

Use IIS URL Rewrite for Mobile Redirect

Introduction

This document explains how to redirect mobile devices by detecting the browser agent using an IIS URL Rewrite.

Prerequisites

1. Ensure the following items are installed and running before configuring URL Rewrite

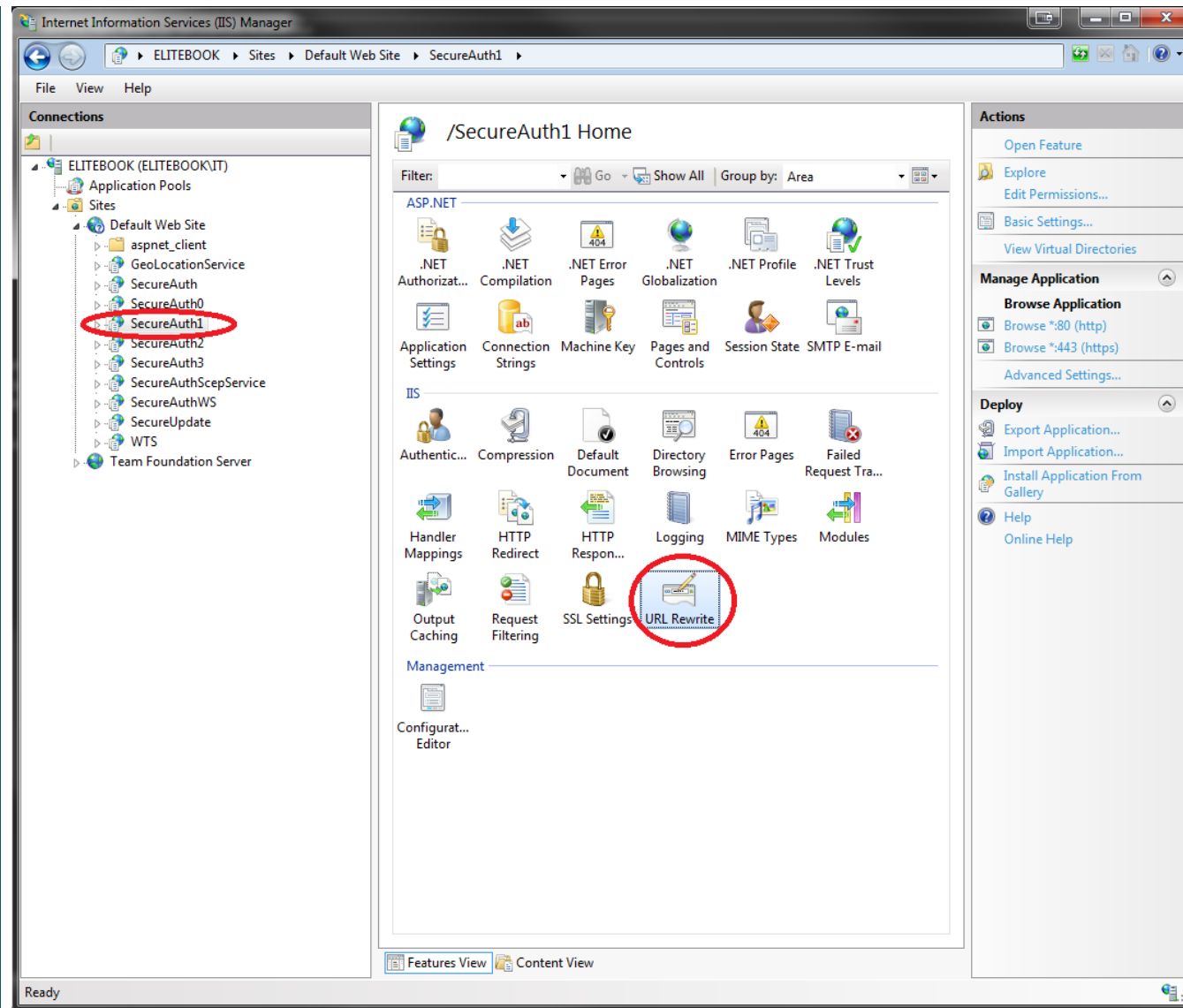
- SecureAuth IdP Version 7.x+
- Windows Server 2008, 2008 R2, 2012, or 2012 R2

2. Install [URL Rewrite extension](#) on the Windows server

Note that IP and Domain Restrictions in IIS take precedence over URL Rewrite

When configuring the Windows server to use the URL Rewrite add-on, set the feature settings under IP and Domain Restrictions to **Allow**

Configuration Steps



1. In the IIS window, select the SecureAuth IdP realm from the tree view pane
2. On the target pane, double-click the **URL Rewrite** icon

URL Rewrite

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
------	-------	-------	---------

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

Name	Input	Match	Pattern	Action Type	Action Value	Stop
------	-------	-------	---------	-------------	--------------	------

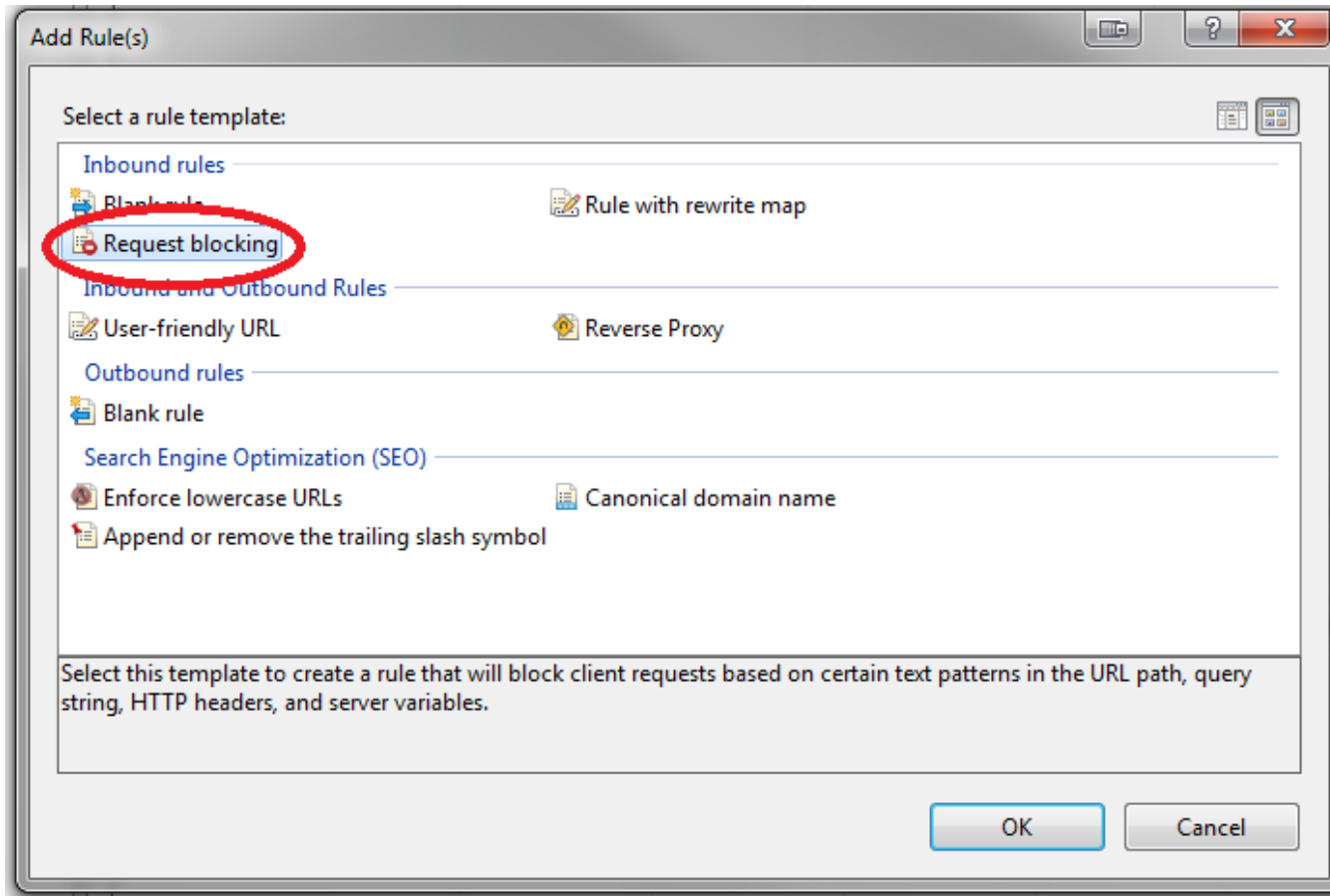
Actions

- [Add Rule\(s\)...](#)
- [Revert to Parent](#)
- Manage Server Variables**
 - [View Server Variables...](#)
- Manage Providers**
 - [View Rewrite Maps...](#)
 - [View Providers...](#)
- Inbound Rules** ▲
 - [Import Rules...](#)
- Outbound Rules** ▲
 - [View Preconditions...](#)
 - [View Custom Tags...](#)
- Help**
 - [Online Help](#)

Features View Content View

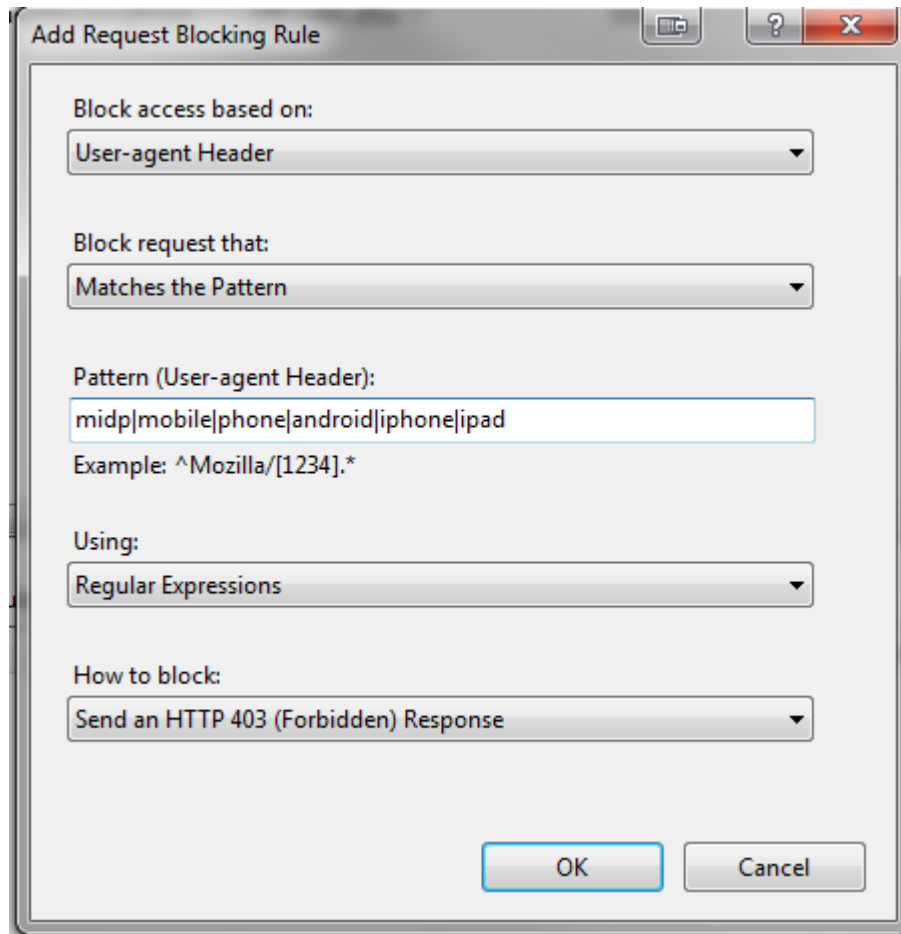
3. On the **URL Rewrite** pane, on the Actions section in the upper right corner, click **Add Rule(s)** to create the first rule (i.e. to allow internal access to remain on this realm)

Add Rule(s)



4. On the **Add Rule(s)** dialog, select **Request blocking** and click **OK**

Add Request Blocking Rule



5. On the **Add Request Blocking Rule** dialog, select **User-agent Header** from the **Block access based on** dropdown
6. Select **Matches the Pattern** from the **Block request that** dropdown
7. Enter the **Pattern (User-agent Header)** using the format **midp|mobile|phone|android|iphone|ipad** – note each word in the pattern is separated by a pipe character (|) without any spaces
8. Select **Regular Expressions** from the **Using** dropdown
9. Select **Send an HTTP 403 (Forbidden Response)** from the **How to block** dropdown
10. Click **OK**

Edit Inbound Rule



Edit Inbound Rule

Requested URL:

Matches the Pattern

Using:

Regular Expressions

Pattern:

*

Test pattern...

Ignore case

Conditions

Logical grouping:

Match All

Input	Type	Pattern
{HTTP_USER_A...	Matches the Pattern	midp mobile phone android i...

Add...

Edit...

Remove

Move Up

Move Down

Track capture groups across conditions

Server Variables

Action

Action type:

Redirect

Action Properties

Redirect URL:

/SecureAuth3

Append query string

Redirect type:

Permanent (301)

11. Double-click the newly created rule to edit the settings for that rule
12. On the **Edit Inbound Rule** pane, select **Redirect** from the **Action type** dropdown
13. On the **Actions** section in the upper right corner, click **Apply**

The newly configured mobile redirect rule can be renamed to a more descriptive name such as "MobileRedirectRule"

Sample Web.Config Section for a Successful Configuration

```
<rule name="MobileRedirectRule" patternSyntax="ECMAScript" stopProcessing="true">
  <match url=".*" ignoreCase="true" negate="false" />
  <conditions logicalGrouping="MatchAny" trackAllCaptures="false">
    <add input="{HTTP_USER_AGENT}" pattern="midp|mobile|phone|android|iphone|ipad" />
  </conditions>
  <action type="Redirect" url="/SecureAuth3" appendQueryString="true" redirectType="Permanent" />
</rule>
```

Related Topics

- [Use URL Rewrite for IP Restrictions](#)
- [Use X-Forwarded-For \(XFF\) with URL Rewrite Module](#)

