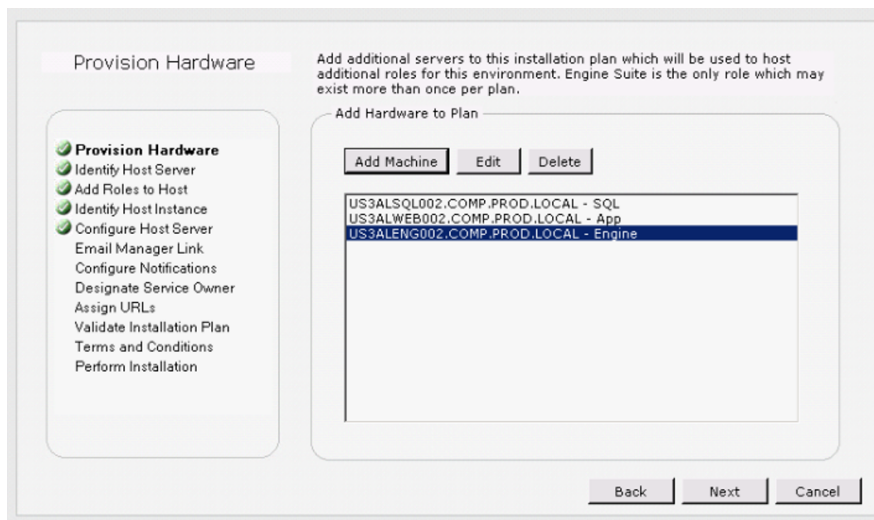


21. Specify the Install Path for the CM components on the Engine server. The CM Deployer will also install Engine to the specified server as part of the clean install. Configure Engine Server settings with:

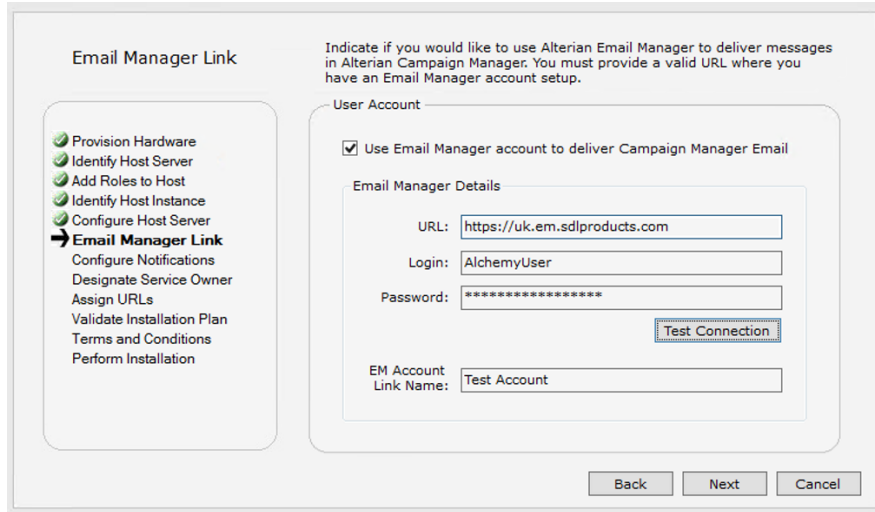
- Install Path: The local path for Engine Program files.
- ProjectBase Path: The local path where a default ProjectBase folder will be created.
- Note: Validation exists to prevent naming the folder 'ProjectBase', as the ProjectBase folder is created under this path on install. This folder must not exist, if it does an error will be thrown.
- License Key Reg File: should be located on the CM deployer server, and is applied to the Engine server during installation. Contact Alterian Support if you require a license key.



22. Check that all required machines have been set up. For a three-server architecture, the screen will appear as below. Add additional Engine Servers if required.



23. If you are using Email Manager to deliver email messages in Campaign Manager, populate the 'Email Manager Link' screen with the applicable Email Manager account details. You should use an Admin user login and password in the Login and Password fields, not an SA account. The account used associates the installation with the Email Manager client associated with the login\password provided. When using Creative Builder in the Frame, it is recommended that the Campaign Manager hosting site uses the same protocol as the Email Manager API (http compared to https).



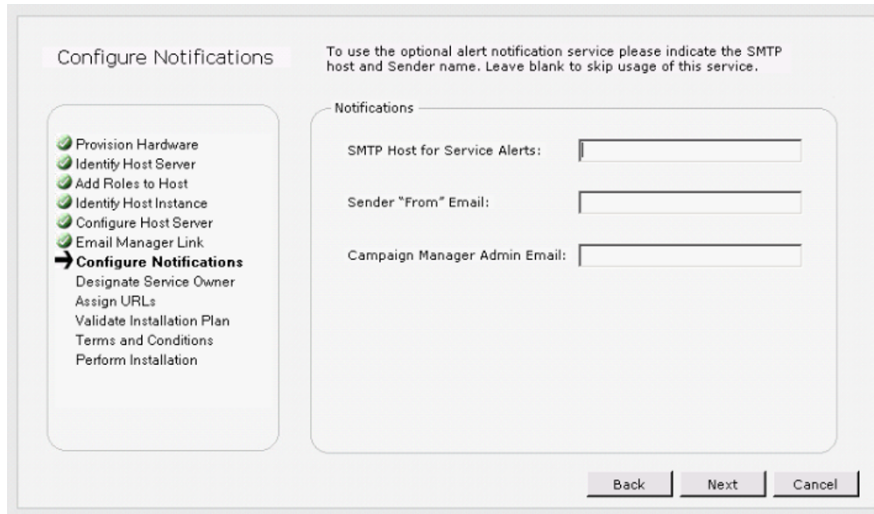
The following Email Manager URLs are available. These are regional, based on the data center where your account is hosted:

Location EM URL

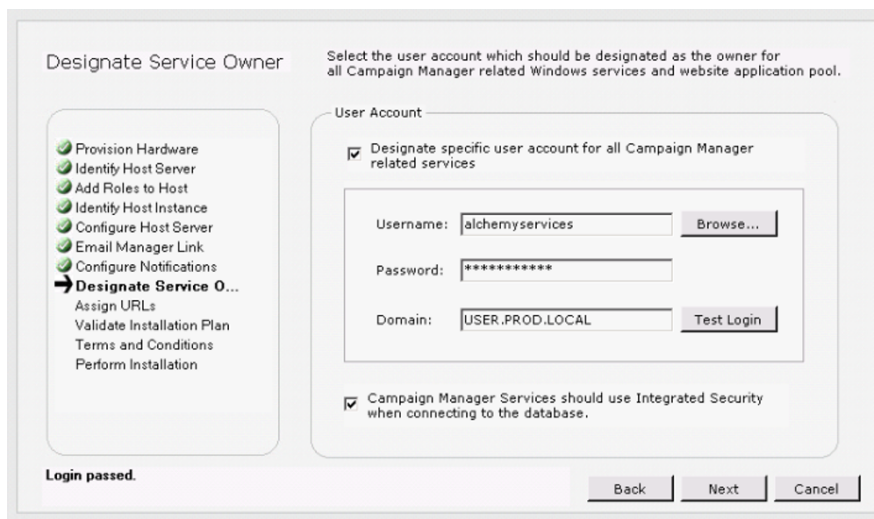
| Location | EM URL |
|----------|--------------------------------|
| Bristol | http(s)://em.emea.alterian.net |
| Denver | http(s)://em.nasa.alterian.net |
| Sydney | http(s)://em.apac.alterian.net |

NOTE: The account details shown in the screen shot are for example purposes only. If upgrading you are required to supply a URL. The above URLs are subject to change.

24. Click Test Connection to test the connection.
25. Use the 'Configure Notifications' screen to enter email details so that the system administrator receives alert notifications of any errors.



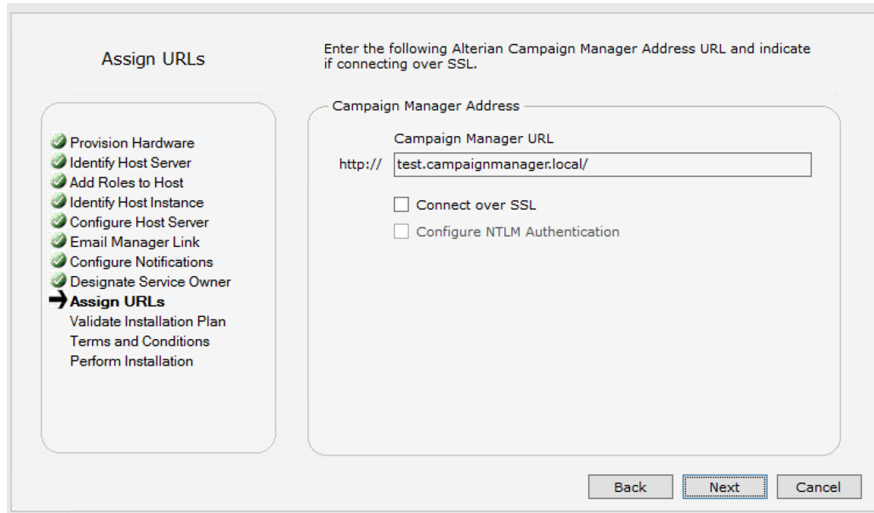
26. Enter the Domain Service Account Details. It is recommended to leave the Campaign Manager Services should use Integrated Security when connecting to the database check box selected.



27. Assign URLs screen. This is the Campaign Manager URL used for accessing CM. If you want to configure the system for multiple Campaign Manager clients and site URLs after the initial install, it is recommended that the initial URL does not contain any customer related naming. Additional clients with customer-specific site URLs can be added after the initial install.
 - a. If you select the Connect over SSL check box, it has to be the same for both Campaign Manager and Email Manager. The integration will not work if they do not share a protocol.

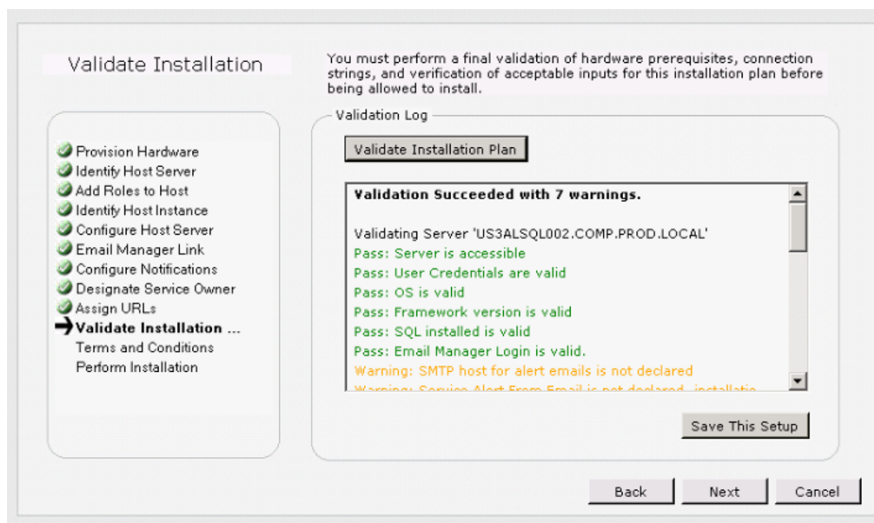
NOTE: the Campaign Manager Deployer configures SSL settings in the website web.config files, as well as in the database. However, you must install the SSL certificate in IIS, and add the necessary bindings to the hosting site.

- b. To use Windows Authentication, select the Configure NTLM Authentication check box. See the 'Windows Authentication' topic in the online Alterian product help for further information on how to configure Windows Authentication.



The URLs in the screen shot are for example purposes only.

28. Click Validate Installation Plan to perform the final validation of the configured parameters. A 'Validation Succeeded' message is displayed if successful.



29. Click Save This Setup to save the setup to a secure location.
30. Click Next.
31. Click Next to agree to the Terms and Conditions.
32. After the install is validated, click Install to start the process using the parameters entered in previous steps. A confirmation message is displayed when the installation is complete.

4.2. LAUNCHING CAMPAIGN MANAGER

To launch Campaign Manager:

1. Navigate to the location of your Campaign Manager URL.
2. The User Name is system.
3. The Password is password.
4. As part of the installation, a default user and group with the following set of permissions are created:
 - Allow Track Campaigns
 - Change Campaign States
 - Edit Campaigns

These can be used as a basis for creating system users that have access to a subset of analytical tools and campaign functionality.

You can grant additional permissions at any time. There is no restriction on creating new users with full permissions.

5. POST INSTALLATION CONFIGURATION

5.1. CONFIGURE APP SERVER

This section details the extra configuration steps that must be taken on the App Server once the installation has successfully completed.

Assuming that the Deployer has setup the IIS sites and App pool, and that all required certificates and services are installed, you will need to configure external DNS to point to external IP for the FQDN of host headers.

5.2. CONFIGURE ENGINE SERVER

This section details the extra configuration steps that must be taken on the Engine Server once the installation has successfully completed.

The following Engine configuration changes should be made:

1. To use the pause/resume and attribution features, the Application server must be accessible via `http://` or `https://` from the Engine server. If it is not accessible you can either:
 - Adjust DNS to properly resolve the FQDN of the application serverOR
 - Add a host entry to the Engine server
2. In AMC, select the Engine project. Navigate to Engine & Server Configuration, then Process Configuration. Enter an internal location for the machine setting temp folder in both the General and Machine Setting areas. If you fail to do this, the `c:\windows\temp` area is used, which may result in running out of disk space. Repeat this step for every Engine project.

NOTE: that running anti-virus software on certain Engine server folders can severely impact system performance and Engine functionality.

Exclude the following Engine folders from any anti-virus scan:

- Main Repository Folders for any Engine projects
- Engine temp folders: internal temp folders and machine settings temp folders (located under Process configurations).

Note: To avoid any pagefile issue it is recommended to set the pagefile to be system managed and not a pre-defined size.

5.3. CONFIGURE SQL SERVER

This section details the extra optional configuration steps that take place on the SQL Server after the installation has successfully completed.

To lockdown SQL permissions: for the SQL login used for the AlchemyDSA

- On the Server Roles tab:
 - Select the 'bulkadmin' and 'public' roles.
 - Select the 'dbcreator' role if you are planning to create additional client databases.
 - The 'sysadmin' server role can be cleared.
- On the User Mapping tab:
 - Select the 'public' and 'db_owner' roles for Alchemy, AlchemyStore, almain, AlterianAuth, and any additional client databases.

You must provide access to the alchemy domain service account to xp_cmdshell. In SQL Management Studio, click the master database and [new query] and enter:

```
EXEC sp_xp_cmdshell_proxy_account 'DOMAIN\user', 'password'  
GRANT exec ON xp_cmdshell TO [DOMAIN\user]
```

Change 'DOMAIN\user' and 'password' to the username and password for the alchemy domain service account.

5.4. CONFIGURE CLIENT MACHINES

The optimum screen resolution for accessing the Campaign Manager client is 1440 x 900. The application can still be used at lower resolutions, but note that usability issues may be experienced, for example scroll bars not displaying correctly.

Install Silverlight 5.1 on each client machine that will be using the software.

6. ADVANCED CONFIGURATION

6.1. IDENTITY PROVIDERS

Single sign on, with Alterian authentication, will work without the need for any configuration.

Active Directory/Windows Authentication is documented in the 'Windows Authentication' section of the online Alterian product help. For all other SAML2.0 external identity providers, contact Alterian Support.

7. INSTALLING KETTLE

Kettle, Java Runtime Environment and the Alterian External Integrations Pack plugins are included as part of a new install. If you already have the External Integrations Pack plugins installed, they will be overwritten by the new Campaign Manager 6.0 install.

For information on how to configure Kettle for use with Campaign Manager see the Pentaho Data Integration (Kettle) section in the online Alterian product help.

Note: If you have any bespoke plugins or scripts in kettle folder, these can be restored from a backup folder (data-integration.backup) in the existing install location on the App and Engine Servers. It is advised that scripts are not saved to the kettle installation directory.

8. UNINSTALLING CAMPAIGN MANAGER

You can fully uninstall Campaign Manager using the deployer.

NOTE: This will remove all SQL Server databases, all shares and system files, and all related services. Ensure that the BCP folder has been removed from the SQL server, and the temp folder has been removed from the App Sever. If you need to retain any of these files, make a backup. Prior to uninstall, the administrator must shut down Engine.

To uninstall Campaign Manager

1. Ensure that Engine has been shut down.
 2. Save the Installer package to the App Server.
 3. Run the CM.Deployer.exe file. This will launch the Installer wizard.
-

NOTE: If you have locked down the SQL Server permissions they will need to be adjusted so that the user is a member of the sysadmin role, otherwise the uninstall will fail due to insufficient permissions.

4. Select the Uninstall option and navigate the wizard selecting the applicable options.
5. Uninstall Engine using Control Panel > Programs > Programs and Features.

9. TROUBLESHOOTING

For each Deployer run, a CM.DeployerLog.txt file is created in the same folder as the deployer EXE. This contains information logged during usage of the wizard and execution of the install/upgrade/uninstall. If reporting an issue with Alterian Support, please also include the log file to assist with investigation.

The validation step also performs a range of checks to highlight potential issues with the install/upgrade.

This section provides additional information to help resolve error messages.

9.1. ERROR MESSAGES

FAIL: OS IS INVALID

Check all servers have Microsoft Windows Server 2008 R2 SP1 (x64) English Language Standard, Enterprise, Web Server edition installed, or Windows 2012 R2 Standard edition.

Microsoft Windows 7 Professional is also allowed, but not supported.

.NET FRAMEWORK 4.5.2 OR LATER REQUIRED ON APP, ENGINE AND SQL SERVER/S

Ensure that .NET framework 4.5.2 or later is installed on each server.

CURRENT USER IS NOT A MEMBER OF THE BUILT-IN ADMINISTRATORS GROUP

Recheck the pre-requisites for each server and add the common domain account as a local admin. Ensure the account has "logon as a service" right on each machine.

IIS6 WMI MANAGEMENT COMPATIBILITY MUST BE INSTALLED ON THE APP SERVER

Recheck the IIS pre-requisites for the App Server to ensure this is included.

INVALID KETTLE ZIP FILE

Contact Alterian Support as the supplied kettle zip could be corrupt.

FAIL: SERVER IS NOT ACCESSIBLE

This indicates the server cannot be accessed via Ping. Check the items in the Installation Prerequisites section of this guide, for example firewall configuration between servers; check the common domain account has local administrator access to all servers; check the servers are accessible on the domain e.g. by using the command line Ping utility to verify accessible.

FAIL: USER CREDENTIALS ARE INVALID

Check the common domain account has local administrator access on all servers.

FAIL: FRAMEWORK VERSION IS INVALID

Check all servers have Microsoft .Net framework v4.5.2 or later 64 bit installed.

FAIL: SQL IS NOT VALID

The Deployer expects SQL 2008 R2 Standard or Enterprise Edition product version 10.50.nnnn.n, SQL Server 2012, or SQL Server 2014 SP1

To check the product version use `SELECT @@Version` on the SQL Server.

FAIL: IIS IS INVALID

The Deployer expects IIS7, IIS8 or above.

FAIL: EMAIL MANAGER ACCOUNT LINK NAME MUST BE SPECIFIED

The link name must be completed in the Configure Email Manager link step. Click the Test Connection button to populate with a default link name, based on the EM account details.

FAIL: EMAIL MANAGER UNABLE TO VALIDATE URL

Check the Email Manager URL is reachable from the App server (e.g. using Internet Explorer)

FAIL: ALCHEMY SERVICE CREDENTIALS ARE INVALID (OR); FAIL: SERVICE CREDENTIALS FAILED DB CONNECTION

Check the service account has local admin rights on each server.

Check the account has a corresponding login on the SQL Server. On a clean install, this should be a member of the sysadmin role, before proceeding with locking down the permissions after the install.

FAIL: INACCESSIBLE XXXX COMPONENT (ID N)

The Deployer checks that each component is accessible prior to upgrade.

The component information is obtained from the `Almain.AL.ProcessIndex` table, which contains an ID, hostname, and networkPath for each component.

The validation message will provide an ID for a component entry that cannot be reached.

This may be due to accessibility problems (e.g. the Deployer cannot reach the file share indicated by the networkPath). To verify this, use Windows Explorer to ensure the networkPath can be reached, and is writeable (e.g. create a temp file).

If the component entry is invalid (e.g. the networkPath does not exist) please contact Alterian Support. This may be due to a previously failed install, and the component should be reviewed and removed if necessary before retrying validation.

FAIL: INSTALL FOLDER CANNOT BE CREATED AND SHARED

This fail occurs if the Deployer cannot create or share the installation folder due to insufficient permissions. Perform the following checks:

- That the Deployer was started using the 'Run as Administrator' option
- The Deployer user is a local admin
- That the File and Print sharing feature is enabled on the server
- That the firewall is disabled
- The Remote Registry Windows service can be started (i.e. startup mode Automatic)

HTTP ERROR 500.0 - INTERNAL SERVER ERROR CALLING LOADLIBRARYEX ON ISAPI FILTER "C:\WINDOWS\MICROSOFT.NET\FRAMEWORK\V4.0.30319\ASPNET_FILTER.DLL" FAILED

This fail occurs if an ISAPI filter entry exists for "ASP.NET_4.0.xxxxx" referencing the 32 bit .Net framework. To resolve the issue:

1. Open IIS Manager on the App Server.
2. Click the server and double click ISAPI Filters.
3. If an ISAPI filter entry exists for "ASP.NET_4.0.xxxxx" referencing the 32 bit .Net framework, remove this entry.
4. The .NET Framework 4.0 entries for "ASP.Net_4.0_32bit" and "ASP.Net_4.0_64bit" are valid should be retained.
5. Browse to Campaign Manager after removing the ISAPI entry.

FAIL: ENGINE ALREADY INSTALLED

For a clean install of Campaign Manager 6.0, the Engine server must not contain any previous version of Engine. Please uninstall Engine via the Control Panel Add/Remove programs option from the specified server and retry.

FAIL – SQL FILESTREAM: FULL ACCESS NOT CONFIGURED

Check the SQL instance has Full filestream access enabled in SQL Server Management Studio. In the SQL Server Configuration Manager, check the server has Filestream enabled for Transact-SQL and File I/O accessFail

FAIL: ENGINE PROJECTBASE PATH EXISTS

For clean install, an existing Engine installation Projectbase folder must not exist. Remove or rename the specified folder

FAIL: ENGINE INSTALL PATH NOT ACCESSIBLE; FAIL: ENGINE PROJECTBASE PATH NOT ACCESSIBLE

Check the specified path can be accessed on the Engine server. The drive should be writable for access by the Campaign Manager Deployer user account.

FAIL: UNIVERSAL C RUNTIME NOT INSTALLED

Version 10.0.10240.0 of this component is required, See **Common Prerequisites (All Servers)** on page 8 for further details.

FAILURE TO RUN KETTLE FROM CAMPAIGN MANAGER

If you cannot run Kettle jobs from CM, check Java is installed on the server and the JAVA_HOME environment variable references a valid location for the Java runtime. To access the environment variable, open Control Panel > System > Advanced system settings and click the Environment Variables button. Add or update the JAVA_HOME value in the System variables section of the dialog that opens. Click OK to ensure the new value is propagated to the system.

FAILURE TO INSTALL JAVA

If the Java prerequisite installation fails with error code '1' in the deployer log, check if you have logged on to each server with the user account used for running the CM deployer. This ensures the required user profile is present on each server.

9.2. ENGINE TROUBLESHOOTING

The Engine Suite component is installed by the Campaign Manager Deployer on the App and Engine server/s. If the Engine installer returns an error:

- The MSI error code will be displayed in the deployer GUI
- The Engine installation will be rolled-back, and the deployer run will be aborted before attempting Campaign Manager.
- Detailed logging for the failure is included at the end of the CM Deployer Log file.

Summary information for MSI return codes can be found here: <http://msdn.microsoft.com/en-us/library/aa376931%28v=vs.85%29.aspx>

To investigate any failure, the full Engine MSI and bundle log files are located in the:

- Deployer package Integrations folder when Engine is installed on the App server.
- Alchemy share TempInstall folder when Engine is installed on a dedicated server.

The main MSI log file will be named in the following format "Engine.InstallLog-YYYY_MM_DD_HH_MM_SS_pkgEngineMsi.txt".

Take the MSI error code displayed in the Deployer, and locate all instances of the code in the MSI log file (you can do this using Notepad, for example). The MSI log file should

provide further details on the issue. After resolving the issue, re-run the deployer to attempt install again.

10. APPENDICES

10.1. APPENDIX A – ADDING EM URLS

This appendix documents how to add an EM URL to Campaign Manager 6.0 if the EM URL was not created at the time Campaign Manager was deployed.

db_owner access to Almain, AlterianAuth and CM client databases are needed to run the utility. The utility uses Windows Authentication to connect with the SQL Server.

ADDING AN EM URL

1. Run the SysAdminApp.exe utility located in the PauseResume folder under the CM install location on the Engine Server.
2. Open a command prompt and change directory to the PauseResume folder location.
3. Run the utility using the following command:
 - Sysadminapp /sqlserver=sqlservername /addEMSite

If you have multiple Campaign Manager URLs configured the utility will ask which Campaign Manager URL to associate the new Email Manager site with.



Replace sqlservername based on your SQL Server name. If the Campaign Manager SQL Server isn't the default instance, supply the sqlserver as sqlservername\instancename. If SQL Server is installed as the default instance, use the machine name rather than (local) or "."

The utility only adds an Email Manager site if an Email Manager site has not already been configured.
