

eCAGE

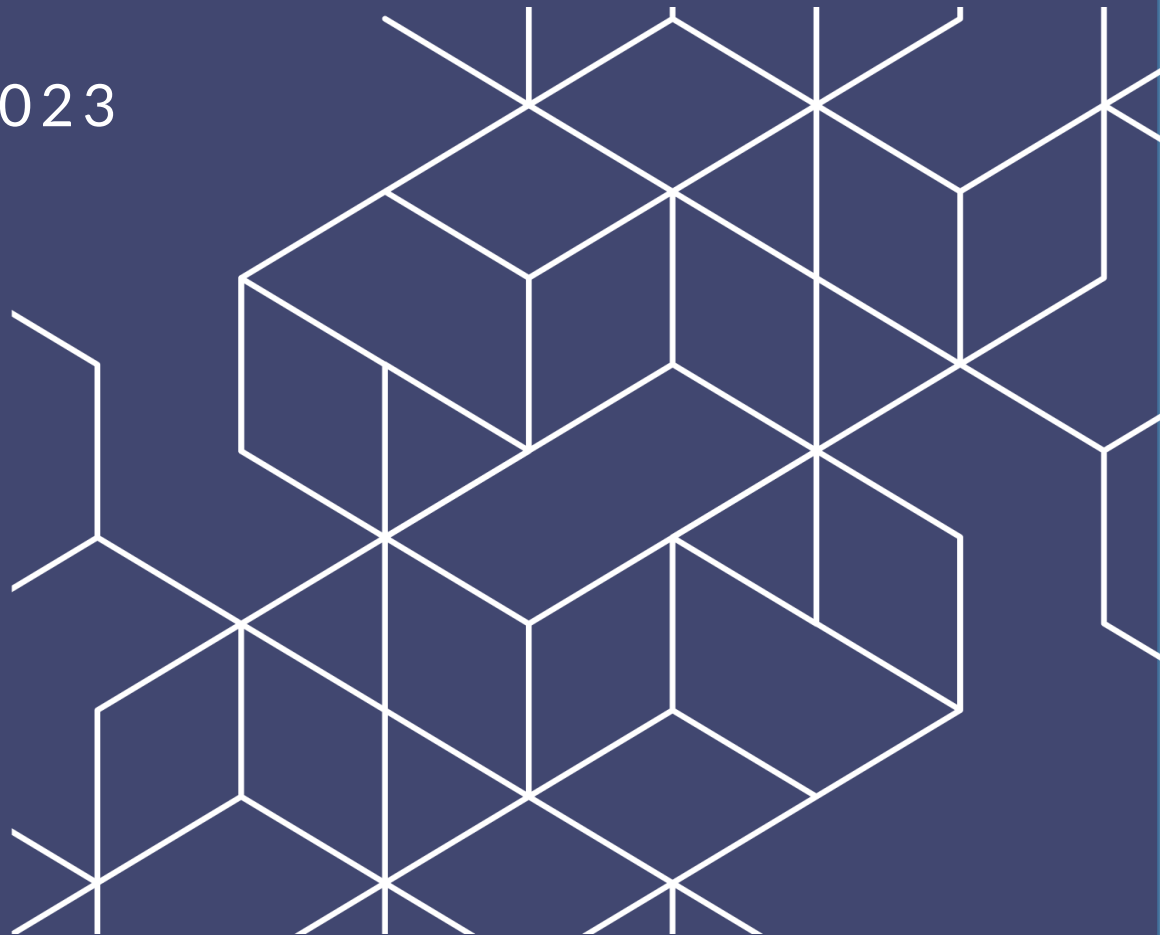


OPEXUS

PIV Configuration

v11.1.0

August 2023



eCASE v11.1.0 PIV Configuration

Notice of Rights

Copyright © 2023, AINS, LLC d/b/a OPEXUS. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the publisher: AINS, LLC. For information on obtaining permission for reprints and excerpts, contact info@opexustech.com.

Additionally, all copyrights, confidential information, patents, design rights and all other intellectual property rights of whatsoever nature contained herein are, and shall remain, the sole and exclusive property of the publisher.

Notice of Liability

The information in this publication is believed to be accurate and reliable. However, the information is distributed by the publisher (AINS, LLC.) on an “As Is” basis without warranty for its use, or for any infringements of patents or other rights of third parties resulting from its use.

While every precaution has been taken in the preparation of this publication, neither the author (or authors) nor the publisher will have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused, directly or indirectly, by the information contained in this publication or by the computer software and hardware products described in it.

Notice of Trademarks

The publisher’s company name, company logo, company patents, and company proprietary products are trademarks or registered trademarks of the publisher: AINS, LLC. All other trademarks or registered trademarks are the property of their respective owners.

Non-Disclosure Statement

This document’s contents are confidential and proprietary to AINS, LLC. This document cannot be released publicly or outside the purchasing agency without prior written permission from AINS, LLC.

Images in this manual are used as examples and may contain data and versioning that may not be consistent with your version of the application or information in your environment.

Additional Notice

Information in this documentation is subject to change without notice and does not represent a commitment on the part of AINS, LLC.

Notwithstanding any of the foregoing, if this document was produced as a Deliverable or other work for hire under a contract on behalf of a U.S. Government end user, the terms and conditions of that contract shall apply in the event of a conflict.



Contents

- Using This Manual 4
- Acronyms..... 4
- 1 Introduction 5
 - 1.1 About This Manual..... 5
 - 1.2 System Requirements for PIV Server 5
- 2 Steps to Configure eCASE for PIV 6
 - 2.1 Take Database Backup..... 6
 - 2.2 Install Latest Service Pack 6
 - 2.3 Install PIV Card Authentication Hotfix 6
 - 2.4 Install SLL Certification and Configure IIS (Single Server Option) 7
 - 2.5 Install SSL Certificate and Configure IIS (Two Servers Option) 8
 - 2.5.1 Application Sever 8
 - 2.5.2 PIV Server 9
 - 2.6 Set the Banner Page Location (Two Servers Option)..... 12



Using This Manual

The following formatting conventions are used in this manual to highlight important information:

- *Italicized* text indicates a location, for example a particular *Folder*, *Tab*, or *Window*.
- **Bold** text indicates a specific user action, such as clicking a **button**.
- **Red** text and this symbol (!!) are used in Notes to **bring attention to crucial information**.

Acronyms

All acronyms used in this document are defined in the following table:

Acronym	Definition
IIS	Internet Information Services
PIV	Personal Identity Verification
SSL	Secure Socket Layer



1 Introduction

1.1 About This Manual

This manual is intended to assist eCASE Administrators with Personal Identity Verification (PIV) configuration. In this document you'll find system requirements for the PIV server, as well as steps to configure your eCASE application for PIV.

Please contact support@opexustech.com if you need any more information, or if you encounter issues with this configuration.

1.2 System Requirements for PIV Server

The PIV server for eCASE must meet the following minimum requirements:

- Windows 2016 Server with IIS 10 server
- Install URL Rewrite and ARR IIS Modules. You can download these extensions from Microsoft web sites. Try these links: <https://www.iis.net/downloads/microsoft/url-rewrite>, <https://www.microsoft.com/en-us/download/details.aspx?id=47333>



2 Steps to Configure eCASE for PIV

Follow the steps in the subsections below to configure eCASE for PIV.

2.1 Take Database Backup

Follow the steps below to take a database backup:

1. Access the eCASE database server.
2. Open *Microsoft SQL Server Management Studio*.
3. Right-click the **eCASE database** and take a backup of the database.
4. Once the backup is complete, proceed to Section 2.2 to install the latest service pack. If the latest service pack is already applied, move to Step 2.3.

2.2 Install Latest Service Pack

Follow the steps below to install the latest Service Pack, if it is not already applied:

1. Access the application server where eCASE is installed as an Administrator.
2. Copy the *eCASE v11.1.0 Latest Service Pack*.
3. In the main root of the folder, run **Hotfix.exe** as an Administrator.
4. Provide the Backup location to take the backup of the files.
5. Click **Apply**.
6. Confirm that the eCASE database is backed up.
7. Run the installation wizard.
8. After the Hotfix is installed successfully, click **OK**.
9. Proceed to Step 3.

2.3 Install PIV Card Authentication Hotfix

Follow the steps below to install the PIV Card Authentication Hotfix:

1. Access the application server where eCASE is installed as an Administrator.
2. Add the following entries to the web.config file located in the eCASE installed directory:
C:\Program Files\AINS eCase\eCase
<location path="Banner/Disclaimer.aspx">

<system.web>



```
<authorization>
  <allow users="?" />
</authorization>
</system.web>
</location>
<location path="NoPIV.aspx">
  <system.web>
    <authorization>
      <allow users="?" />
    </authorization>
  </system.web>
</location>
```

3. Next, run the *eCASE Database Configuration Tool* as an Administrator.
4. Under *Application/Service*, select **eCASE**.
5. Click **Save**.
6. Navigate to the *Sign-on Mode* tab.
7. Check the **Two-Factor Authentication** checkbox and provide the *Subject* from the SSL Certificate.
8. Click **Save**.

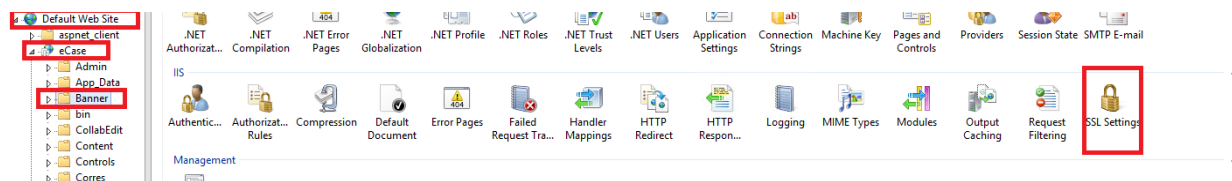
2.4 Install SSL Certification and Configure IIS (Single Server Option)

Follow the steps below to install the SSL certificate and configure IIS when using the option for a single server:

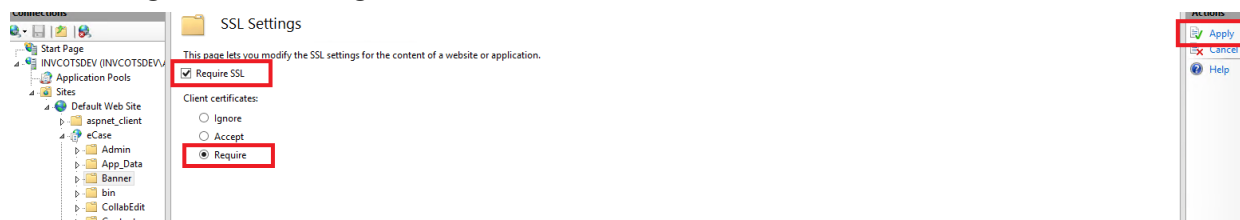
1. Install the Server Certificate into IIS and configure bindings for HTTPS on the eCASE Application Server.
2. Open the IIS and click **SSL Settings**.



Steps to Configure eCASE for PIV



3. Configure the settings as shown below:

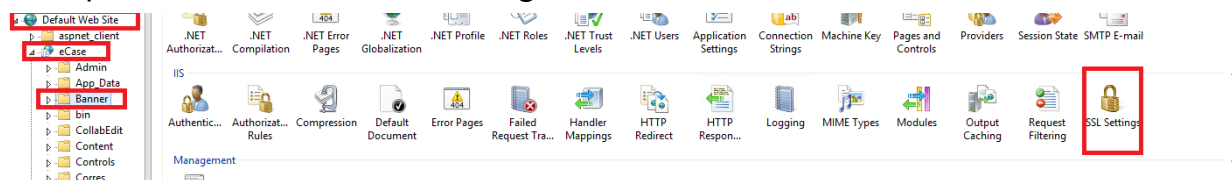


4. Reset IIS.

2.5 Install SSL Certificate and Configure IIS (Two Servers Option)

2.5.1 Application Sever Installation

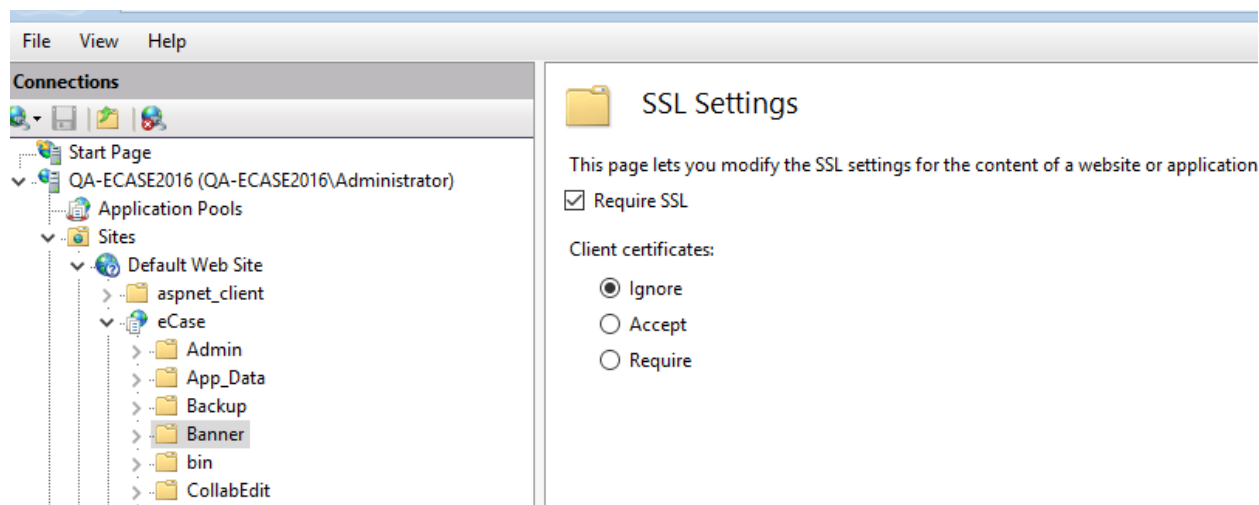
1. Install the Server Certificate into IIS and configure bindings for HTTPS on the eCASE Application Server.
2. Open the IIS and click **SSL Settings**.



3. Configure the settings as shown below.



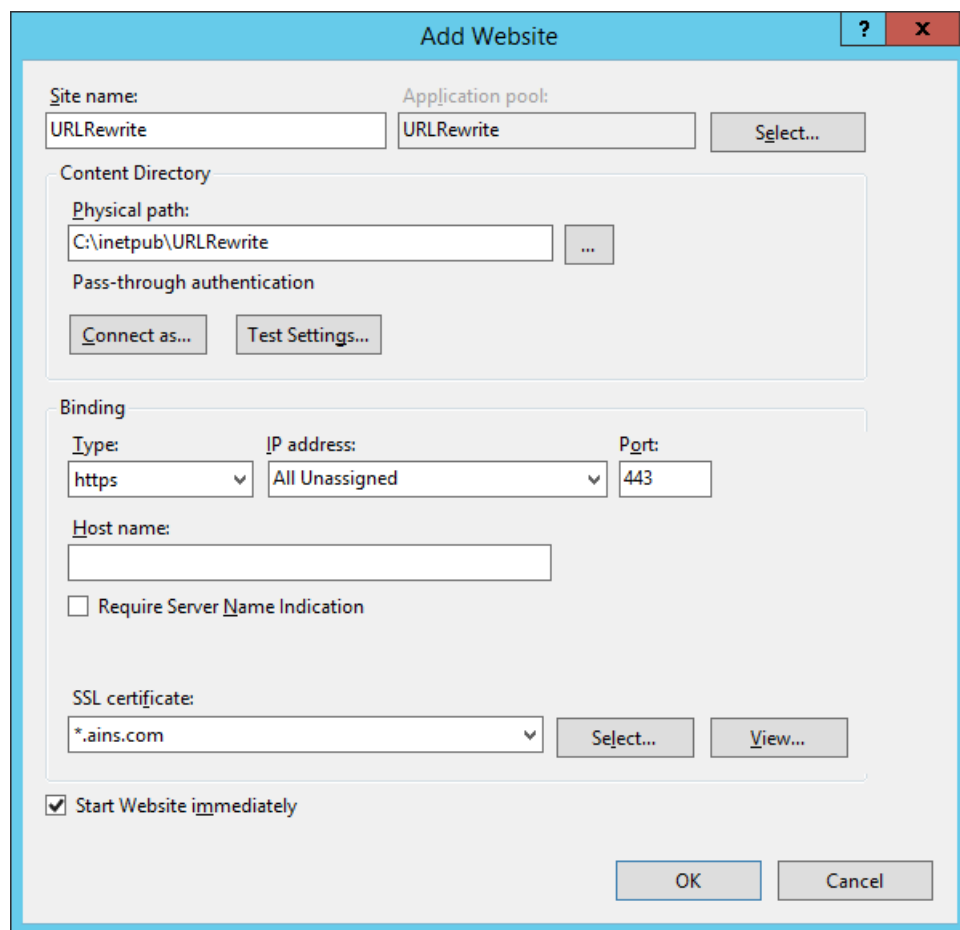
Steps to Configure eCASE for PIV



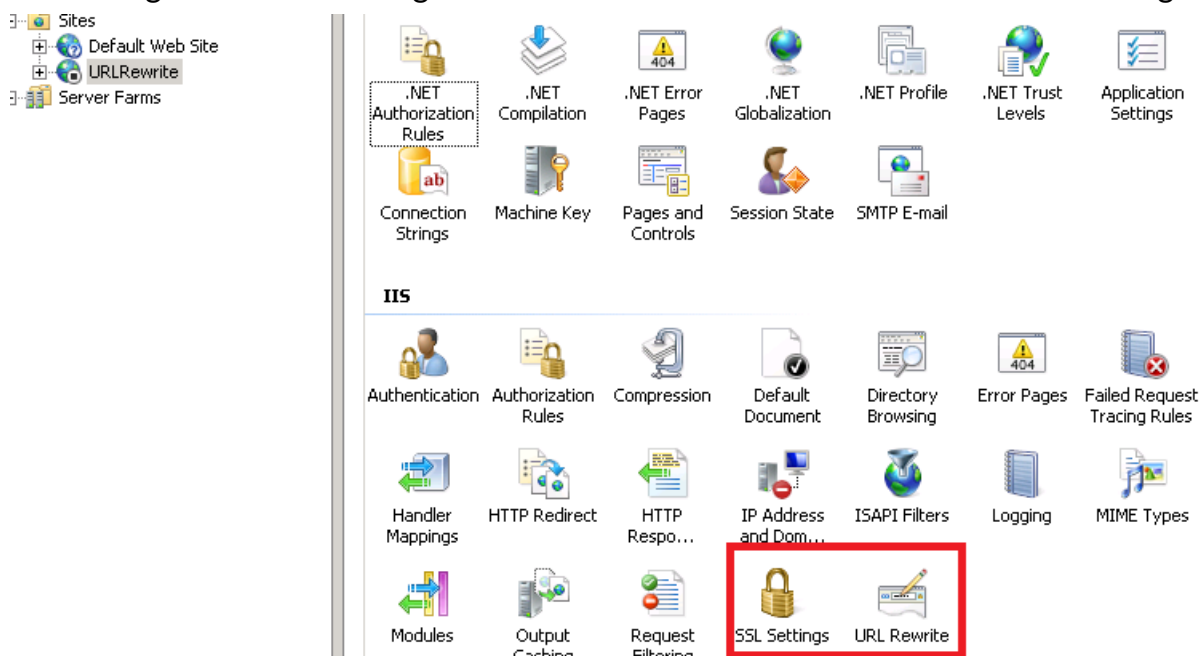
4. Reset IIS.

2.5.2 PIV Server Installation

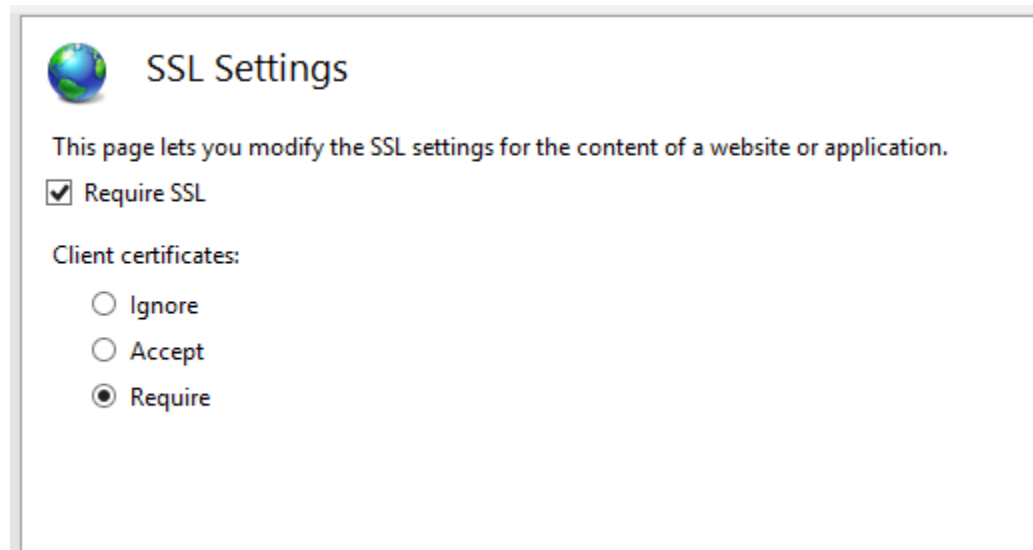
1. Install Server Certificate into IIS and configure bindings for HTTPS on PIV Server.
2. Open the IIS, and create a new web site with name URLRewrite with HTTPS binding.



3. Configure the SSL Settings and URL Rewrite rules as described in the following steps.




4. Configure the SSL Settings as shown below:



5. Add a Rewrite rule with Request Blocking template to abort application related traffic, except Images and Disclaimer.aspx.
6. Configure the URL blocking rules as shown below. Please make sure type, patterns, and Conditions and Action are configured as shown:

Steps to Configure eCASE for PIV

 Edit Inbound Rule

RequestBlockingRule1

Match URL

Requested URL: Using:

Pattern:

☒ Ignore case

Conditions

Logical grouping:

Input	Type	Pattern
{URL}	Does Not Match the Pattern	*/eCase/Banner/Disclaimer.aspx
{URL}	Does Not Match the Pattern	*/eCase/Images/*.*

☐ Track capture groups across conditions

Server Variables

Action

Action type:

7. Add a Rewrite rule with Reverse Proxy template to rewrite the traffic to the application server.
8. Click **Add Rule** and enter the application server name to forward the request:



Add Reverse Proxy Rules

Inbound Rules
 Enter the server name or the IP address where HTTP requests will be forwarded:

 Example: contentserver1
☐ Enable SSL Offloading
 Selecting this option will forward all HTTPS requests over HTTP.

Outbound Rules
☐ Rewrite the domain names of the links in HTTP responses
 Responses that are generated by applications that are behind a reverse proxy can have HTTP links that use internal domain names. These links must be updated to use external domain names.
 From:

 Example: contentserver1
 To:

 Example: www.contoso.com

OK Cancel

(!!) Note: The Request Blocking rule should be before Reverse Proxy rule. These rules will ensure only PIV requests are sent to the dedicated PIV server, and all application requests are sent to the eCASE Application server. The second server configuration provides the ability to monitor PIV server traffic and ignore the application traffic.

2.6 Set the Banner Page Location (Two Servers Option)

Run the following SQL query in the eCASE database with the proper PIV Server name to set to the banner page location:

Update EC_CONFIGURATION

SET CONFIG_VALUE='https://<pivservername>/eCase/Banner/Disclaimer.aspx'

where CONFIG_KEY='BannerPage'

