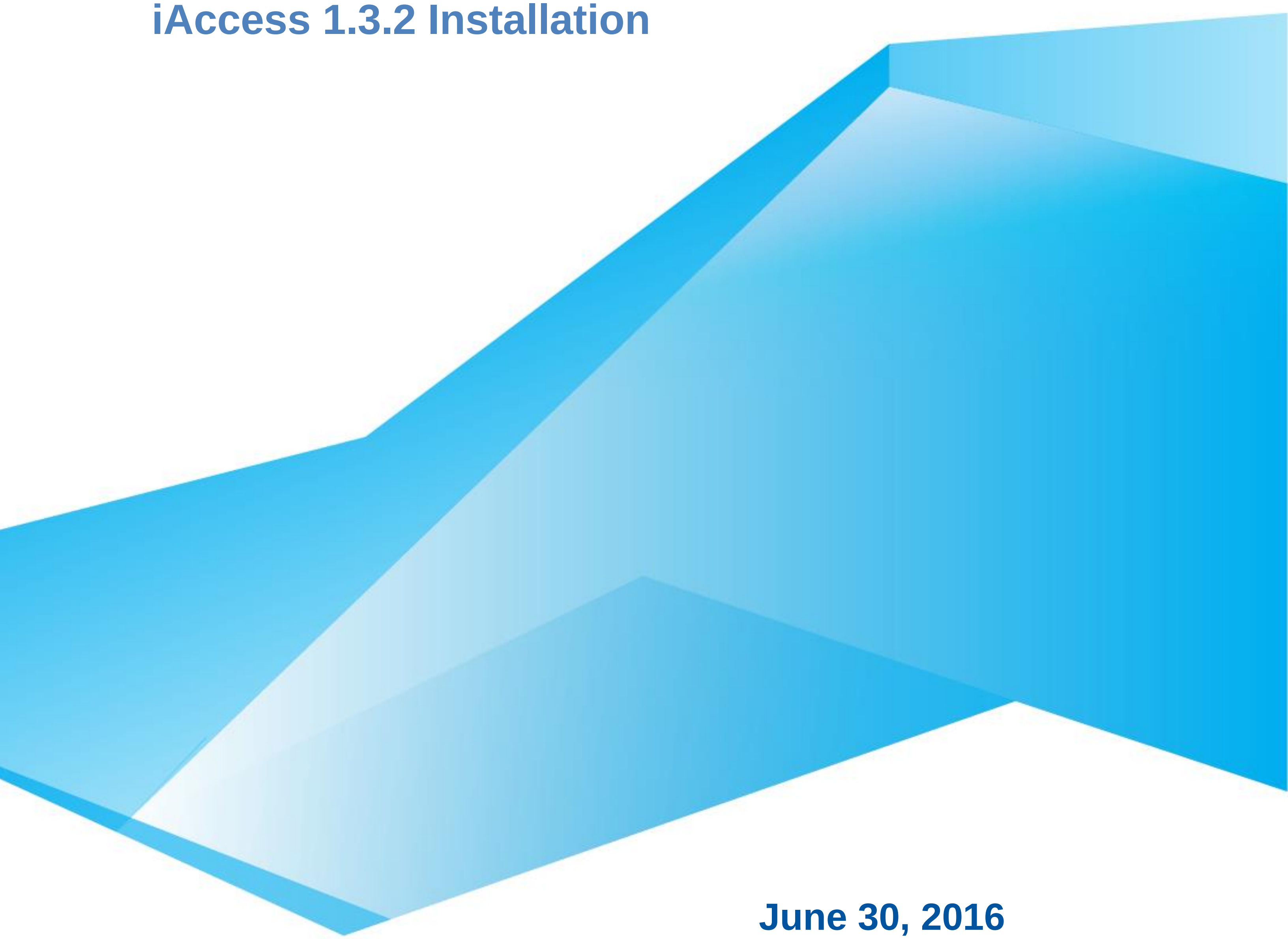
Deltek Know more. Do more.™

Deltek Maconomy®

iAccess 1.3.2 Installation



June 30, 2016

While Deltek has attempted to verify that the information in this document is accurate and complete, some typographical or technical errors may exist. The recipient of this document is solely responsible for all decisions relating to or use of the information provided herein.

The information contained in this publication is effective as of the publication date below and is subject to change without notice.

This edition published June 2016.

Contents

Overview ... 1

Prerequisites ... 1

MConfig Installation ... 3

MConfig Installation ... 3

Create a Website Using Apache ... 6

Download Apache ... 6

Enable Compression ... 7

Set Up Virtual Host ... 7

Verify the Setup ... 11

Create a Website Using IIS ... 12

Enable IIS Support Automatically Using MConfig ... 12

Enable IIS Support Manually Using IIS Manager ... 12

Add the Site ... 12

Add MIME Types ... 13

Configure Proxy Setup ... 13

Preserve the Host Header ... 18

Set Up HTTPS ... 19

Domain Login and Single Sign On ... 21

Browser Setup for Single Sign On ... 21

Domain Controller Setup ... 23

Maconomy Server Setup ... 24

Additional Related Procedures ... 25

Configure Web Server to Reduce Risk of Clickjacking ... 25

Downloading Deltek Products using the Deltek Software Manager ... 25

Adding Custom Notes to This Guide ... 27

Overview

Welcome to the Deltek iAccess Installation Guide. This guide leads you through the installation process, including prerequisites.

Installing iAccess for the first time is a two-step process. First, you install via MConfig, and second you set up websites, via Apache or IIS.

This document contains instructions for:

- Prerequisites and information you need to know before you begin
- MConfig Installation
- Creating a website using Apache

  or
- Creating a website using Internet Information Services (IIS)

Use of HTTPS/TLS

While Deltek offers no formal security recommendations, Deltek best practice recommends that you configure web servers to use HTTPS (instead of HTTP). Using HTTPS/TLS encrypts your network traffic, making it difficult for anyone to access the credentials as they are passed to the web server.

Use the Extension Manual to Complete Installation

To complete the installation, refer to the Deltek Maconomy iAccess 1.3.2 Extension Manual.

Prerequisites

The following are prerequisites to installing iAccess:

- Maconomy 2.2.3 or 2.3 LA installation
- MConfig 8.10 or later for 2.2.3, and MConfig 8.11 or later for 2.3 LA
- Extender 1.6
- RESTful Web Services is enabled in the Coupling Service
- iAccess downloaded from DSM, and iAccess FPU placed in the PUs folder (with the APU and TPU)
- If you are using Apache as the webserver, download the Apache binary package including OpenSSL, and install it from the following link:

  http://httpd.apache.org/

Additionally, this document assumes that you have already set up an application. For detailed instructions on setting up applications, see the *Deltek Maconomy 2.2.3 Installation Guide*, or the *Deltek Maconomy 2.3 LA Installation Guide*.

Address Risk of Clickjacking

To reduce the likelihood of clickjacking, Deltek suggests you follow the OWASP guidelines to defend against clickjacking attacks. Based on the OWASP guideline, you can perform additional steps when configuring your webserver. Details are provided in the Additional Related Procedures section of this document.

While Deltek recommends these procedures, ultimately each company is liable for its own security. The landscape evolves quickly, and each firm should continuously take internal measures to ensure its own security.

MConfig Installation

MConfig Installation

To begin installation with MConfig, complete the following steps:

1. Right-click the MConfig executable and select **Run as administrator**, and click through any informational prompts, accepting defaults.

   Make sure you are using the latest version of MConfig. If you try to perform installation with an older version, you will receive error messages.

2. In the Configure Global Parameters window, enter the path for the PUs, and click **OK**.
3. If any of the specified folders are new, you are prompted to approve their automatic creation. Accept the default selections on the prompts.

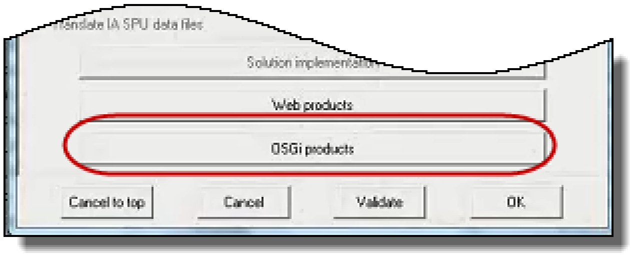
   Once the folders are accessed or created, MConfig opens automatically.

4. In the MConfig Main Window, double-click on the application to open.

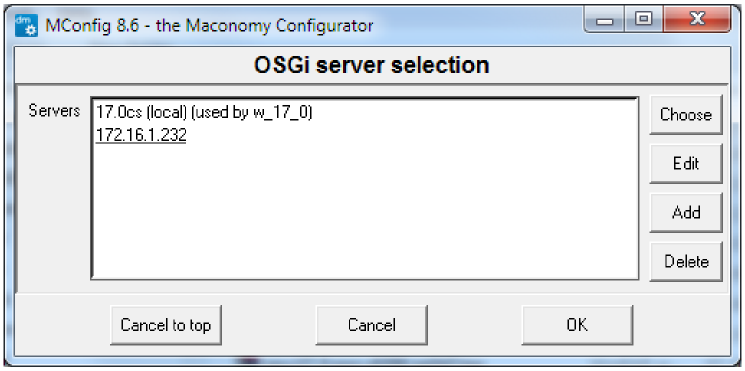
   The Application Instance window displays.

5. Click **OSGi products**.

   The OSGi Server Selection screen appears.



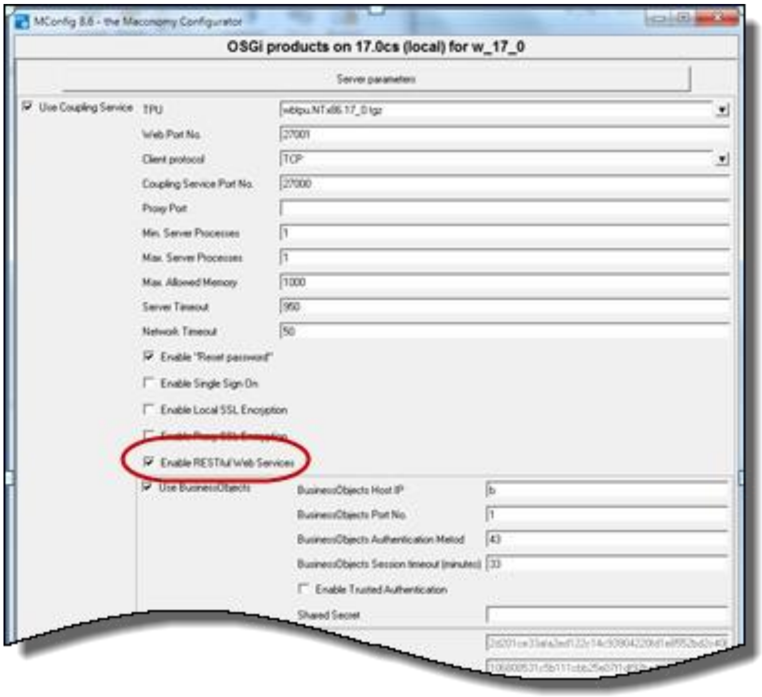
6. Select the Coupling Service to update.



OSGi server selection

Servers
17.0cs (local) (used by w_17_0)
172.16.1.232

7. Select the **Enable RESTful Web Services** check box.



MConfig 8.6 - the Maconomy Configurator

OSGi products on 17.0cs (local) for w_17_0

☑ Use Coupling Service

TPU	wbtpu.NT.x86.17_0.tgz
Web Port No.	27001
Client protocol	TCP
Coupling Service Port No.	27000
Proxy Port	
Min. Server Processes	1
Max. Server Processes	1
Max. Allowed Memory	1000
Server Timeout	950
Network Timeout	50

☑ Enable "Reset password"

☐ Enable Single Sign On

☐ Enable Local SSL Encryption

☐ Enable Proxy SSL Encryption

☑ Enable RESTful Web Services

☑ Use BusinessObjects

BusinessObjects Host IP	b
BusinessObjects Port No.	1
BusinessObjects Authentication Metod	43
BusinessObjects Session timeout (minutes)	33

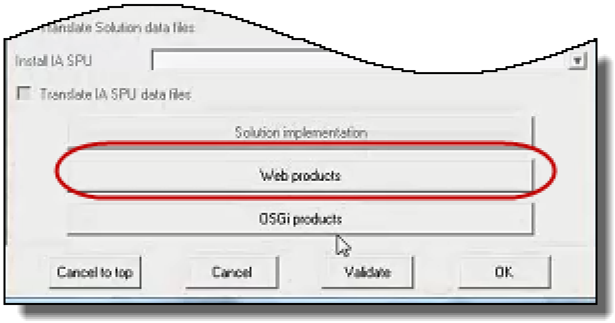
☐ Enable Trusted Authentication

Shared Secret	
	2d201ce33afa3ed122c14c93904220d1e8f55bd2c40
	106800531c5b111cbb25e071d9

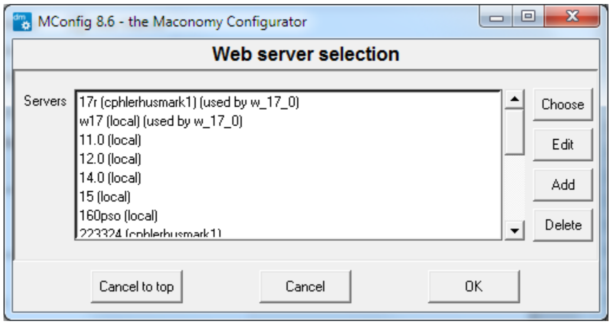
8. Click **OK** to save, and click **OK** at the SSL warning to return to the Application Instance window.

SSL setup is described here.

9. In the Application Instance window, click **Web products**.



10. On the **Web server selection** screen, select the application to update.

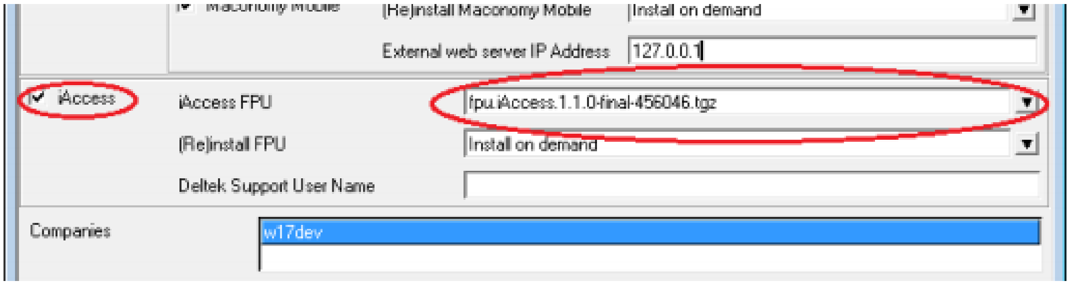


Servers

17r (cphlerhusmark1) (used by w_17_0)
w17 (local) (used by w_17_0)
11.0 (local)
12.0 (local)
14.0 (local)
15 (local)
160pso (local)
223324 (cphlerhusmark1)

The Web Products window displays.

11. Select the **iAccess** check box.



(Re)install Maconomy Mobile: Install on demand

External web server IP Address: 127.0.0.1

☑ iAccess

iAccess FPU: fpu.iAccess.1.1.0-final-456046.tgz

(Re)install FPU: Install on demand

Deltek Support User Name:

Companies: w17dev

12. In the **iAccess FPU** field, select the relevant FPU from the drop-down list.
13. In the **Deltek Support User Name** field, enter a user name.

    This enables the online help.
14. Click **OK**, **OK**, and **OK** to accept the changes and return to the main screen.
15. Click **Next**, **Next**, and **Yes** to complete the installation.

    MConfig will request the password for the Deltek Support user name you entered.

When you change your Deltek Support account password (which expires every three months), you also have to update it in MConfig.

The MConfig part of the installation is complete. Next, create the website using Apache or IIS.

Create a Website Using Apache

If you are using Apache as your webserver, complete the steps in this section.

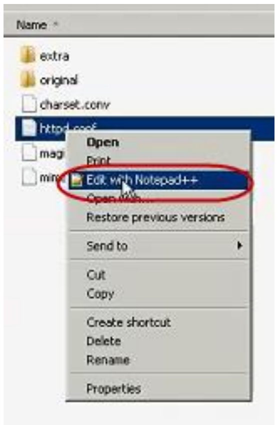
You need to:

- Download Apache
- Enable compression
- Set up virtual host
- Verify the SSL setup

Download Apache

To download and set up Apache, complete the following steps:

1. Download the Apache 2.2 binary package (including OpenSSL).
2. Install the package.
3. Open Apache.
4. Navigate to **Program Files » Apache Software Foundation » Apache [version] » conf » httpd.conf**.
5. Right-click, then click **Edit with Notepad**.



6. In **httpd.conf**, comment in the following modules:

```
LoadModule headers_module modules/mod_headers.so
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule ssl_module modules/mod_ssl.so
```

7. Comment in the following inclusion:

```
Include conf/extra/httpd-vhosts.conf
```

8. Comment out `#Listen 80`, as you will use the `httpd-vhosts.conf` file instead.

Enable Compression

To enable compression, complete the following steps:

1. In **httpd.conf**, comment in the following module:

   ```
   LoadModule deflate_module modules/mod_deflate.so
   ```

2. Configure compression as follows:

   ```
   <IfModule deflate_module>
      AddOutputFilterByType DEFLATE text/html text/plain text/xml text/css
   text/javascript application/javascript
      SetOutputFilter DEFLATE
      DeflateCompressionLevel 5
    </IfModule>
   ```

For more information, refer to the Apache Deflation Module (https://httpd.apache.org/docs/2.2/mod/mod_deflate.html).

Set Up Virtual Host

You must set up a virtual host to serve iAccess. If your company already uses a dedicated hardware component with an encrypted line, choose to setup without SSL. If your company does not have dedicated hardware and an encrypted line, use the instructions for setting up with SSL.

Setup without SSL

The following is a template for setting up a virtual host that serves iAccess ***without*** SSL.

To set up a virtual host without SSL, complete the following steps:

1. Open **httpd-vhosts.conf**, and then right-click to edit in Notepad.
2. Copy the template below, and paste it into the file.
3. Replace the variables as follows:
   - Replace **<server-name>** with the host name.
   - Replace **<port>** with the port number.
   - Replace **<iAccess-installation-directory>** with the path to the folder containing iAccess's index.html file, such as **C:/Maconomy/Webservers/ace17/app**.

The following is the template to copy (variables are flagged):

```
Listen <port>
<VirtualHost *:<port>>
    ServerName <server-name>

    # Server iAccess files from installation directory
    DocumentRoot "<iAccess-installation-directory>"
```

```
    <Directory <iAccess-installation-directory>>
       Order deny,allow
       Allow from all
    </Directory>

    <Proxy *>
       Order deny,allow
       Allow from all
    </Proxy>

    ProxyRequests      Off
    ProxyPreserveHost  On

    # Proxy the web services from the coupling service
    ProxyPass  /containers               http://<coupling-service-
host>:<coupling-service-web-port>/containers              retry=0
    ProxyPass  /filedrop                 http://<coupling-service-
host>:<coupling-service-web-port>/filedrop                retry=0
    ProxyPass  /configurations           http://<coupling-service-
host>:<coupling-service-web-port>/configurations          retry=0
</VirtualHost>
```

The following is an example of the template with the variables replaced:

```
Listen 8090
<VirtualHost *:8090>
    ServerName techwebproject

    # Server iAccess files from installation directory
    DocumentRoot "C:/Maconomy/Webservers/ace17/app"

    <Directory C:/Maconomy/Webservers/ace17/app>
       Order deny,allow
       Allow from all
    </Directory>

    <Proxy *>
       Order deny,allow
       Allow from all
    </Proxy>

    ProxyRequests      Off
    ProxyPreserveHost  On

    # Proxy the web services from the coupling service
    ProxyPass  /containers     http://localhost:8085/containers     retry=0
    ProxyPass  /filedrop       http://localhost:8085/filedrop       retry=0
    ProxyPass  /configurations           http://localhost:8085/configurations
retry=0
```

```
</VirtualHost>
```

Setup with SSL

The following is a template for setting up a virtual host that serves iAccess ***with*** SSL.

To set up a virtual host with SSL, complete the following steps:

1. Open a **httpd-vhosts.conf** file, and then right-click to edit in Notepad.
2. Copy the template below, and paste it into the file.
3. Replace the variables as follows:
    - Replace **<server-name>** with the host name.
    - Replace **<port>** with the port number.
    - Replace **<iAccess-installation-directory>** with the path to the folder containing iAccess's index.html file, such as **C:/Maconomy/Webservers/ace17/app.**

The following is the template to copy (variables are flagged):

```
Listen <port>
<VirtualHost *:<port>>
    ServerName <server-name>

    # Server iAccess files from installation directory
    DocumentRoot "<iAccess-installation-directory>"

    <Directory <iAccess-installation-directory>>
       Order deny,allow
       Allow from all
    </Directory>

    <Proxy *>
       Order deny,allow
       Allow from all
    </Proxy>

    ProxyRequests      Off
    ProxyPreserveHost  On
    # Signal to the coupling service that the originating protocol is HTTPS
    RequestHeader set X-Forwarded-Proto "https"

    # Proxy the web services from the coupling service
    ProxyPass  /containers               http://<coupling-service-host>:<coupling-service-web-port>/containers              retry=0
    ProxyPass  /filedrop                 http://<coupling-service-host>:<coupling-service-web-port>/filedrop                retry=0
    ProxyPass  /configurations           http://<coupling-service-host>:<coupling-service-web-port>/configurations          retry=0
    # Set up this virtual host to use SSL
    SSLEngine              On
    SSLProxyEngine         On
    SSLCertificateFile     <crt-file-location>
    SSLCertificateKeyFile  <key-file-location>
</VirtualHost>
```

The following is an example of the template with the variables replaced:

```
Listen 443
<VirtualHost *:443>
    ServerName techwebproject

    # Server iAccess files from installation directory
    DocumentRoot "C:/Maconomy/Webservers/ace17/app"

    <Directory C:/Maconomy/Webservers/ace17/app>
       Order deny,allow
       Allow from all
    </Directory>

    <Proxy *>
       Order deny,allow
       Allow from all
    </Proxy>

    ProxyRequests      Off
    ProxyPreserveHost  On
    # Signal to the coupling service that the originating protocol is HTTPS
    RequestHeader set X-Forwarded-Proto "https"

    # Proxy the web services from the coupling service
    ProxyPass  /containers    http://localhost:8085/containers       retry=0
    ProxyPass  /filedrop      http://localhost:8085/filedrop         retry=0
    ProxyPass  /configurations           http://localhost:8085/configurations
retry=0

    # Set up this virtual host to use SSL
    SSLEngine              On
    SSLProxyEngine         On
    SSLCertificateFile     c:/sslkeys/server.crt
    SSLCertificateKeyFile  c:/sslkeys/server.key
</VirtualHost>
```

Verify the Setup

Verify the setup by executing a cURL command that makes a web service call.

For example:

```
curl -k -u'Administrator:123456'
https://techwebproject/containers/v1/w17pso2/timesheets
```

where

- Username is `Administrator`
- Password is `123456`
- Shortname is `w17pso2`

Create a Website Using IIS

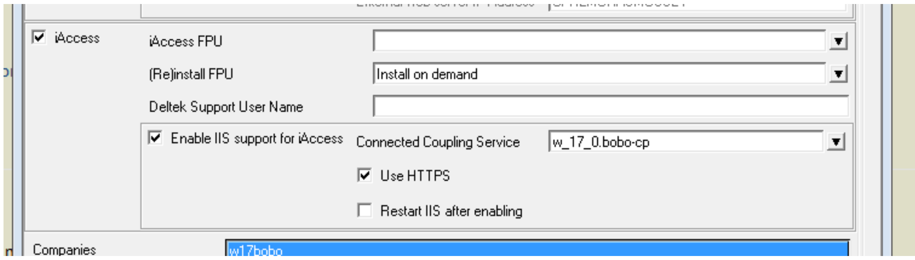
To create a website using IIS, you can enable IIS support automatically using MConfig, or perform the steps manually using IIS Manager.

Enabling IIS support with MConfig automatically completes the steps described under the manual installation. Use MConfig for the initial setup of an iAccess website using IIS. However, modifying the setup later should be done manually using IIS Manager.

Enable IIS Support Automatically Using MConfig

To enable IIS support using MConfig, follow these steps:

1. In MConfig, go to the Web Products window.
2. Select the **Enable IIS support for iAccess** check box and click **OK**.



☑ iAccess

iAccess FPU

(Re)install FPU: Install on demand

Deltek Support User Name

☑ Enable IIS support for iAccess

Connected Coupling Service: w_17_0.bobo-cp

☑ Use HTTPS

□ Restart IIS after enabling

Companies: w17bobo

After you complete the initial installation with MConfig, you should check the setup in IIS Manager and possibly modify parameters, such as Web Server Port Number.

Enable IIS Support Manually Using IIS Manager

To enable IIS support manually using IIS Manager, complete the steps in this section.

You need to:

- Add the site
- Add MIME types
- Configure proxy setup
- Preserve the host header
- Set up HTTPS

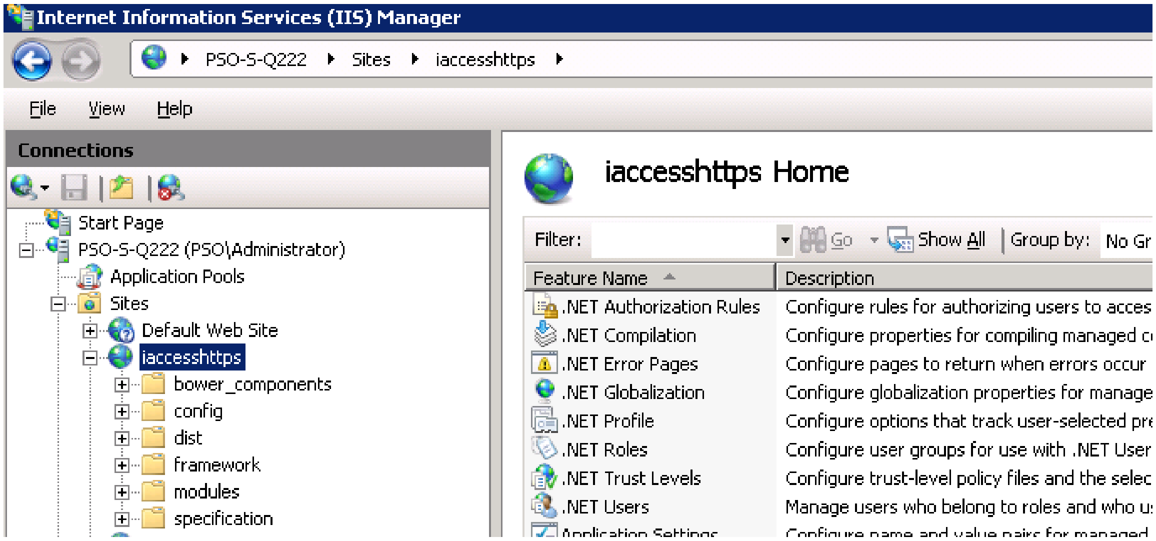
It is not possible to run both HTTP and HTTPS on the same IIS site.

Add the Site

To add the site, complete the following steps:

1. Connect to your server in the IIS Manager application.
2. Set up the site.

   The site should have the files shown in the following screenshot as root files.



Feature Name	Description
.NET Authorization Rules	Configure rules for authorizing users to acces
.NET Compilation	Configure properties for compiling managed c
.NET Error Pages	Configure pages to return when errors occur
.NET Globalization	Configure globalization properties for manage
.NET Profile	Configure options that track user-selected pre
.NET Roles	Configure user groups for use with .NET User
.NET Trust Levels	Configure trust-level policy files and the selec
.NET Users	Manage users who belong to roles and who u
Application Settings	Configure name and value pairs for managed

Add MIME Types

To add MIME types, complete the following steps:

1. Click **MIME Types**.
2. Add the following rows to the table:

```
.json application/json

.woff application/font-woff
```

In IIS 8.0 and 8.5, the .woff extension exists by default but with a different type. Change it to `application/font-woff`.

Configure Proxy Setup

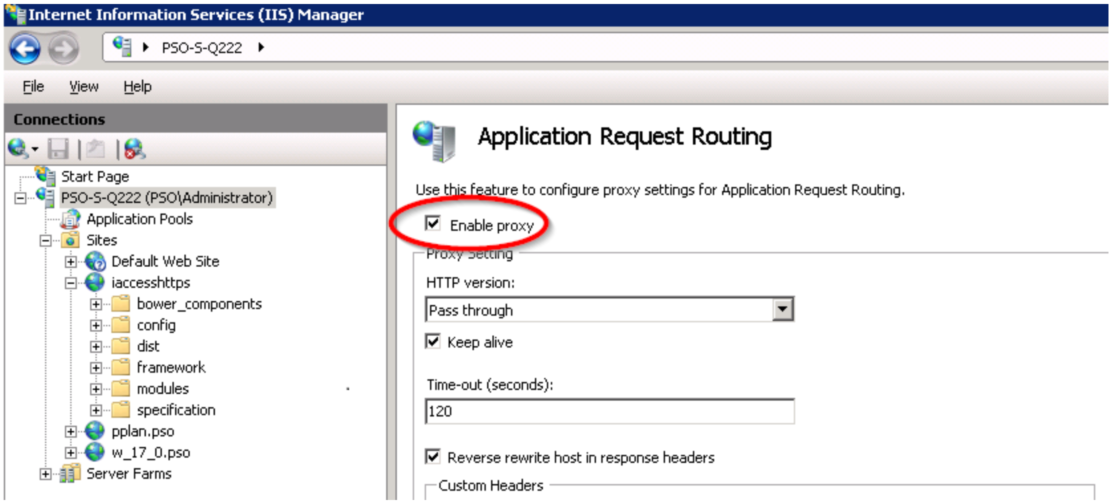
To configure proxy setup, complete the following steps:

1. To install Application Request Routing (ARR), click the following link:

   http://www.microsoft.com/en-us/download/details.aspx?id=39715

   In IIS 8.0 and 8.5, you need to install the “Web Platform Installer” before you can install the ARR plugin.

2. Restart IIS Manager.
3. In the “Application Request Routing” configuration window, click **Server Proxy Settings**.
4. Select **Enable proxy**.



Application Request Routing

Use this feature to configure proxy settings for Application Request Routing.

☑ Enable proxy

Proxy Setting

HTTP version: Pass through

☑ Keep alive

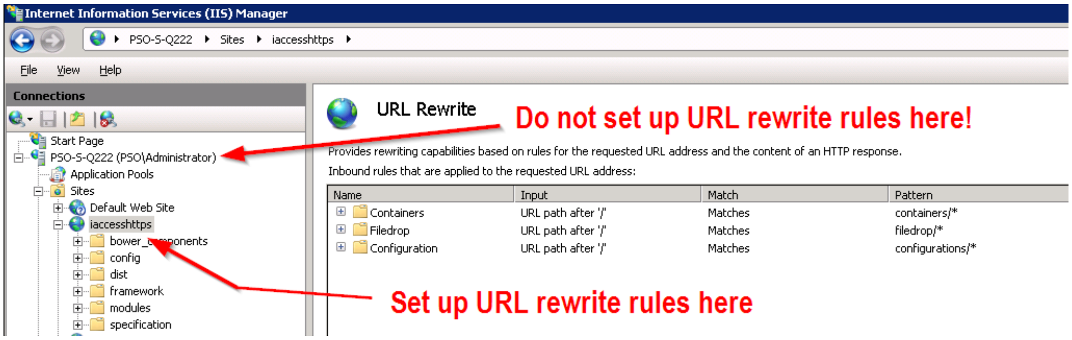
Time-out (seconds): 120

☑ Reverse rewrite host in response headers

Custom Headers

5. To add proxy rules for the container and filedrop APIs, click **URL Rewrite** and then **Add Rules**.

This must be done on the local site, not globally. Refer to the following screenshot:



URL Rewrite

Do not set up URL rewrite rules here!

Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern
Containers	URL path after '/'	Matches	containers/*
Filedrop	URL path after '/'	Matches	filedrop/*
Configuration	URL path after '/'	Matches	configurations/*

Set up URL rewrite rules here

Add Rules to Container API

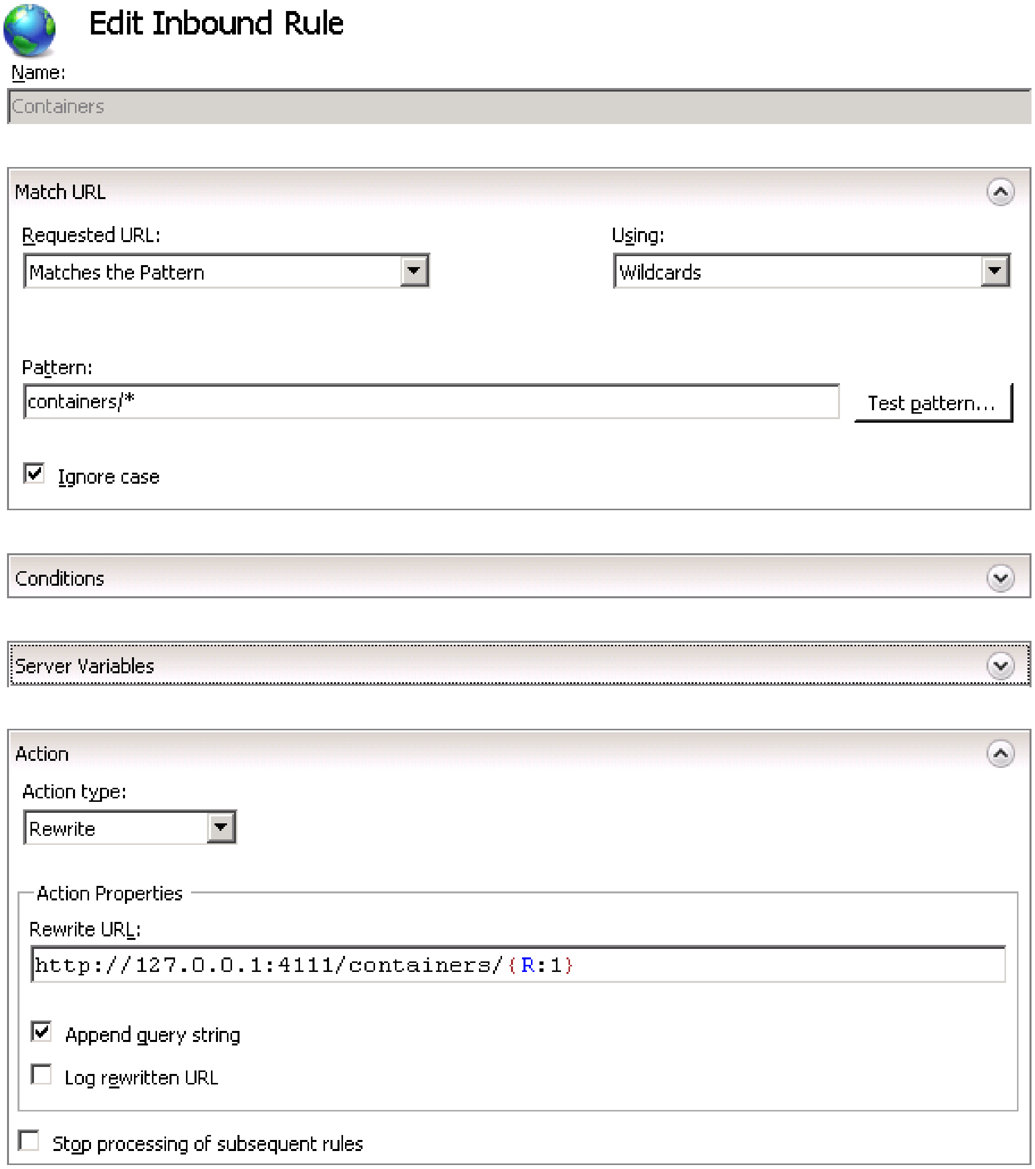
To add rules to Container API, complete the following steps:

1. Click **Add Rule...**.
2. Select a blank rule.

   The Edit Inbound Rule screen displays.
3. Complete the following fields:
   - **Requested URL** — Select **Matches the Pattern**.
   - **Using** — Select **Wildcards**.
   - **Pattern** — Select **containers/***.
   - **Unchecked** — Ignore case.
   - **Action Type** — Select **Rewrite**.
   - **Rewrite URL** — Enter the URL for the RESTful API.

Make sure to choose the Coupling Service webport (for example, 8081 in the following screenshot). The host should be the ip or hostname of the coupling service, not necessarily 127.0.0.1.

- **Append query string** — Select this check box.



Edit Inbound Rule

Name: Containers

Match URL

Requested URL: Matches the Pattern

Using: Wildcards

Pattern: containers/*

☑ Ignore case

Action

Action type: Rewrite

Action Properties

Rewrite URL: http://127.0.0.1:4111/containers/{R:1}

☑ Append query string

□ Log rewritten URL

□ Stop processing of subsequent rules

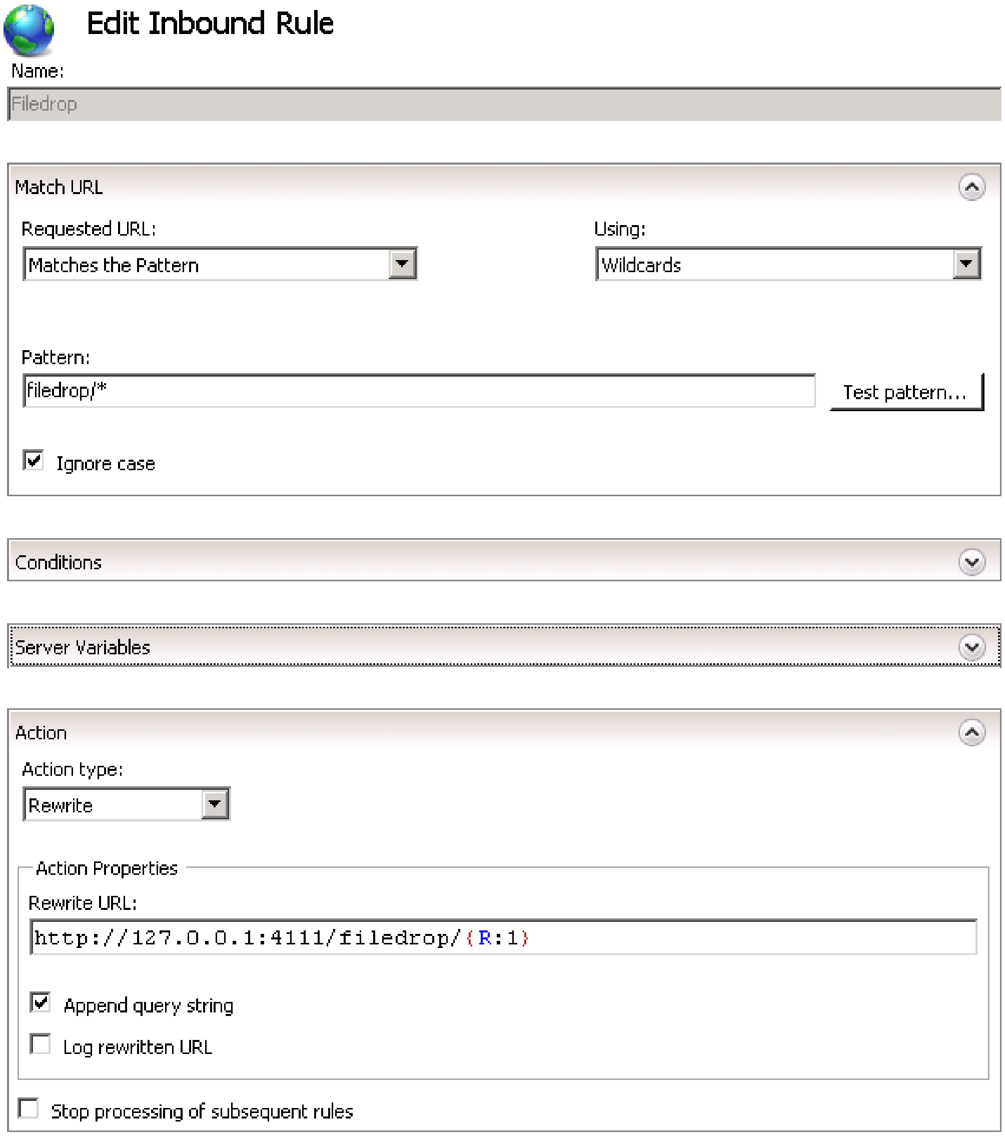
Add Rules to Filedrop API

To add rules to Filedrop API, complete the following steps:

1. Click **Add Rule...**.
2. Select a blank rule.

   The Edit Inbound Rule screen displays.
3. Complete the following fields:

- **Requested URL** — Select **Matches the Pattern**.
- **Using** — Select **Wildcards**.
- **Pattern** — Select **filedrop/***.
- **Ignore case** — Select this check box.
- **Action Type** — Select **Rewrite**.
- **Rewrite URL** — Enter the URL for the RESTful API.
- **Append query string** — Select this check box.



Edit Inbound Rule

Name: Filedrop

Match URL

Requested URL: Matches the Pattern

Using: Wildcards

Pattern: filedrop/*

☑ Ignore case

Action

Action type: Rewrite

Action Properties

Rewrite URL: http://127.0.0.1:4111/filedrop/{R:1}

☑ Append query string

☐ Log rewritten URL

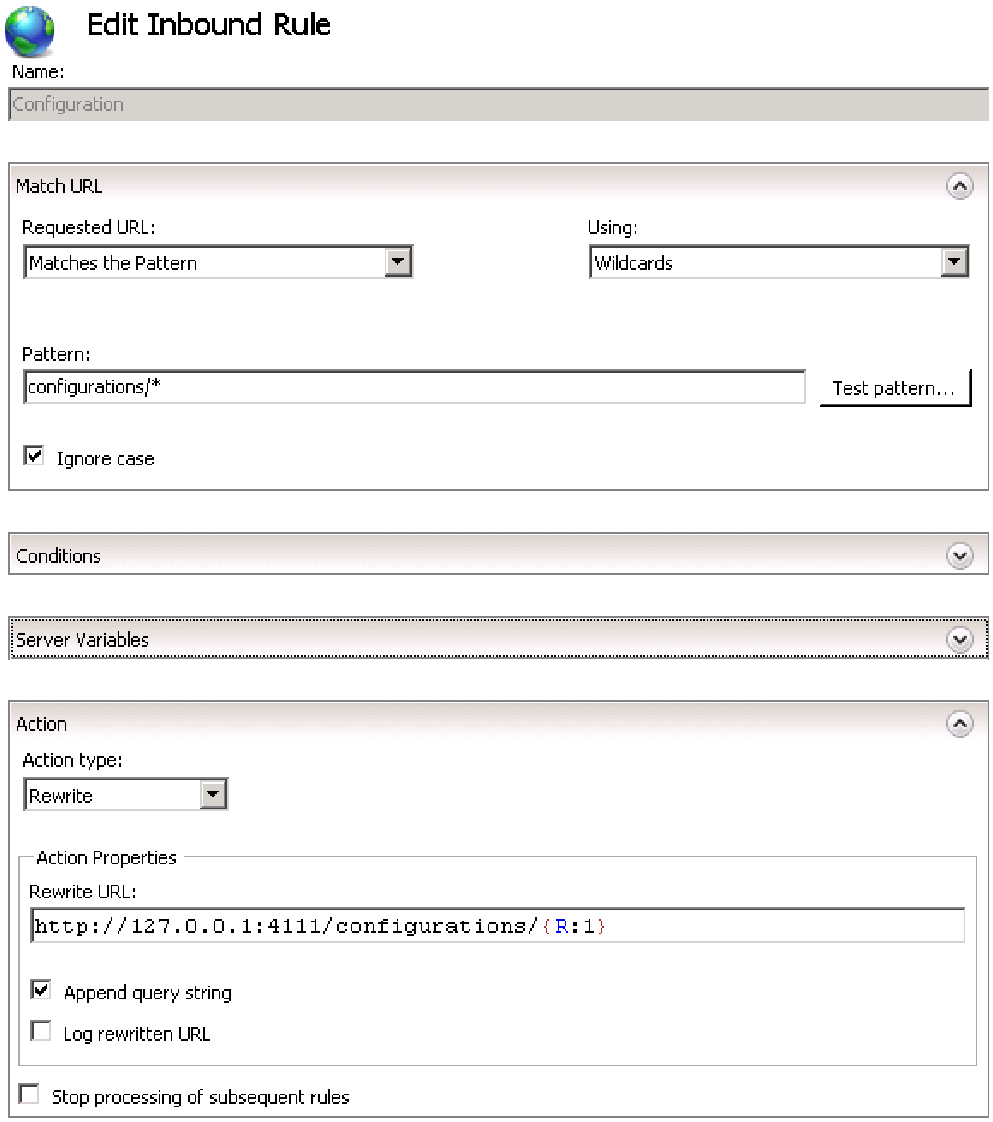
☐ Stop processing of subsequent rules

Add Rules to Configurations API

To add rules to Configurations API, complete the following steps:

1. Click **Add Rule**.
2. Select a blank rule.

   The Edit Inbound Rule screen displays.
3. Complete the following fields:
   - **Requested URL** — Select **Matches the Pattern**.
   - **Using** — Select **Wildcards**.
   - **Pattern** — Select **configurations/***.
   - **Ignore case** — Select this check box.
   - **Action Type** — Select **Rewrite**.
   - **Rewrite URL** — Enter the URL for the RESTful API.
   - **Append query string** — Select this check box.



Edit Inbound Rule

Name:
Configuration

Match URL

Requested URL: Matches the Pattern

Using: Wildcards

Pattern:
configurations/*

☑ Ignore case

Action

Action type: Rewrite

Action Properties

Rewrite URL:
```
http://127.0.0.1:4111/configurations/{R:1}
```

☑ Append query string

□ Log rewritten URL

□ Stop processing of subsequent rules

Preserve the Host Header

To preserve the host header, complete the following steps:

1. Open a console with Administrative privileges, and navigate to **C:\Windows\System 32\inetsrv**.
2. To enable **preserverHostHeader**, run the following command:

   ```
   cd C:\Windows\System32\inetsrv
   appcmd.exe set config -section:system.webServer/proxy
   /preserveHostHeader:"True" /commit:apphost
   ```

   To preserve the spacing, copy the command and paste it in the command prompt.

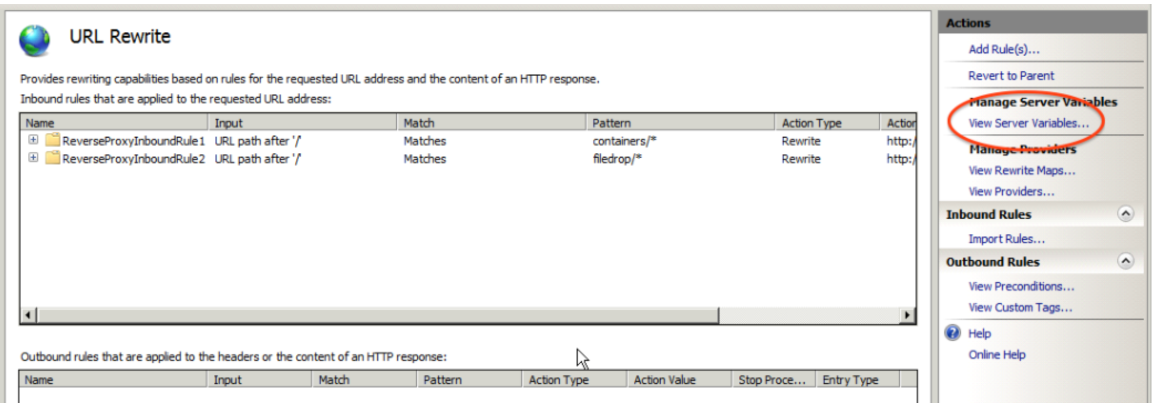
3. Restart the webserver.

Set Up HTTPS

To set up HTTPS, complete the following steps:

1. In the URL Rewrite screen, click **View Server Variables...**.

   The Server Variables screen displays.



URL Rewrite

Provides rewriting capabilities based on rules for the requested URL address and the content of an HTTP response.

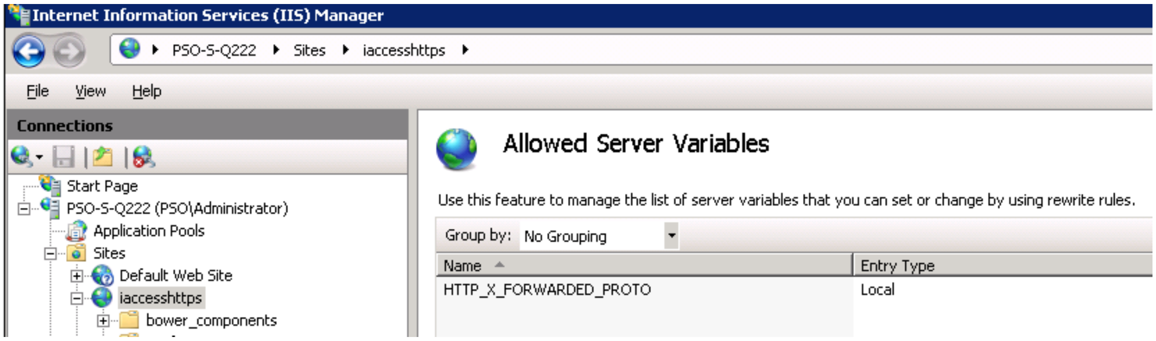
Inbound rules that are applied to the requested URL address:

Name	Input	Match	Pattern	Action Type	Actior
ReverseProxyInboundRule1	URL path after '/'	Matches	containers/*	Rewrite	http:/
ReverseProxyInboundRule2	URL path after '/'	Matches	filedrop/*	Rewrite	http:/

Outbound rules that are applied to the headers or the content of an HTTP response:

Name	Input	Match	Pattern	Action Type	Action Value	Stop Proce...	Entry Type

2. In the Server Variables screen, click **Add...** then add the variable **HTTP_X_FORWARDED_PROTO**.



Internet Information Services (IIS) Manager
PSO-S-Q222 ▸ Sites ▸ iaccesshttps ▸
File
View
Help
Connections
Start Page
PSO-S-Q222 (PSO\Administrator)
Application Pools
Sites
Default Web Site
iaccesshttps
bower_components

Allowed Server Variables

Use this feature to manage the list of server variables that you can set or change by using rewrite rules.

Group by: No Grouping

Name	Entry Type
HTTP_X_FORWARDED_PROTO	Local

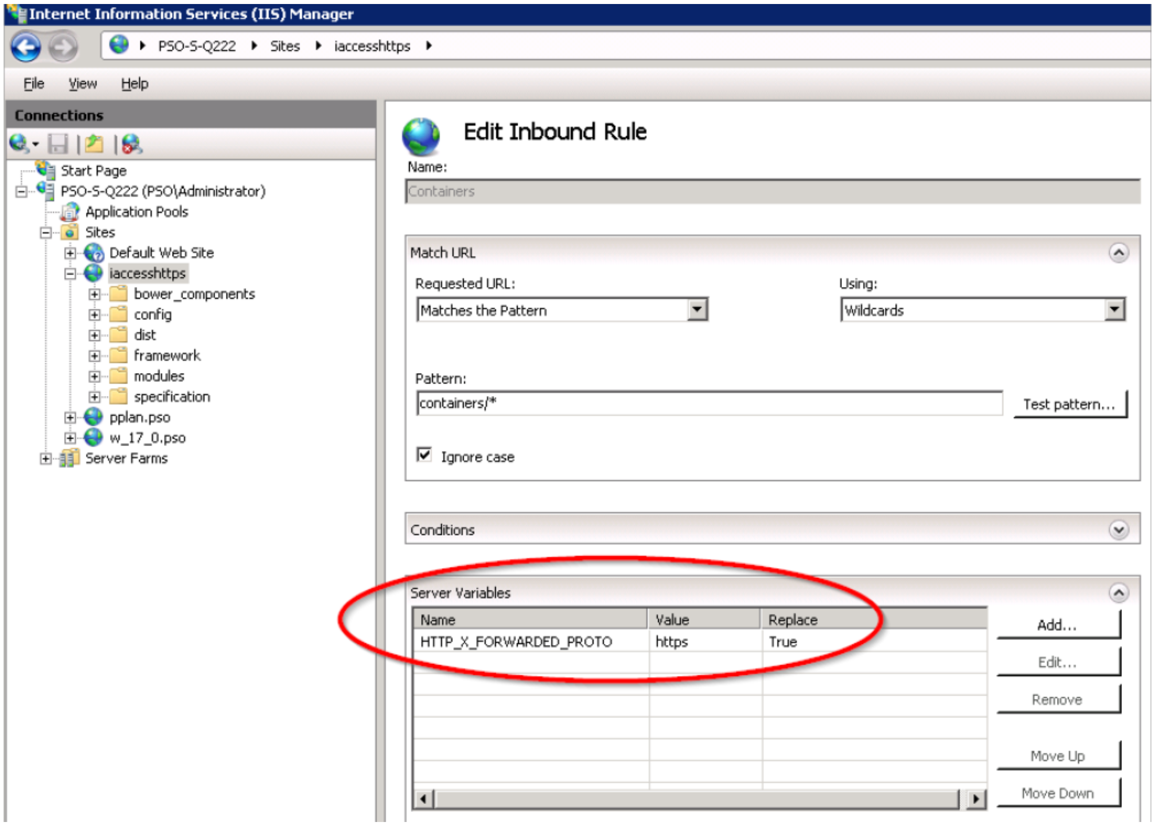
3. In the URL Rewrite Rules (for all endpoints) that proxy the web service, set the server variable

   from

   HTTP_X_FORWARDED_PROTO

   to

   https



Edit Inbound Rule

Name: Containers

Match URL

Requested URL: Matches the Pattern

Using: Wildcards

Pattern: containers/*

☑ Ignore case

Server Variables

Name	Value	Replace
HTTP_X_FORWARDED_PROTO	https	True

4. Restart the webserver.

   The webserver configuration is complete.

Beginning with release 1.3, usage tracking with Google Analytics is available in iAccess. Enabling/disabling this enhancement is divided into three parts, the first two of which have to be configured during installation. The third part can be configured during installation, or at a later stage. Refer to the Deltek Maconomy iAccess 1.3.2 Extension Manual for details.

Domain Login and Single Sign On

The domain login functionality in iAccess is based on Kerberos service tickets obtained through the SPNEGO authentication protocol. This protocol allows for direct Single Sign On (SSO) when the user is running iAccess while already authenticated against the domain (meaning, logged in to their computer via a domain account).

If the user is not authenticated against the domain, the browser typically prompts for domain credentials. Click **Cancel** in the browser login window and use the iAccess domain login page.

Browser Setup for Single Sign On

Refer to the instructions in this section to set up Single Sign On (SSO) for various browsers.

SSO Setup for Internet Explorer

For Internet Explorer (IE), you may need to add the iAccess server address to the Local intranet zone if it is not already in this zone, as IE does not permit Kerberos-based SSO for websites in the Internet zone.

More details are available in this Microsoft article on security zones in Internet Explorer:

https://support.microsoft.com/en-us/kb/174360

SSO Setup for Chrome

Follow the steps in the guide “Set Chrome policies for devices” (link below) to configure Chrome to work with SSO using Kerberos authentication.

https://support.google.com/chrome/a/answer/187202?hl=en

The configurations should be done by IT administrators who want to set Chrome policies on their corporate-managed devices. The templates contain hundreds of available policies that can be set, but you should only focus on two of these, namely:

AuthNegotiateDelegateWhitelist (http://www.chromium.org/administrators/policy-list-3#AuthNegotiateDelegateWhitelist**)**

and

AuthServerWhitelist (http://www.chromium.org/administrators/policy-list-3#AuthServerWhitelist).

The properties should be set to the domain you want to authenticate against, such as:

“*.example.com”.

SSO Setup for Chrome on Windows

After following the above guide from Google you can set **AuthNegotiateDelegateWhitelist** and **AuthServerWhitelist** in the following way**:**

1. Navigate to **Administrative Templates » Classic Administration Templates (ADM) » Google » Google Chrome » Policies for HTTP Authentication**.
2. Click “Kerberos delegation server whitelist".
3. Click **Enabled**.
4. In the **Input** field, enter the domain you want to authenticate against, such as “*.example.com”.
5. Click **Apply**.

6. Click on “Authentication server whitelist”.
7. Click **Enabled**.
8. In the input field, enter the domain you want to authenticate against, such as “*.example.com”.
9. Click **Apply**.
10. Open Chrome.
11. Check the values by navigating to the URL: chrome://policy

SSO Setup for Chrome on Mac

After following the preceding guide from Google you should also read the Mac Quick Start guide from Google at:

http://www.chromium.org/administrators/mac-quick-start

If the “Workgroup Manager from Apple” is not available for your version of OS X, then you can set **AuthNegotiateDelegateWhitelist** and **AuthServerWhitelist** in the following way**:**

1. Create **com.google.Chrome.plist** file with the following content:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
      <key>AuthNegotiateDelegateWhitelist</key>
      <string>*.example.com</string>
      <key>AuthNegotiateDelegateWhitelist</key>
      <string>*.example.com</string>
</dict>
</plist>
```

2. Set the two string attributes to the domain you want to authenticate against.
3. Convert the **com.google.Chrome.plist** to the binary format by running this command from the Terminal:

```
plutil -convert binary1 com.google.Chrome.plist
```

4. Copy the file to “/Library/Managed Preferences/“ by running this command from the Terminal:

```
sudo -s
cp com.google.Chrome.plist /Library/Managed Preferences/<username>
```

5. Open Chrome.
6. Check the values by navigating to the URL: chrome://policy

SSO Setup for Safari

No setup is needed.

SSO Setup for iOS

Follow the steps in this guide:

https://samuelyates.wordpress.com/2013/10/11/kerberos-single-sign-on-in-ios-7/

Remember to put your own servername on the URLPrefixMatches field. As the name implies, this has to contain a URL prefix. This could be "https://myserver.example.com:8080", so basically this will be set to the base server URL including an optional port number.

You can use Apple Configurator 2 to install the profile on a number of iPads:

https://itunes.apple.com/us/app/apple-configurator-2/id1037126344

Domain Controller Setup

The SPNEGO authentication protocol works by assuming the presence of a specific Service Principal Name (SPN) on the domain controller:

HTTP/*name*.*domain* or HTTP/*name*

where *name* and *domain* are the web server DSN name and domain respectively, as seen from the user's computer.

For example, if the user is opening iAccess using the internet address https://some-server.some-domain.com then the browser expects one of the following SPNs to be present on the domain controller: HTTP/*some-server* or HTTP/*some-server.some-domain.com*.

SPN Setup

It is a task for the domain administrator to ensure that these SPNs are created and associated with the existing domain account used for Maconomy SSO.

SSO with Active Directory

For Active Directory, associating SPNs with the existing domain account is done with the 'setspn' command.

To associate SPN with an existing domain account, complete the following step:

1. On a command line enter the following:

   setspn -A HTTP/*name account*

   setspn -A HTTP/*name*.*domain account*

   where *account* is the name of the domain account used for Maconomy SSO.

Special Instructions for SPN Conflicts

If iAccess is installed on a web server that already hosts other web applications with SNEGO authentication, this causes a conflict on the SPN, as an SPN can only be associated with one domain account.

To resolve the issue, either install only one web application on each web server, or create multiple local DNS names for the web server, so that each web application can be accessed through different addresses and will thereby map to different SPNs.

Maconomy Server Setup

Please refer to Single Sign On with Kerberos section in the *Deltek Maconomy System Administrator Guide.*

Additional Related Procedures

Configure Web Server to Reduce Risk of Clickjacking

You can reduce the risk of clickjacking by performing an additional step when configuring your web server. This step applies to both Apache and IIS.

To configure your web server and reduce the risk of clickjacking, complete the following step:

1. Configure your web server to always reply with the following response headers:
   - Content-Security-Policy: frame-ancestors ‘self’
   - X-Frame-Options: SAMEORIGIN

   These headers are then added to all responses.

Downloading Deltek Products using the Deltek Software Manager

You can use the Deltek Software Manager (DSM) to download complete Deltek products, hot fixes, and sub-releases. You can access DSM directly or through the Deltek Customer Care Connect site.

When you access DSM directly, you will be prompted to log on before you can access the application. If you access DSM from within the Deltek Customer Care site, you do not have to log on since you are already logged into the Customer Care site.

Accessing DSM Directly

To access Deltek Software Manager directly, complete the following steps:

1. Launch Deltek Software Manager by taking one of the following actions:
   - Click here.
   - On your desktop, click **Start » Programs » Deltek » Maconomy iAccess » Deltek Software Manager**.
2. In the Deltek Software Manager logon dialog box, enter your Deltek Customer Care **User ID** and **Password**, and click **Logon**.
3. To select the folder where you want to download Deltek products, click **Settings** above the right pane of Deltek Software Manager.

   When you log on for the first time, Deltek Software Manager asks you to select a default folder where Deltek products are to be downloaded.

4. Use the Settings dialog box to specify the folder where you want to download Deltek products, and click **OK**.

   You can change this folder anytime in the Settings dialog box.

5. In the left pane of Deltek Software Manager, expand the Deltek product that you want to download, if it is not already expanded.

   > If you clicked the link in step 1 to access DSM, the application automatically selects Maconomy iAccess for you.

6. Select the product type that you want to download. Your options are **Complete**, **HotFix**, and **Sub-Release**.
7. In the table, select the check box that corresponds to the Deltek product that you want to download. The right pane displays a message stating that the product has been added to the download queue.

   > To view the items in the download queue, click **View Download Queue** at the bottom of the left pane.

8. Click **Download** at the bottom of the left pane. Deltek Software Manager downloads the product to the folder that you selected.

Accessing DSM from within the Customer Care Connect Site

To access Deltek Software Manager from within the Customer Care Connect site, complete the following steps:

1. In your Web browser, go to http://support.deltek.com.
2. Enter your Customer Care Connect **Username** and **Password**, and click **Log In.**
3. When the Customer Care Connect site displays, click the Product Downloads tab.

   You are automatically logged into Deltek Software Manager.
4. To select the folder where you want to download Deltek products, click **Settings** above the right pane of Deltek Software Manager.

   > When you log on for the first time, Deltek Software Manager asks you to select a default folder where Deltek products are to be downloaded.

5. Use the Settings dialog box to specify the folder where you want to download Deltek products, and click **OK**.

   > You can change this folder anytime in the Settings dialog box.

6. In the left pane of Deltek Software Manager, expand the Deltek product that you want to download, if it is not already expanded.
7. Select the product type that you want to download. Your options are **Complete**, **HotFix**, and **Sub-Release**.
8. In the table, select the check box that corresponds to the Deltek product that you want to download. The right pane displays a message stating that the product has been added to the download queue.

To view the items in the download queue, click **View Download Queue** at the bottom of the left pane.

9. Click **Download** at the bottom of the left pane. Deltek Software Manager downloads the product to the folder that you selected.

DSM Documentation and Troubleshooting

- To view the online help for Deltek Software Manager, click here.
- To view a tutorial on how to use Deltek Software Manager, click here.
- To view more information on troubleshooting Deltek Software Manager, click here.

The preceding troubleshooting link only works if you are logged in to Deltek Customer Care Connect.

Adding Custom Notes to This Guide

If you would like to add custom notes to this guide that are specific to your company, Adobe® Reader® X provides this ability. If you do not already use Adobe Reader X, you can download it here free from Adobe.

To add a custom note using Adobe Reader X, complete the following steps:

1. On the Reader toolbar, click **Comment** at the far right.
2. In the **Annotations** pane that displays, click 💬 **Sticky Note**. The cursor changes to match the button.
3. Position the cursor at the location in the guide where you want the note to appear, and click. A note icon is inserted at the location and a text box pops up.
4. Enter your information in the text box.
5. Continue adding notes as needed.
6. Save the document.

Deltek recommends that you save the document to a slightly different filename so as to keep the original from being overwritten.

When reading the document, cursor over a note icon to see the information. Double-click a note icon to edit the information.