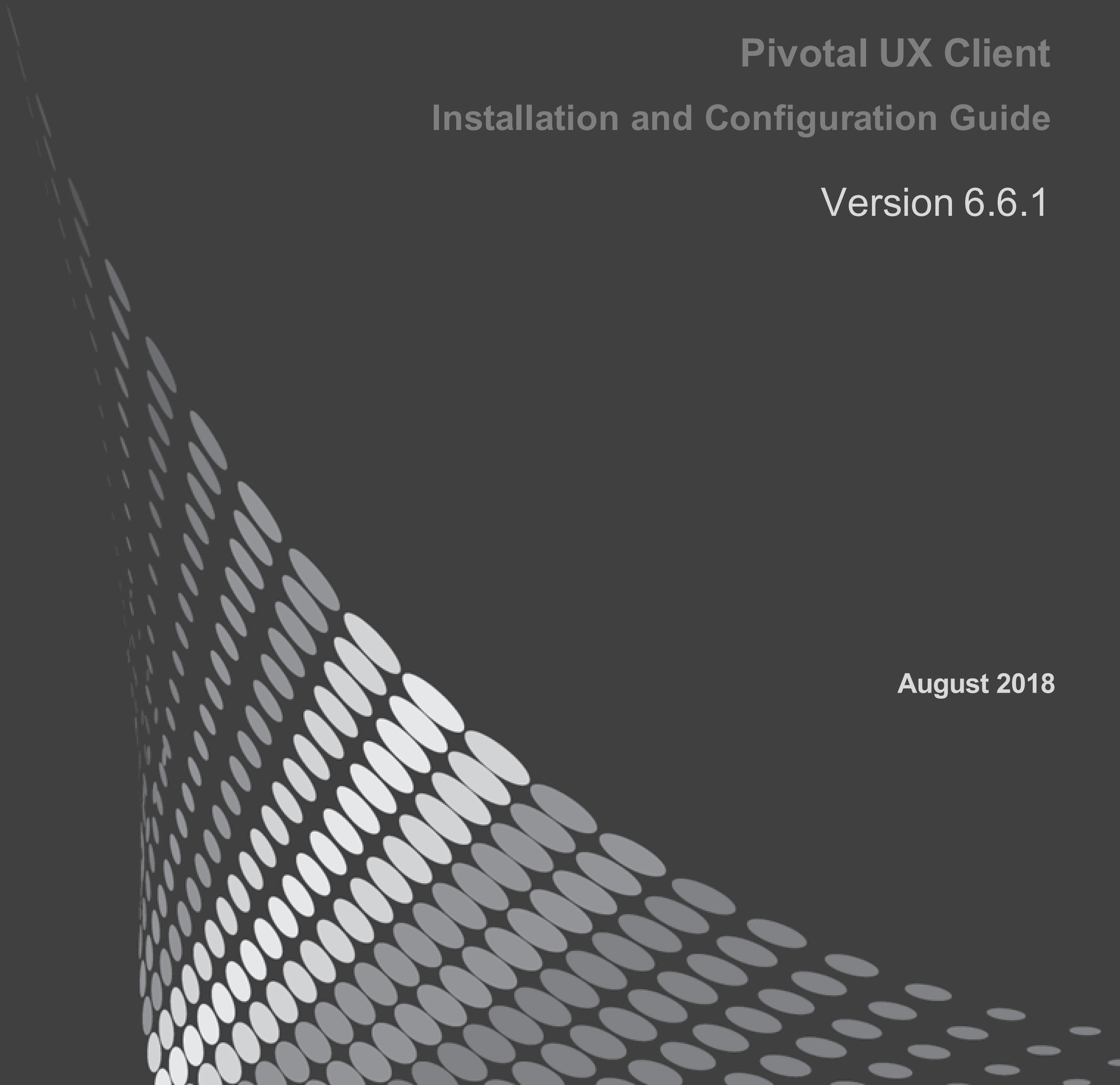
PIVOTAL CRM

Pivotal UX Client

Installation and Configuration Guide

Version 6.6.1



August 2018

APTEAN

4325 Alexander Drive, Suite 100 • Alpharetta GA 30022-3740 • www.aptean.com • info@aptean.com

Copyright © 2018 Aptean. All Rights Reserved. These materials are provided by Aptean for informational purposes only, without representation or warranty of any kind, and Aptean shall not be liable for errors or omissions with respect to the materials. The only warranties for Aptean products and services are those set forth in the express warranty statements accompanying such products and services, if any, and nothing herein shall be construed as constituting an additional warranty. No part of this publication may be reproduced or transmitted in any form or for any purpose without the express written permission of Aptean. The information contained herein may be changed without prior notice. Some products marketed by Aptean contain proprietary software components of other software vendors. Aptean and other Aptean products and services referenced herein as well as their respective logos are registered trademarks or trademarks of Aptean or its affiliated companies.

Contents

1

Introduction

Overview

Pivotal UX Client enables users to access Pivotal CRM data and functionality by using browsers on devices and desktop computers, through a URL. Pivotal CRM Sales UX Edition application provides out-of-the-box elements such as forms, searches, subjects, and topics that can be accessed by Pivotal UX Client. The Pivotal CRM Sales UX Edition application can optionally be installed on an existing CMS or PCM with SFA systems to use the out-of-the-box form, navigation, and other elements.

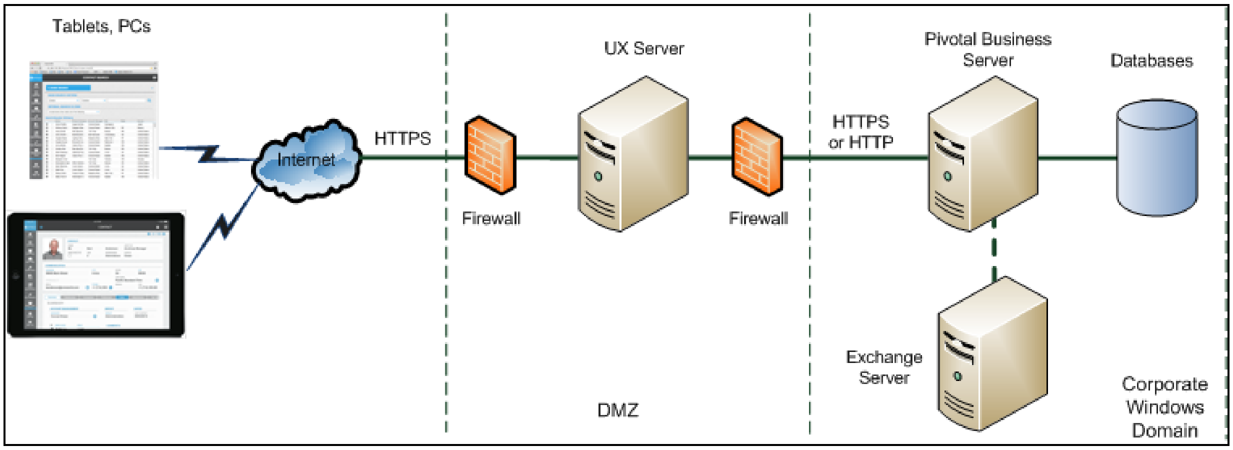
Customizers can use Pivotal Toolkit to create new UX Forms and navigation that can be used on Pivotal UX Client. For more information about customizing Pivotal UX Client, refer to the *Chapter 5, Pivotal Toolkit Guide.*

What's New in This Document

- Enhanced Security Policy: Enhanced security for Cross Site Scripting attacks and secured HTTP headers.
- Configuring User Exchange Accounts: Pivotal 6.6.1 has provided an option for Administrator to map a Pivotal user to an Exchange user using email address for the user.

Architecture

The image below illustrates the Pivotal CRM 6.6.1 architecture with Pivotal UX Client.



Pivotal CRM 6.6.1 has a three-tier architecture:

- Data Layer: Includes the databases. The Business module contains the meta data for CMS or PCM with SFA application.
- Business Logic Layer: Includes the Pivotal UX Server and the Pivotal Business Server.
- Presentation Layer: Includes Pivotal UX Client on devices or desktop computers.

The Pivotal UX Client sends requests over HTTP(S) to the UX Server. The UX Server processes the request, and delegates it to the PBS. The UX Server then waits for a response from the PBS, packages the response, and sends it back to the UX Client, which displays the data in the browser.

❗ **Important:** Use HTTPS between the UX Server and the browser or device to encrypt data, usernames and passwords.

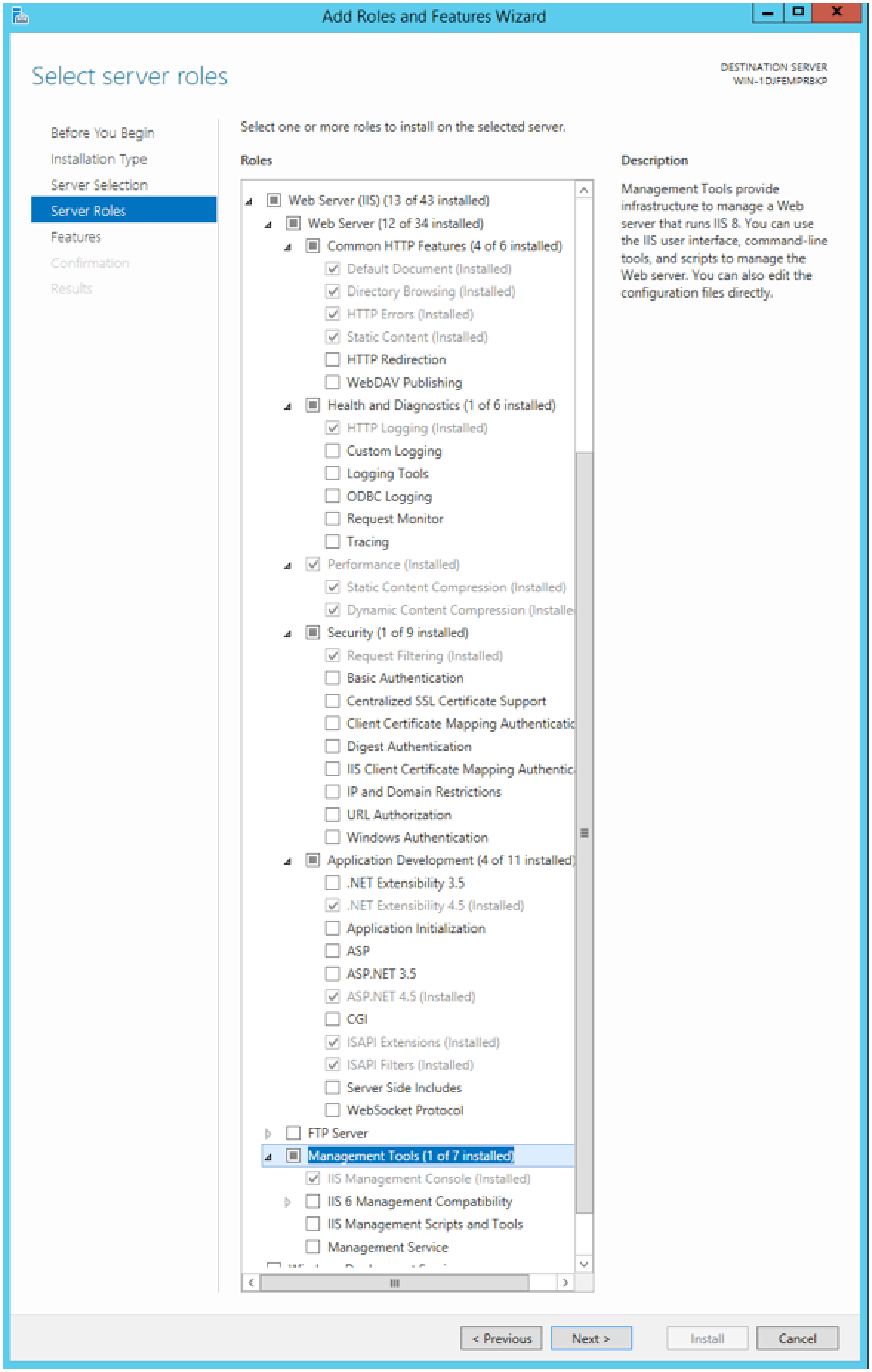
Prerequisites

Before installing Pivotal UX Client, ensure that you have installed and configured the following:

- Pivotal CRM 6.6.1
- For CMS Version
  - Customer Management System 6.0.5
  - Pivotal Foundation Library 6.0 SP1 HF2
- For PCM Version
  - Pivotal Contact Management 6.6
  - Sales Force Automation 6.0.8 HF4

The following are the software features required to use Pivotal UX Client on Windows Server 2012 R2 version:

- Web Server:
  - Common HTTP Features
  - Dynamic Contact Compression (recommended)
  - Security: Windows Authentication if this is being used for UX login (not required for OAUTH and SSO)
  - Application Development: .NET Framework 4.7



Select server roles

DESTINATION SERVER
WIN-1DJFEMPRBKP

Select one or more roles to install on the selected server.

Roles

- ▣ Web Server (IIS) (13 of 43 installed)
  - ▣ Web Server (12 of 34 installed)
    - ▣ Common HTTP Features (4 of 6 installed)
      - ☑ Default Document (Installed)
      - ☑ Directory Browsing (Installed)
      - ☑ HTTP Errors (Installed)
      - ☑ Static Content (Installed)
      - ☐ HTTP Redirection
      - ☐ WebDAV Publishing
    - ▣ Health and Diagnostics (1 of 6 installed)
      - ☑ HTTP Logging (Installed)
      - ☐ Custom Logging
      - ☐ Logging Tools
      - ☐ ODBC Logging
      - ☐ Request Monitor
      - ☐ Tracing
    - ☑ Performance (Installed)
      - ☑ Static Content Compression (Installed)
      - ☑ Dynamic Content Compression (Installe
    - ▣ Security (1 of 9 installed)
      - ☑ Request Filtering (Installed)
      - ☐ Basic Authentication
      - ☐ Centralized SSL Certificate Support
      - ☐ Client Certificate Mapping Authenticatic
      - ☐ Digest Authentication
      - ☐ IIS Client Certificate Mapping Authentic
      - ☐ IP and Domain Restrictions
      - ☐ URL Authorization
      - ☐ Windows Authentication
    - ▣ Application Development (4 of 11 installed)
      - ☐ .NET Extensibility 3.5
      - ☑ .NET Extensibility 4.5 (Installed)
      - ☐ Application Initialization
      - ☐ ASP
      - ☐ ASP.NET 3.5
      - ☑ ASP.NET 4.5 (Installed)
      - ☐ CGI
      - ☑ ISAPI Extensions (Installed)
      - ☑ ISAPI Filters (Installed)
      - ☐ Server Side Includes
      - ☐ WebSocket Protocol
  - ☐ FTP Server
  - ▣ Management Tools (1 of 7 installed)
    - ☑ IIS Management Console (Installed)
    - ☐ IIS 6 Management Compatibility
    - ☐ IIS Management Scripts and Tools
    - ☐ Management Service

Description

Management Tools provide infrastructure to manage a Web server that runs IIS 8. You can use the IIS user interface, command-line tools, and scripts to manage the Web server. You can also edit the configuration files directly.

Hardware and Software Requirements

The following devices are supported:

- Surface Pro 3
- iPad Air
- iPhone 6 and iPhone 6S Plus
- Samsung Galaxy S2
- Samsung Galaxy S7
- Google Pixel

The following operating systems are supported:

- iOS 11.4
- Android 6
- Android Marshmellow
- Windows 8.1
- Windows 10

The following browsers are supported:

- Internet Explorer 11.0.9600.18537+
- Chrome 56+
- Firefox 51+
- Safari 10.0+
- Microsoft Edge 25.10586+
- Samsung Internet stock browser version 4

Installers

The installers described in the following table are provided for installing Pivotal UX Client and Pivotal Sales for UX application. For more information on Sales for UX Installation, refer to the *Sales for Pivotal UX 6.6 Installation and Configuration guide*.

No.	Installer	Description
1	Pivotal UX Client Installer	Installs Pivotal UX Client in the `..\Program Files (x86)\Aptean\Pivotal CRM\UX Client` folder. This folder contains the following folders: • `CSVs`: Contains language definition strings for Pivotal UX Client • `\Localization\<Language Code>`: Language definitions strings for specific language for Pivotal UX Client • `Development Tools`: Contains scripts to stop and start Pivotal services. Also, includes REST API tester and Exchange Tester Tools. • `Documentation`: Contains technical reference guide for Pivotal UX Client • `Themes`: Contains pre-built themes for Pivotal UX Client • `www`: Contains the install code for Pivotal UX Client If you opt to install the source code for Pivotal UX Client, the code is installed under the `..\Program Files (x86)\Aptean\Pivotal CRM\UX Client\www\Client` folder.
2	Sales for Pivotal UX Installer	Refer to the *Sales for Pivotal UX 6.6 Installation and Configuration Guide*. **Note:** For existing users, upon upgrading to 6.6.1 UX platform, do the following changes based on the application: • For UX application versions prior to 6.5.2, uninstall and reinstall the application pointing to `..\Program Files (x86)\Aptean\Pivotal CRM\UX Client\` • For application version Pivotal UX 6.5.2 onwards, manually copy the applications folder and Scripts related to the applications in `www\scripts` folder to installed UX location and `www\scripts` respectively.

2

Installing Pivotal UX Client

Installing Pivotal UX Client

Install Pivotal UX Client on the server machine.

To install UX Client

1. Browse to the location where you unzipped the `PivotalUXClient6.6.1.zip` file.
2. Run `setup.exe`.
3. Click **Next**, accept the license agreement, and click **Next**.
4. In the **Destination Folder** screen, perform the following steps:

- Select the feature that needs to be installed from the following options:
  - UX Client and REST API

Note: You will require license, if you select this option.

  - REST API only: If you need to consume only REST API and do not require UX client, then select this option. Else, select UX Client and REST API.
- Accept the default install path or optionally, change the path.

1. Select the **Install Client source code here** check box to install the code. You can install the code if you are a licensed user of Sencha ExtJS and want to perform advanced customization on the core platform of Pivotal UX Client.

Note: You do not need to install the Pivotal UX Client source code to write UX Client Scripts. You can perform regular customization of business logic without installing the source code.

2. Click **Next**.
3. In the **Website Application** screen, specify the details of the UX Client website and click **Next**. This site is accessed by the end-users in their browsers on devices or desktop computers.
4. In the **Set Application Pool Identity** screen specify the credentials under which the web application is run. Select one of the following options and click **Next**.

   - **Built-in account "ApplicationPoolIdentity"**

     a. Select any of the following authentication type:

        - **OAUTH Authentication** to display a login form requesting the user's Windows credentials.

        - **Windows Authentication** to run the website as the current logged on user.
        - **SAML SSO Authentication**
        - **OAUTH and SAML SSO Authentication**

          For more information on **SAML SSO Authentication** and **OAUTH and SAML SSO Authentication**, refer *Pivotal UX Single Sign on Technical Overview*.

     b. Click **Next**

- **Specified user account**

     a. If you select this option, you must specify the credentials of a valid Windows user account under which the website is run. In the Application Pool Identity screen, specify the **Domain name**, **User Name**, and **Password** for the Windows user account.

     b. Click **Next**.

     c. Select any of the following authentication type:

        - **OAUTH Authentication** to display a login form requesting the user's Windows credentials.
        - **Windows Authentication** to run the website as the current logged on user.
        - **SAML SSO Authentication**
        - **OAUTH and SAML SSO Authentication**

          For more information on **SAML SSO Authentication** and **OAUTH and SAML SSO Authentication**, refer *Pivotal UX Sigle Sign On Technical Guide*.

     d. Click **Next**.

5. A message box is displayed prompting to setup the `Web.config` file. Click **Yes** to specify options to set up access to a Pivotal system in the `Web.config` file. If you click **No**, the `Web.config` file is not updated. You can however, edit the file later to include authentication details.
6. If you click **Yes** in the message box, **Configure the web.config file** screen is displayed. Specify the Pivotal environment details.

   a. In the **Environment Name** box, specify the Pivotal CRM environment name.

   b. In the **Description** box, specify a description. This description is displayed on the Web site.

c. In the **PBS server URL** box, specify the PBS server address in the `http://<server name/IP>` or `https://<server name/IP>` format.

d. In the **Pivotal System Name** box, specify the name of the Pivotal Production or Offline system that is defined on the Pivotal Business Server computer.

e. Click **Next**.

f. In the **Enter the Identity to connect to the PBS** screen, select an authentication method and click **Next**.

g. If you select **Specified user account**, specify the **Domain name**, **User Name**, and **Password** for the Windows account that is used to access the PBS URL, and click **Next**.

Note: If you don't specify user account and select appPoolIdentity, appPoolidentity credentials are used to authenticate and connect to PBS URL.

11. In the **Options** screen:

a. Optionally select **Enable Demo Mode** to enable demo mode for a specific licensed Pivotal user. Enabling Demo Mode displays a **Demo** button on the login screen, enabling the users to bypass entering credentials.

Note: Alternatively, you can enable demo mode after the installation is complete by modifying the `Web.config` file. For more information, see *Enabling Demo Mode on page 3-7*.

b. Select **Enable Google Maps** to enable the display of maps for relevant fields, such as **Address** when a record is opened.

Note: To enable Google Maps you need a valid Google Maps API key.

c. Select **Allow insecure HTTP** to enable HTTP. If you do not select this check box, HTTPS protocol is used.

d. Select **Enable Online REST API documentation** check box to enable REST API documentation to be available online.

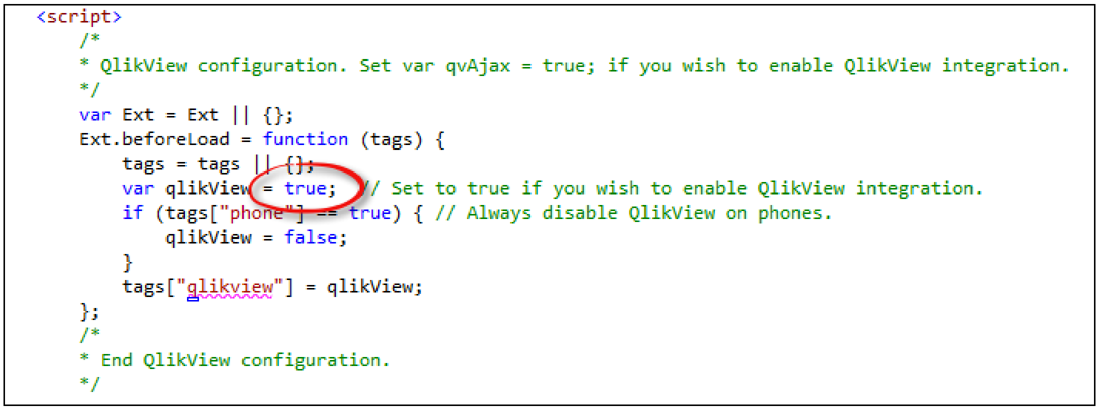
12. Click **Next**.

13. If you have selected **OAUTH Authentication**, you can optionally specify the Default Domain and click **Next**.This is used if a user enters their Windows name in the login form without a domain specified

14. Click **Install**. If you have selected Windows Authentication, a warning message prompting that IIS authentication could not be set. Click **OK** to proceed with the installation. You need to manually set the authentication mode after the installation. For more information about setting authentication mode, *Changing Authentication Mode on page 3-5*.

15. For system where previously UX Client was installed, a message box with backup details of `Web.config` file is displayed, click **Accept**.
16. When the installation is complete, click **Finish**.
17. If an old `web.config`file was backed up then manually merge any custom changes in it into the installed `web.config` file.
18. If QlikView integration is required then enable it in the `Pivotal UX index.html` file at: `..\Program Files (x86)\Aptean\Pivotal CRM\UX Client\www\index.html..`

    Set the qlikView variable to true, as shown below:



```
<script>
    /*
    * QlikView configuration. Set var qvAjax = true; if you wish to enable QlikView integration.
    */
    var Ext = Ext || {};
    Ext.beforeLoad = function (tags) {
        tags = tags || {};
        var qlikView = true; // Set to true if you wish to enable QlikView integration.
        if (tags["phone"] == true) { // Always disable QlikView on phones.
            qlikView = false;
        }
        tags["qlikview"] = qlikView;
    };
    /*
    * End QlikView configuration.
    */
```

Note: The above script always disables QlikView on mobile phones because it is not optimized for small devices.

Import CSV File

Import the UX Client Language strings by importing the `..\Program Files (x86)\Aptean\Pivotal CRM\UX Client\CSVs\UX Platform Strings - English 0x0409.csv` file.

To import the strings

1. In Pivotal Toolkit, on the **eTab**, click **Pivotal Agents**, and then click **List of Agents**.
2. In the **Agents** window, double-click **Language**, double-click **Import and Export**, and then click **Import System Strings**.
3. In the **Instruction** dialog box, click **OK**.
4. In the **Import File** dialog box, browse to the `..\Program Files (x86)\Aptean\Pivotal CRM\UX Client\CSVs` directory and select `UX Platform Strings - English 0x0409.csv`.

    A message box is displayed when the strings are imported.

3

Configuration Procedures

Configuring Pivotal UX Client

Configuring Pivotal UX Client involves the following procedures:

- Configuring Activity Management
- Changing the Authentication Mode
- Creating a Standard Email Template
- Enabling Demo Mode

Configuring Activity Management

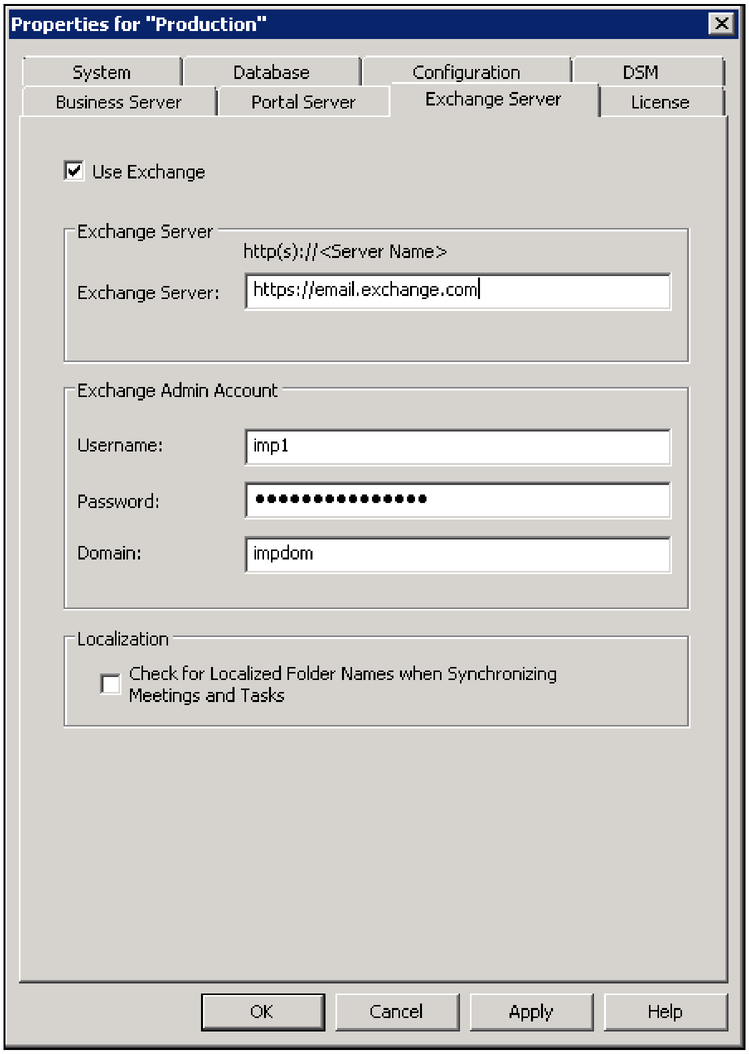
Activity Management enables a user to send emails, set appointments or meetings and tasks using Pivotal UX Client. Pivotal UX uses Exchange Impersonation to use the Activity Management feature.

Create an Exchange Impersonation account. For more information about creating an Exchange impersonation account:

- On Microsoft Exchange Server 2007, refer to http://msdn.microsoft.com/en-us/library/bb204095(v=exchg.80).aspx.
- On Microsoft Exchange Server 2010, refer to http://msdn.microsoft.com/en-us/library/office/bb204095(v=exchg.140).aspx.
- On Microsoft Exchange Server 2013, refer to http://msdn.microsoft.com/en-us/library/office/dn722377(v=exchg.150).aspx.
- On Microsoft Office 365, refer to https://msdn.microsoft.com/en-us/library/office/dn722376(v=exchg.150).aspx.

To configure Activity Management

1. On the Administration computer, open the **Pivotal Administration Console**.
2. Right-click the Offline/Production System and click **Properties**.
3. In the **Properties** dialog box, click **Exchange Server**.



☑ Use Exchange

Exchange Server

http(s)://<Server Name>

Exchange Server: https://email.exchange.com

Exchange Admin Account

Username: imp1

Password: •••••••••••••••

Domain: impdom

Localization

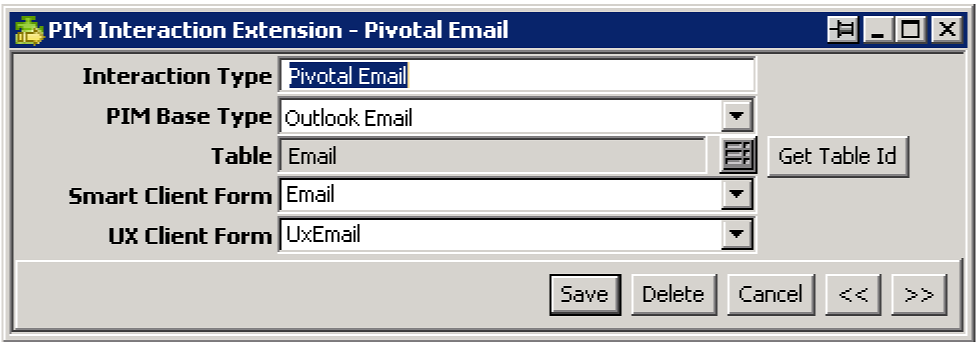
□ Check for Localized Folder Names when Synchronizing Meetings and Tasks

4. Specify the **Exchange Server URL** and the **Exchange Admin Account** details. Ensure that the impersonation user is a licensed Pivotal user.
5. Click **OK**.

After configuring Activity Management, you must modify the Interaction Extension forms for Pivotal Email, Pivotal Call, and Pivotal Meeting with the UX Client form details.

To specify Pivotal UX Client form for Interaction Extension form

1. In Pivotal Toolkit, on the **eTab**, click **Interaction Extension**, and then click **List of Interaction Extension**.
2. In the **List of Interaction Extension** click an Interaction Extension, such as **Pivotal Email**.
3. In the **PIM Interaction Extension - <Name>** dialog box, select the relevant **UX Client Form** from the drop-down list.



PIM Interaction Extension - Pivotal Email

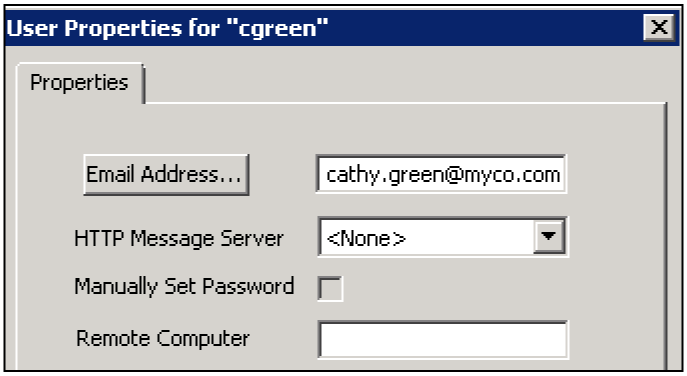
Interaction Type	Pivotal Email
PIM Base Type	Outlook Email
Table	Email
Smart Client Form	Email
UX Client Form	UxEmail

4. Click **Save**.
5. Repeat steps 2 through 4 for all the Interaction Extensions.
6. Apply Customization Changes on the Production System.

Configuring User Exchange Accounts

Each user using Activity Management must have the following:

- A valid mailbox on the Exchange server
- The mailbox must allow impersonation
- A mailbox or an alias that matches the Windows username of the user. That is, if the user's Windows login is "cgreen" then the Exchange mailbox must be "cgreen" or the mailbox has an alias of "cgreen". An alias of mailbox such as "cgreen@myco.com" will not work because it has to match the Windows username. If you have not configured alias in Exchange, then you need to specify the email address in Pivotal Administration Console (refer to the following image).



User Properties for "cgreen"

Email Address...	cathy.green@myco.com
HTTP Message Server	<None>
Manually Set Password	□
Remote Computer	

Note: Ensure that the authenticated user (or demo user you specified in the `Web.config` file) has a valid mailbox on the Exchange server, that it allows impersonation, and that it has a mailbox or alias that matches the Pivotal username. The Pivotal username is the Windows username of the user. That is, if the user's Windows login is "cgreen" then the Exchange mailbox must be "cgreen" or the mailbox must have an alias of "cgreen".

In the case where more than one mailbox matches the Pivotal username then use aliases to ensure only one mailbox has an alias with that username. For example, "Brian.Smith@myco.com" and "Brian.Jones@myco.com" can be matched by Exchange with a username of "brian" (use Outlook's "Check Names" function to test). Create an alias of "brian" for one of the mailboxes.

If you have not configured alias in Exchange, then you need to specify the email address in Pivotal Administration Console using the following steps:
- In Pivotal Administration Console, right-click the User Name > Click **User Properties** > Enter the email address of the user in **Email Address** field.
Please ensure that the length of email id does not exceed 99 characters.

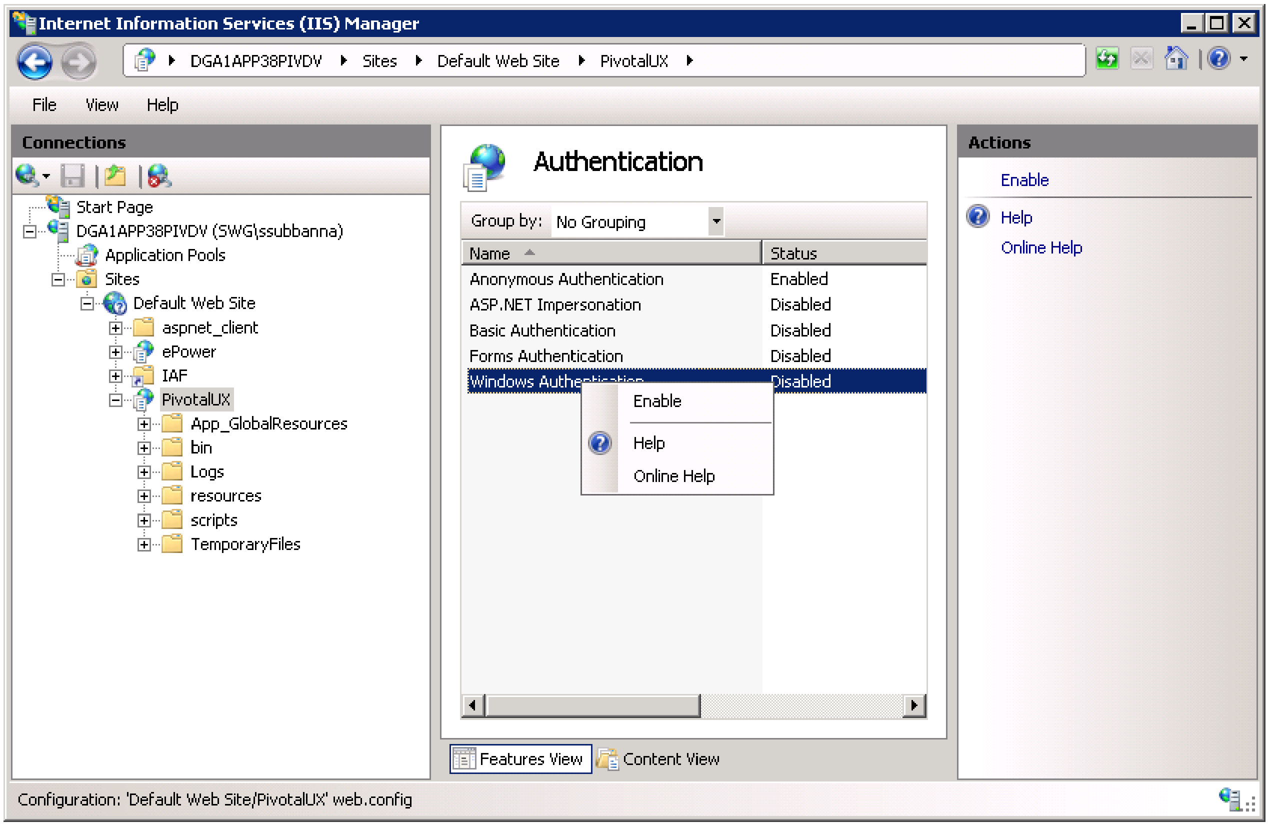
For more information about a demo user, see *Enabling Demo Mode on page 3-7*.

Changing Authentication Mode

If you want to change the authentication mode between Windows authentication and OAUTH/SSO authentication, you must change the authentication option in IIS Web App and in the `Web.config` file.

To change the authentication mode

1. Open **IIS Manager**.
2. In **IIS Manager**, double-click **Authentication** under the **IIS** group.
3. In the **Authentication** window, to enable Windows Authentication mode, right-click **Windows Authentication**, and click **Enable**. To enable OAUTH/SSO authentication, right-click **Anonymous Authentication** and click **Enable**.



Name	Status
Anonymous Authentication	Enabled
ASP.NET Impersonation	Disabled
Basic Authentication	Disabled
Forms Authentication	Disabled
Windows Authentication	Disabled

Configuration: 'Default Web Site/PivotalUX' web.config

Note: When you enable an authentication mode, ensure that you disable the other mode.

4. Navigate to the `..\Program Files (X86)\Aptean\Pivotal CRM\UX Client\www` folder and open the `Web.config` file.
5. In the `Web.config` file, locate the `<appSettings>` tag.

```
        <!-- Custom settings for the whole web application. -->
        <appSettings>

          <!-- AuthenticationMode. Determines if Pivotal UX is using Windows or OAuth authentication.
          Supported values for AuthenticationMode  | IIS authentication configuration:
                        "OAuth"                    | Your application must have Anonymous
    Authentication enabled.
                        "Windows"                  | Your application must have Windows
    Authentication enabled (and only the NTLM provider - for iPad support) and Anonymous
    Authentication disabled.
          NOTE: If using Windows authentication then iPad only supports the NTLM provider, and not
    "Negotiate".
          -->
          <add key="AuthenticationMode" value="OAuth" />
```

6. Change the value of the `AuthenticationMode` key to `Windows` or `OAUTH` to match the value set in the **IIS Authentication** window.
7. Save `Web.config`.

8. Restart IIS.
9. Restart PBS.

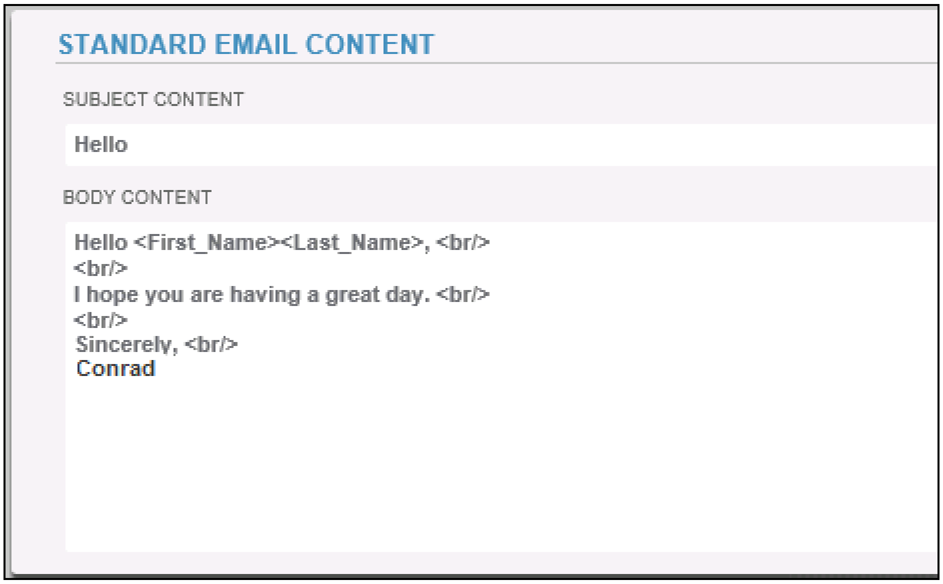
Creating Standard Email Template

Note: An administrator has to be a part of the **UX Contact Management Administrators** group or **Administration** subject must be copied to the relevant security group before you create a standard email template.

To set standard email template

1. In Pivotal UX Client, click/tap on the **Administrator** > **New Standard Email** topic.
2. The **Standard Email** template is displayed.

   While creating a standard email template, you must explicitly specify the database field values that you want to use in the template and any other formatting, such as line breaks, using HTML tags. Ensure that you specify the tag for the sender's name as `<From_EmployeeName>`. The name in the Employee records of the current logged on user is used. For example, in the following image, an email template with First Name and Last Name is created with appropriate line breaks, and the sender's name is specified as `<From_EmployeeName>`. In this case if Conrad is the current logged on user, `<From_EmployeeName>` is replaced with `Conrad Green`.



STANDARD EMAIL CONTENT

SUBJECT CONTENT

Hello

BODY CONTENT

Hello <First_Name><Last_Name>,
<br/>
I hope you are having a great day. <br/>
<br/>
Sincerely, <br/>
Conrad

3. Specify the content and save.

You can use this template to send standard emails from a **Lead** form.

Enabling Demo Mode

You can enable the Demo Mode by modifying the `Web.config` file.

To enable Demo Mode in Web.config file

1. Navigate to the `..\Program Files (x86)\Aptean\Pivotal CRM\UX Client\www` folder on the Pivotal server.
2. Open `Web.config` as an Administrator.
3. Locate `<DemoUser...>` tag.
4. Edit the tag as follows to enable Demo Mode:.

   ```
   <DemoUser allow="true" pivotalusername="[Licensed Pivotal
   User]">
   ```

   When you specify a licensed Pivotal user as the demo user, the credentials of that user is used to log on to Pivotal UX Client when the user clicks the **Demo** button on the Pivotal UX Client website.

5. Save the `Web.config` file.

Note: For information on configuring SHA-256 password encryption for User Management 6.6, refer to the KB 43413.

4

Enhancing Security

Setting HTTP Response Headers

You can achieve enhanced security for UX Client application using the HTTP response headers. Setting the HTTP response headers can restrict modern browsers from running into easily preventable vulnerabilities. Administrators can modify the HTTP response headerss in `web.config` based on their need or customization done in UX Client.

> ⚠ **Caution:** When choosing the directive, please ensure to test in the Development environment before applying in the production environment.

The following are the HTTP response headers that UX Client application can use to enhance the security:

- X-Frame-Options
- X-XSS-Protection
- X-Content-Type-Options
- Access-Control-Allow-Methods
- Access-Control-Allow-Origin
- Content-Security-Policy
- HTTP Strict Transport Security
- Referrer-Policy

X-Frame-Options

X-Frame-Options response headers improve the protection of web applications against `Clickjacking`. It declares a policy communicated from a host to the client browser on whether the browser must not display the transmitted content in frames of other web pages.

The default value of the X-Frame-Options response header in the `web.config` is `<add name="X-Frame-Options" value="SAMEORIGIN"/>`

Value	Description
deny	No rendering within a frame.
sameorigin	No rendering if origin mismatch.
allow-from: DOMAIN	Allows rendering if framed by frame loaded from DOMAIN.

X-XSS-Protection

X-XSS-Protection response header enables the Cross-site scripting (XSS) protection in browser and instructs the browser to block the response in the event of a malicious script getting inserted from the user input, instead of sanitizing.

The default value of the X-XSS-Protection response header in the `web.config` is `<add name="X-XSS-Protection" value="1; mode=block" />`

Value	Description
0	Filter disabled.
1	Filter enabled. If a cross-site scripting attack is detected, in order to stop the attack, the browser will sanitize the page.
1; mode=block	Filter enabled. Rather than sanitizing the page, when an XSS attack is detected, the browser will prevent rendering of the page.
1; report=http://[YOURDOMAIN]/your_report_URI	Filter enabled. The browser will sanitize the page and report the violation. This is a Chromium function utilizing CSP violation reports to send details to a URI of your choice.

X-Content-Type-Options

Setting this header prevents the browser from interpreting files as something else than declared by the content type in the HTTP headers.

The default value of the X-Content-Type-Options response header in the `web.config` is `<add name="X-Content-Type-Options" value="nosniff" />`

Value	Description
nosniff	Prevents the browser from MIME-sniffing a response away from the declared content-type.

Access-Control-Allow-Methods

The Access-Control-Allow-Methods response header specifies the method or methods allowed when accessing the UX API in response to a preflight request.

The default value of the Access-Control-Allow-Methods response header in the `web.config` is `<add name="Access-Control-Allow-Methods" value="GET,POST,PUT,DELETE" />`

Other options are as follows:

```
<add name="Access-Control-Allow-Methods" value="GET,
HEAD,POST,PUT,DELETE,CONNECT,OPTIONS,TRACE,PATCH" />
```

Access-Control-Allow-Origin

The Access-Control-Allow-Origin response header indicates whether the response can be shared with resources with the given origin.

```
<add name="Access-Control-Allow-Origin" value="http://<hostname>" />
```

```
<add name="Access-Control-Allow-Origin" value="*" />
```

Content-Security-Policy

A Content Security Policy (CSP) requires careful tuning and precise definition of the policy. If enabled, CSP has significant impact on the way browsers render pages (for example, inline JavaScript disabled by default and must be explicitly allowed in policy). CSP prevents a wide range of attacks, including cross-site scripting and other cross-site injections.

Directive	Description
default-src	Define loading policy for all resources type in case of a resource type dedicated directive is not defined (fallback).
script-src	Define which scripts the protected resource can execute.
object-src	Define from where the protected resource can load plugins.
style-src	Define which styles (CSS) the user applies to the protected resource.
img-src	Define from where the protected resource can load images.
media-src	Define from where the protected resource can load video and audio.
frame-src	Define from where the protected resource can embed frames.
font-src	Define from where the protected resource can load fonts.
connect-src	Define which URIs the protected resource can load using script interfaces.
form-action	Define which URIs can be used as the action of HTML form elements.
sandbox	Specifies an HTML sandbox policy that the user agent applies to the protected resource.
script-nonce	Define script execution by requiring the presence of the specified nonce on script elements.
plugin-types	Define the set of plugins that can be invoked by the protected resource by limiting the types of resources that can be embedded.
reflected-xss	Instructs a user agent to activate or deactivate any heuristics used to filter or block reflected cross-site scripting attacks, equivalent to the effects of the non-standard X-XSS-Protection header.
report-uri	Specifies a URI to which the user agent sends reports about policy violation.

For example, <add name="Content-Security-Policy" value="default-src http://localhost 'unsafe-inline' 'unsafe-eval' ; style-src http://localhost 'unsafe-inline' ; script-src http://localhost 'unsafe-inline' 'unsafe-eval'" />

HTTP Strict Transport Security

HTTP Strict Transport Security (HSTS) is a web security policy mechanism which helps to protect websites against protocol downgrade attacks and cookie hijacking. It allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections, and never via the insecure HTTP protocol. HSTS is an IETF standards track protocol and is specified in RFC 6797. A server implements an HSTS policy by supplying a header (Strict-Transport-Security) over an HTTPS connection.

Note: HSTS headers over HTTP are ignored.

Value	Description
max-age=SECONDS	The time, in seconds, that the browser should remember that this site is only to be accessed using HTTPS.
includeSubDomains	If this optional parameter is specified, this rule applies to the subdomains of all the site as well.

For example, all present and future subdomains will be HTTPS for a max-age of 1 year. This blocks access to pages or sub domains that can only be served over HTTP.

<add name="Strict-Transport-Security" value="max-age=31536000; includeSubDomains"/>

Referrer-Policy

The Referrer-Policy HTTP header governs the referrer information sent in the Referrer header that should be included with requests made.

Value	Description
no-referrer	The simplest policy is "no-referrer", which specifies that no referrer information is to be sent along with requests made from a particular request client to any origin. The header will be omitted entirely.
no-referrer-when-downgrade	The "no-referrer-when-downgrade" policy sends a full URL along with requests from a TLS-protected environment settings object to a potentially trustworthy URL, and requests from clients which are not TLS-protected to any origin. Requests from TLS-protected clients to non- potentially trustworthy URLs, on the other hand, will contain no referrer information. A Referrer HTTP header will not be sent.
same-origin	The "same-origin" policy specifies that a full URL, stripped for use as a referrer, is sent as referrer information when making same-origin requests from a particular client.Cross-origin requests, on the other hand, will

Value	Description
	contain no referrer information. A Referrer HTTP header will not be sent.
origin-when-cross-origin	The "origin-when-cross-origin" policy specifies that a full URL, stripped for use as a referrer, is sent as referrer information when making same-origin requests from a particular request client, and only the ASCII serialization of the origin of the request client is sent as referrer information when making cross-origin requests from a particular client.
strict-origin-when-cross-origin	The "strict-origin-when-cross-origin" policy specifies that a full URL, stripped for use as a referrer, is sent as referrer information when making same-origin requests from a particular request client, and only the ASCII serialization of the origin of the request client when making cross-origin requests: - From a TLS-protected environment settings object to a potentially trustworthy URL, and - From non-TLS-protected environment settings objects to any origin. Requests from TLS-protected clients to non- potentially trustworthy URLs, on the other hand, will contain no referrer information. A Referrer HTTP header will not be sent.
unsafe-url	The "unsafe-url" policy specifies that a full URL, stripped for use as a referrer, is sent along with both cross-origin requests and same-origin requests made from a particular client.

For example, <add name="Referrer-Policy" value="same-origin" />

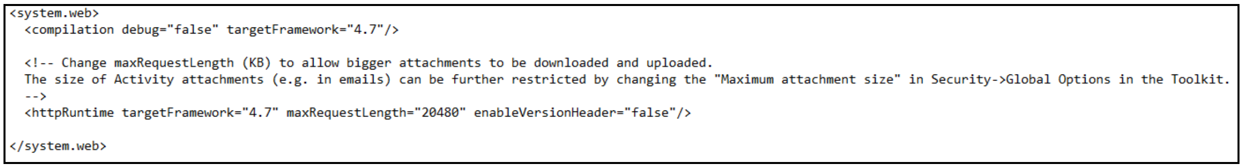
A

Troubleshooting

Large Attachments for a Task on Pivotal UX Client

In Pivotal UX Client, if a large file cannot be attached to a task, perform the following steps:

1. Navigate to the `..\Program Files (x86)\Aptean\Pivotal CRM\UX Client\www` folder and open `Web.config` file.
2. In the `Web.config` file, locate the `<system.web>` tag. Change the `maxRequestLength` value to the new maximum size required, in KB.



```
<system.web>
  <compilation debug="false" targetFramework="4.7"/>

  <!-- Change maxRequestLength (KB) to allow bigger attachments to be downloaded and uploaded.
  The size of Activity attachments (e.g. in emails) can be further restricted by changing the "Maximum attachment size" in Security->Global Options in the Toolkit.
  -->
  <httpRuntime targetFramework="4.7" maxRequestLength="20480" enableVersionHeader="false"/>

</system.web>
```

3. Save the `Web.config`, restart IIS, and restart PBS.

Note: For further troubleshooting cases, refer to Pivotal UX 6.6.1 Technical Reference Guide.