

The logo consists of the letters 'AP' in a bold, black, sans-serif font. The letters are positioned on a white rectangular background. Below the white background is a solid red horizontal bar. The entire logo is set against a dark blue background that covers the rest of the page.

AP

AP ENPS Mobile Administrator's Guide

Version 9.5

Published: March 6, 2024

Copyright © 2024 Associated Press. All rights reserved.

This manual (the “Manual”) and the ENPS software (the “Software”) are copyrighted and all rights are reserved by the Associated Press. No part of the Manual or the Software may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the Associated Press.

The Software described in the manual is furnished under a license agreement and can be used or copied only in accordance with the terms of the license agreement.

The information in the Manual is subject to change without notice. No part of the Manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without prior express written permission of the Associated Press.

THE MANUAL AND THE INFORMATION CONTAINED WITHIN IS PROVIDED “AS IS” AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED.

The Associated Press may have patents or pending patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. The furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property rights except as expressly provided in any written license agreement from the Associated Press.

The terms ENPS, Associated Press and AP are registered trademarks of the Associated Press. Windows is a trademark of the Microsoft Corporation. Other products and company names mentioned herein may be the trademarks of their respective owners.

Table of Contents

Table of Contents	iii
Getting Started	4
Network and Firewall Configuration	5
Installing Mobile Server Applications	8
Installing on Windows Server 2022	8
Installing on Windows Server 2019	26
Upgrading on Windows Server 2019	42
Installing on Windows Server 2016	50
Upgrading on Windows Server 2016	66
Configuring ENPS Mobile	75
Session Timeout	84
ENPS Server Settings for Mobile	84
Media Upload	86
Language Support for Mobile Devices	86
Troubleshooting	88
Not Seeing New Features and Enhancements	90
IIS Issues	90
Duplicate Values	90
ASP .NET Issues	91
User Login Events	92
Appendix A. Purchasing and Installing SSL Certificates	94
Part One: Purchasing an SSL Certificate	94
Part Two: Generating a Certificate Request	95
Part Three: Installing a Server Certificate	96

Getting Started

ENPS Mobile extends ENPS functionality to phones, tablets and desktop/laptop browsers. These platforms provide new ways for journalists to connect and use ENPS from outside the newsroom and wherever news is happening.

Do not install ENPS Mobile on your ENPS Primary or Buddy Server. You must designate a separate machine, or machines, as your ENPS Mobile server(s). These machines will act as the gateway between the mobile devices and the ENPS servers in your enterprise.

The table below describes the minimum hardware and software requirements for ENPS Mobile servers.

Minimum Server Requirements	
CPU	Intel Xeon, minimum of 4 cores, 2 GHz or faster
Supported Operating System	Windows Server 2022 Windows Server 2019 Windows Server 2016
ENPS	ENPS 9 or later
RAM	8 GB
Hard Disk Storage	120 GB
Additional Software	Internet Information Services (IIS) Microsoft .NET Framework 4.8 SSL certificate. This is required to use the AP ENPS app. Strongly recommended, even when using ENPS Mobile entirely within your protected network.

NOTE: The above represents the minimum requirements for a small to medium standalone site or a small enterprise. Larger installations should plan to exceed these minimums and may wish to consult with ENPS support prior to ordering any hardware.

NOTE: In order for Mobile version 9.5 to work properly, you must clear your browser cache on any client devices and ensure you have the latest version of the app before installing the Mobile server components.

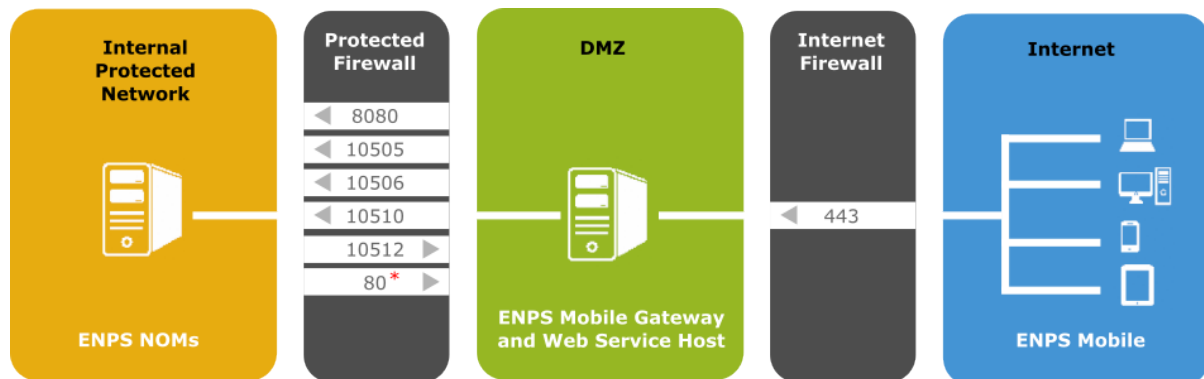
In all cases, performance and speed will be enhanced if your computer's processor, memory, and available disk space exceed the minimum requirements.

Network and Firewall Configuration

ENPS Mobile consists of two parts—the Mobile Gateway and the Web Service Host—that should be installed on a single server. All devices connecting to ENPS Mobile will need direct access to both components.

In a standard installation where ENPS Mobile will be used outside the newsroom and without VPN access, the ENPS Mobile Server should be placed in a DMZ.

If a VPN solution will be required for access to ENPS Mobile, the ENPS Mobile server can be placed inside your protected network. The server can also be placed inside your protected network if it will only be accessed from within the newsroom and studio, (e.g. a dedicated server for use with the Tablet Story Viewer).



* Open from central server only

Suggested Network Deployment for ENPS Mobile with External Access:

Please note the following:

- ENPS Mobile can be configured to work over port 80 (HTTP) or port 443 (HTTPS), however it is strongly recommended to only use port 443 (HTTPS) for maximum security, even if the Mobile servers are entirely within your network and not exposed to the Internet. The native iOS & Android Apps will only work using HTTPS.
- When placing the Mobile server in a DMZ, only port 443 should be allowed inbound from the public Internet (unless you are choosing not to use HTTPS).
- When using HTTPS, a signed SSL certificate from a trusted CA is required. Self-signed certificates cannot be used. See the section below for more information.
- Traffic must be allowed between the ENPS Mobile Server in the DMZ and the ENPS servers inside the protected network as follows:

From the DMZ to the protected network:

- **10505 (TCP)**. Used for user login and all search requests (for search requests ONLY if using IS or WSS). Needs to be open to **all** ENPS servers in the enterprise.
- **10506 (TCP)**. All non-search client data requests. Needs to be open to **all** ENPS servers in the enterprise.
- **10510 (TCP)**. Private channel to the NOM(s) for real-time updates of all non-wire content. Needs to be open to **all** ENPS servers in the enterprise.
- **8080 (TCP)**. Used for search requests when using Solr.

From the protected network to the DMZ (all ports TCP except 10512, which is UDP):

- **10512 (UDP)**. Real-time updates of incoming wire content. Needs to be open from all ENPS servers in the enterprise.
 - **80 (TCP)**. Allows automatic updating of the Web Service Host whenever a change is made to the ENPS global tables. Needs to be open only from the Central Server.
- For sites using UDP broadcasts, the IP address of your Mobile server(s) should be added to the [Reflectors] section of the NWP.INI file on all of your ENPS servers and the NWP restarted.
 - For sites using Multicast, complete the step above and also ensure the following settings are in place:

- MulticastAlsoBroadcast=1 in the Global Configuration Table
- Broadcast=0 in the [NWP] section of NWP.INI
- Broadcast=1 in the [TCPIP] section of NWP.INI
- If your Mobile server is in a subnet that is already receiving UDP traffic from your ENPS servers, none of the above changes to the NWP.INI or Global Configuration table are necessary. No configuration changes are needed for the NOM whether you are using UDP broadcasts or Multicast.
- In order to avoid interference with real-time updates in Mobile, no ENPS desktop clients should be run on the Mobile server.
- Multiple instances of the ENPS Mobile server can be deployed throughout the enterprise, both inside and outside the protected network, as needed.
- No additional components are required on the ENPS server to support ENPS Mobile.

Installing Mobile Server Applications

NOTE: In order for ENPS Mobile version 9.5 to work properly, you must clear your browser cache on any client devices and ensure you have the latest version of the app before installing the Mobile server components.

This section will show you how to install ENPS Mobile. Note the following important points before you start a first-time installation of the ENPS Mobile server:

- Refer to Hardware and Software Requirements to make sure your equipment meets all of the prerequisites.
- ENPS Mobile servers require static IP addresses, not reserved DHCP IP addresses.
- ENPS Mobile servers may not run any other services except SNMP.
- ENPS Mobile servers cannot be Active Directory Domain Controllers.
- **Do not name your Mobile server ENPS.** Most sites use their name. Ex: WXXX-MOB. NOTE: The name you choose should not exceed 15 characters due to a Microsoft threshold.

For sites running ENPS Mobile versions 1.x or 2.x, please note this is a new application and there is no direct upgrade from older versions. If your older ENPS Mobile servers meet the requirements for this version, it is possible to have both versions installed on the same hardware, if needed, during a transition period. Simply follow the standard installation instructions below. To uninstall older versions, go to **Control Panel > Programs and Features**, select the older ENPS Mobile components and choose "uninstall."

Please note that there may be portions of the following steps that are unnecessary if you are installing ENPS Mobile 9.5 on the same machine as a previous version.

Installing on Windows Server 2022

Install ENPS Mobile by following these stages in order:

- "Configure Role Services" below
- "Configure Application Pools" on the next page
- "Install ENPS Mobile" on page 12
- "Enable Secure Sockets Layer" on page 19
- "Configure Application Pools with Advanced Settings" on page 20
- "Configure the Web Service Host" on page 22
- "Synchronize ENPS Global Tables in ENPS Mobile" on page 25
- "Next steps" on page 26

Configure Role Services

First, start *Windows Server Manager* and select **Manage > Add Roles and Features** to open the related wizard.

Complete the wizard by following these instructions, clicking **Next** to move onto each subsequent screen:

<i>Add Roles and Features Wizard</i> screen	Instructions
Before you begin	Read the information.
Installation Type	Ensure that <i>Role-based or feature-based installation</i> is selected.
Server Selection	Ensure that <i>Select a server from the server pool</i> is selected and that your Mobile server is highlighted in the Server Pool pane.
Server Roles	Ensure the following roles are selected: <ul style="list-style-type: none"> • <i>File and Storage Services > File and iSCSI Services > File Server</i> • <i>Web Server (IIS)</i> • <i>Web Server > Common HTTP Features > HTTP Redirection</i>

	<div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; display: inline-block;"> NOTE: Select Add Features if a dialog appears. </div>
Features	<p>Ensure that the following features are selected:</p> <ul style="list-style-type: none"> • <i>NET Framework 4.8 Features > ASP.NET 4.8</i> • <i>WCF Services > HTTP Activation</i>
Web Server Role (IIS)	Read the information.
Web Server Role (IIS) > Role Services	<p>Expand <i>Management Tools > IIS 6 Management Compatibility</i> and select:</p> <ul style="list-style-type: none"> • <i>IIS 6 Metabase Compatibility</i> • <i>IIS 6 Management Console</i> • <i>IIS 6 WMI Compatibility</i> • <i>IIS 6 Scripting Tools</i> <div style="text-align: center;"> <div style="border: 1px solid #0070C0; border-radius: 10px; padding: 5px; display: inline-block;"> NOTE: Select Add Features if a dialog appears. </div> </div>
Confirmation	Read the information, then click Install .
Results	Wait for installation to complete, then click Close .

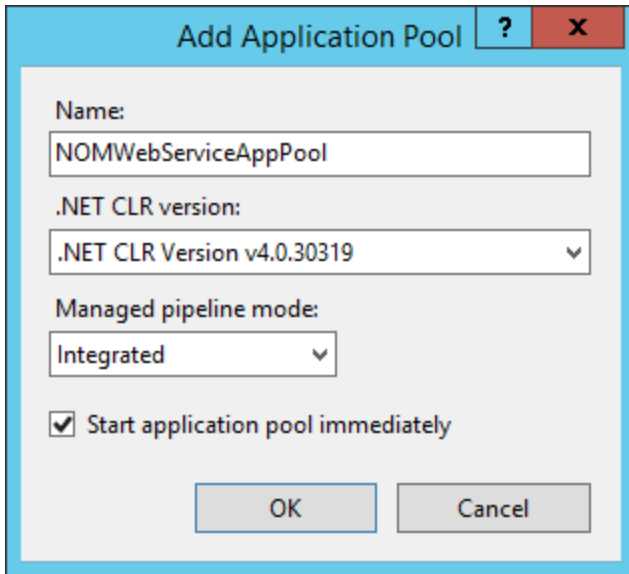
Configure Application Pools

Follow these instructions to configure Application Pools.

NOM Web Service Application Pool

To configure the NOM Web Service Application Pool, follow these steps:

1. Start Windows *Server Manager*.
2. Select **Tools > Internet Information Services (IIS) Manager** to open that tool.
3. In the **Connections** pane expand the server name.
4. Right-click **Application Pools** and select *Add Application Pool*.
5. Set the following fields in the **Add Application Pool** dialog:
 - **Name:** *NOMWebServiceAppPool*
 - **.NET CLR version:** *.NET CLR Version v4.0.30319*

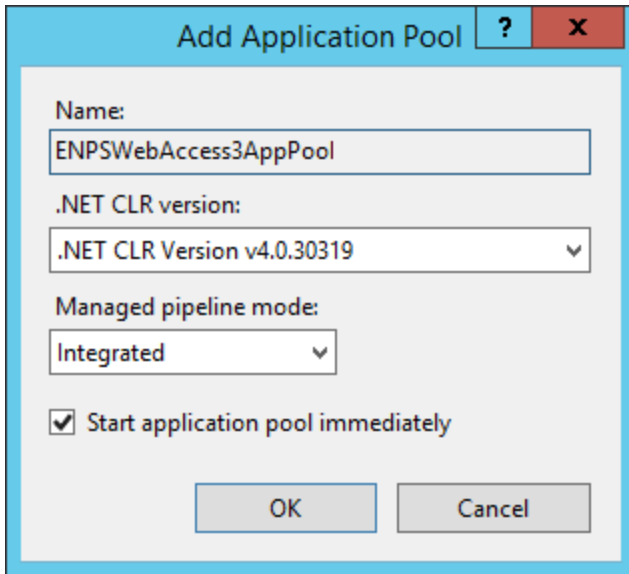


6. Click **OK** to add the application pool and close the dialog.

ENPS Web Access Application Pool

To configure the ENPS Web Access Application Pool, follow these steps:

1. Start Windows *Server Manager*.
2. Select **Tools > Internet Information Services (IIS) Manager** to open that tool.
3. In the **Connections** pane expand the server name.
4. Right-click **Application Pools** and again select *Add Application Pool*.
5. Set the following fields in the **Add Application Pool** dialog:
 - **Name:** *ENPSWebAccess3AppPool*
 - **.NET CLR version:** *.NET CLR Version v4.0.30319*

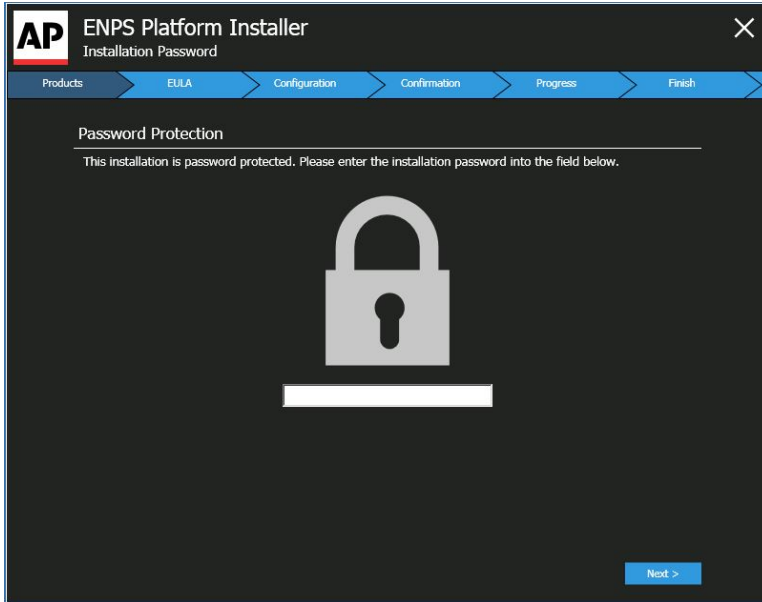


6. Click **OK** to add the application pool close the dialog.

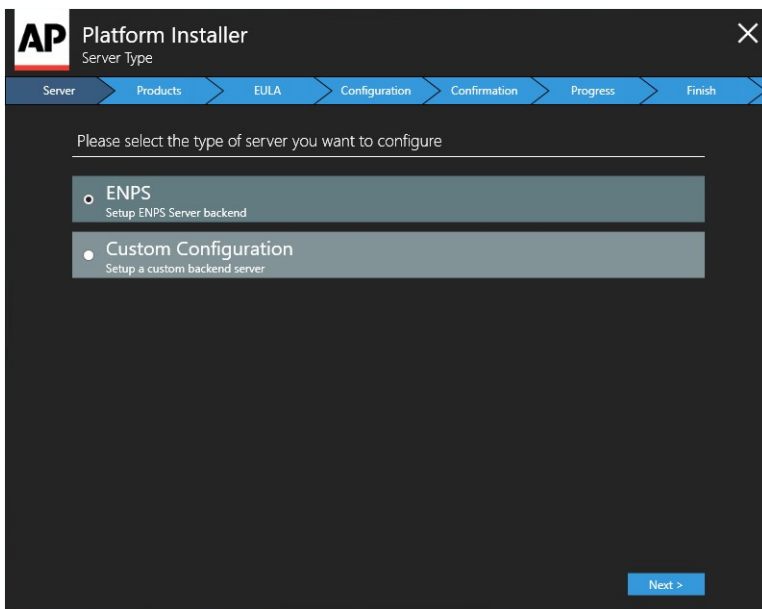
Install ENPS Mobile

Follow these instructions to install ENPS Mobile using the Platform Installer.

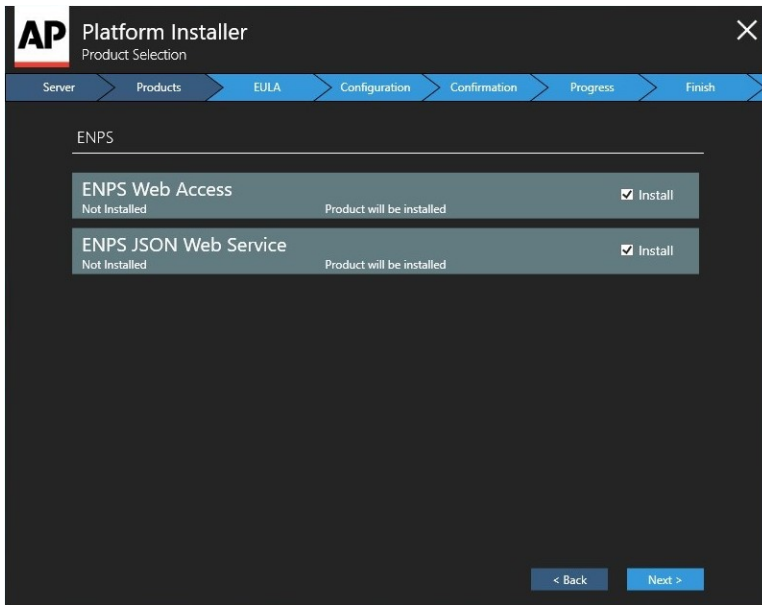
1. Download the ENPS Platform Installer zip file from the ENPS Mobile Download page at <https://downloads.enps.com>. Click **Register** on that page if you don't already have an account.
2. Right-click the zip file and select **Properties** to open the file properties dialog.
3. Ensure that the **Unblock** checkbox is selected in the **General** tab, then click **OK**.
4. Extract the zip file.
5. Open the ENPS Platform Installer. The **Password Protection** screen appears. Enter your password and click the **Next** button.



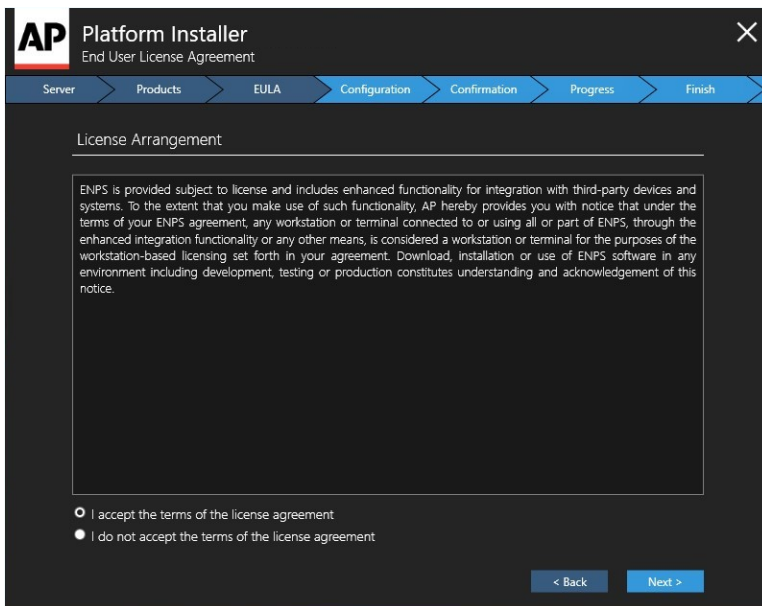
6. In the **Server Type** screen, select **ENPS Web Applications Server** and then click the **Next** button.



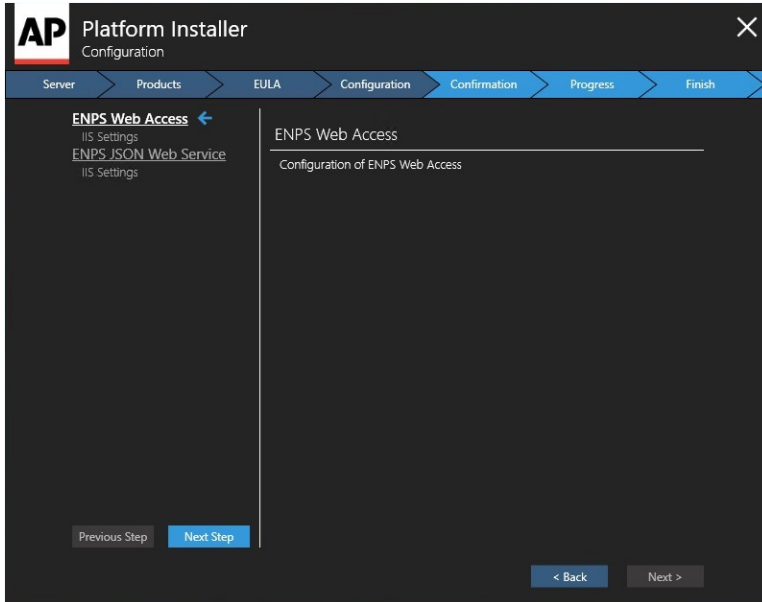
7. In the **Product Selection** screen, select the **Install** checkboxes next to **ENPS Web Access** and **ENPS JSON Web Service**, then click the **Next** button.



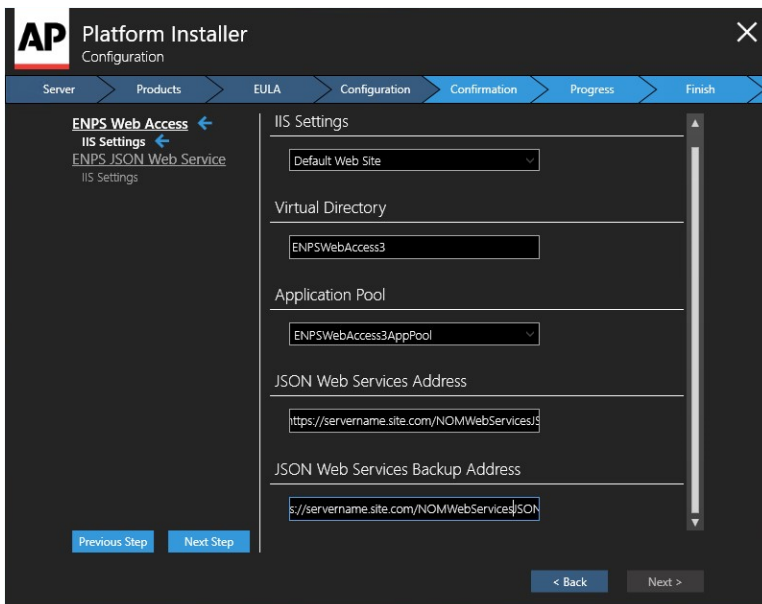
8. In the **End User License Agreement** screen, select the radio button for *I accept the terms of the license agreement*, then click the **Next** button.



9. The **Configuration** screen appears. In the first configuration screen, you do not need to make any selections. Click the **Next Step** button on the **left** panel of the **Configuration** screen to continue.



10. The **IIS Settings** screen for **ENPS Web Access** will appear. In the **IIS Settings** screen, select the following:

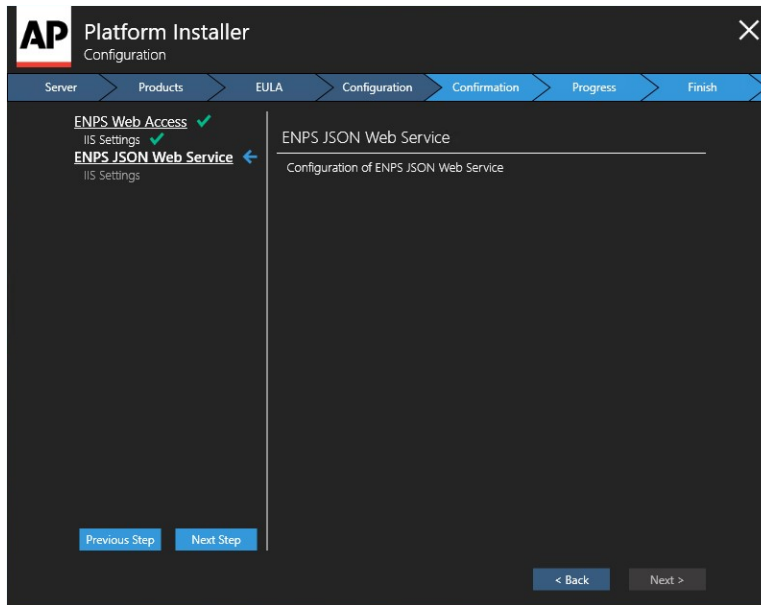


- **IIS Settings.** Enter *Default Web Site*.
- **Virtual Directory.** Enter *ENPSWebAccess3*.
- **Application Pool.** Enter *ENPSWebAccess3AppPool*.
- **JSON Web Services Address.** Enter your server name followed by */NOMWebServices3JSON*. For example, if your JSON Web Services server is

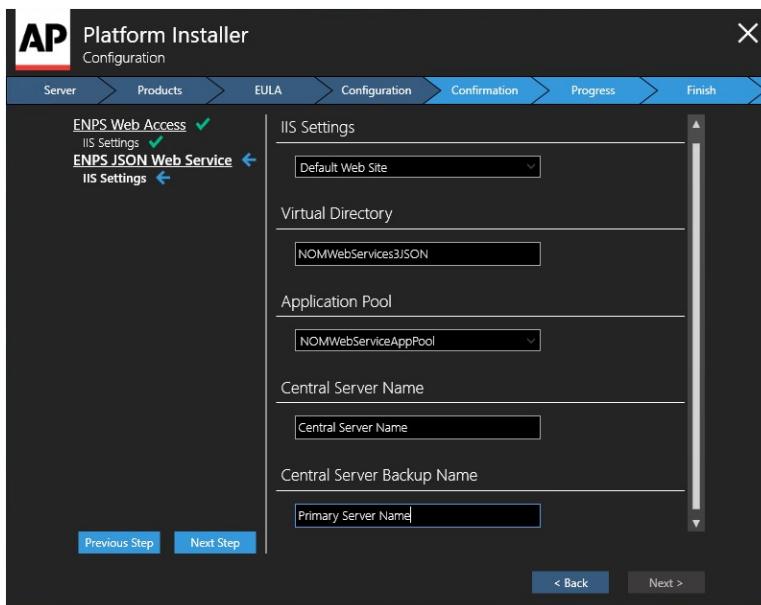
located at `https://servername.site.com`, enter `https://servername.site.com/NOMWebServices3JSON`.

- **JSON Web Services Backup Address.** If the site has a backup JSON address then enter it in this field. Otherwise, enter the same address as the main **JSON Web Services Address** entered above.

Click the **Next Step** button on the **left** side of the screen to continue.



11. The **IIS Settings** screen for **ENPS JSON Web Service** will appear. In the **IIS Settings** screen, select the following:

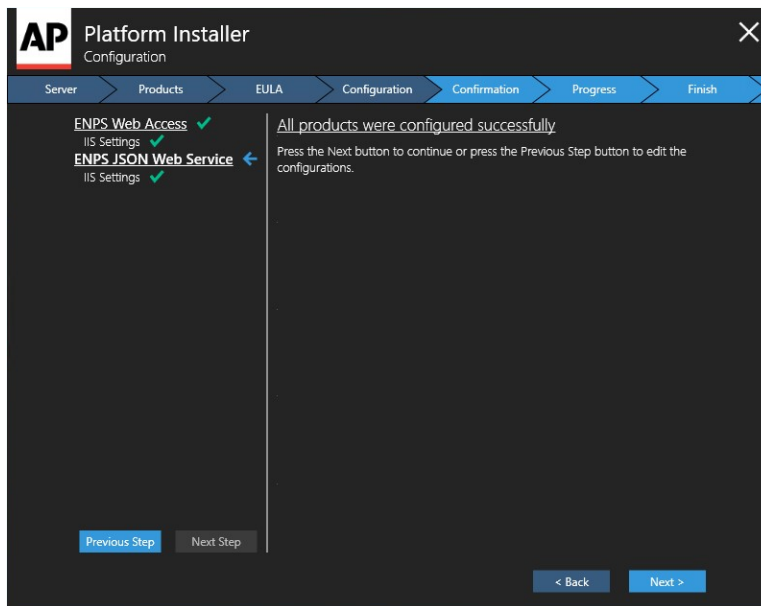


- **IIS Settings.** Select *Default Web Site*.
- **Virtual Directory.** Select *NOMWebservices3JSON*.
- **Application Pool.** Select *NOMWebServiceAppPool*.
- **Central Server Name.** Enter the name of your Central Server. If your enterprise uses only a single Primary-Buddy pair, this is the Primary Server.
- **Central Server Backup Name.** Name or IP address of another ENPS server in your enterprise. This should be an ENPS server local to the site where ENPS Mobile is being installed.

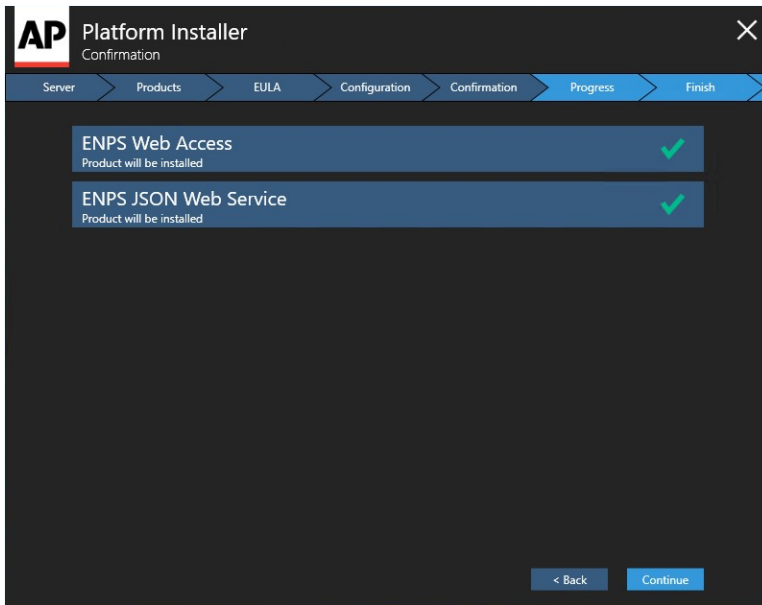
WARNING: Incorrectly setting the **Central Server Name** and **Central Server Backup Name** can cause significant issues in the event of the Central Server failing.

Please contact ENPS Support if you are not sure that you have entered the correct values in these two fields.

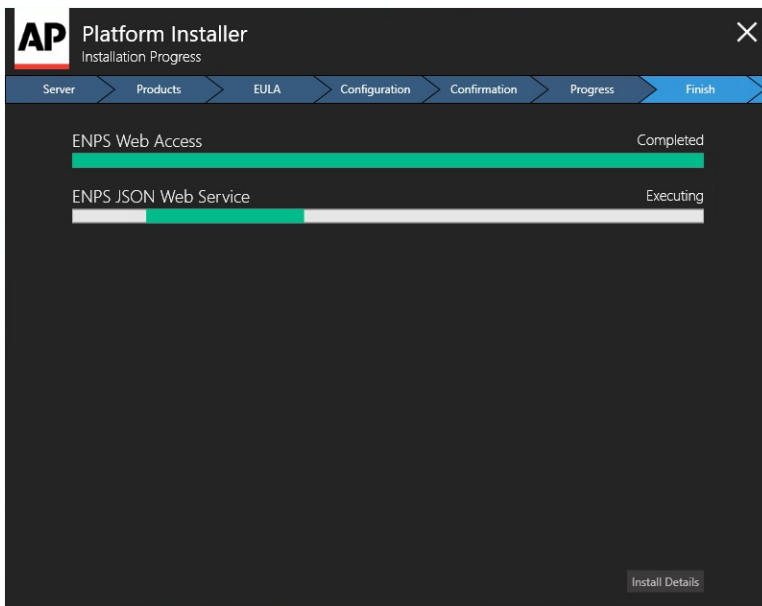
Click the **Next Step** button on the **left** side of the screen to continue.



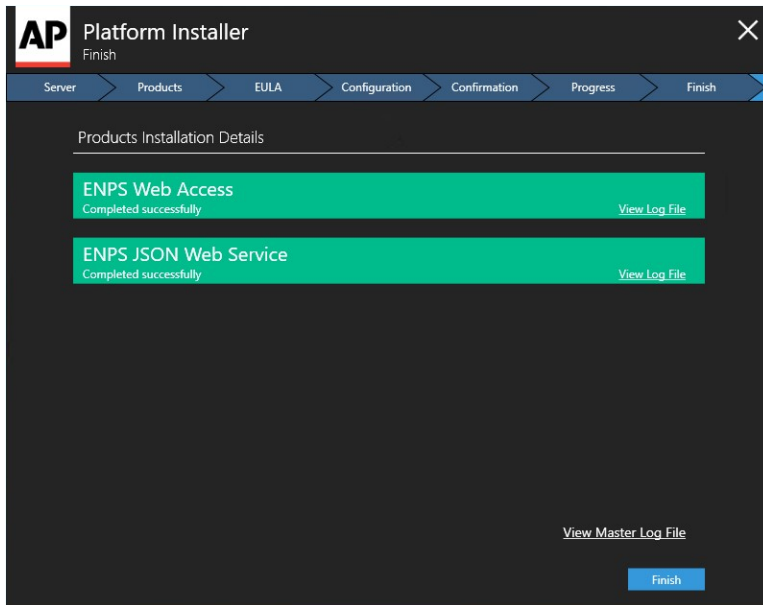
12. The **Confirmation** screen will appear. The **Confirmation** screen will display a list of the products you selected and have configured for installation, indicated by green checkmarks. Click the **Continue** button to begin the installation.



13. The **Installation Progress** screen will appear. Progress bars will be shown for each product you are installing.



14. When the installation is complete, the **Install Details** screen will appear. Select this and you will see the **Finish** screen. The **Finish** screen displays the **Product Installation Details**, which indicate if a product has been installed successfully or if the installation failed. If all products have installed successfully, select the **Finish** button.



Enable Secure Sockets Layer

If you are using Secure Sockets Layer (SSL) and have installed your certificate as described in *Part Three of Appendix A*, now enable SSL for ENPS Mobile.

IMPORTANT: We recommend using SSL. However, if you are not using SSL then you can skip this section and proceed to "Configure Application Pools with Advanced Settings" on the next page.

1. In the **Internet Information Services (IIS) Manager** window, select the name of the server where you installed the certificate.
2. In the left pane of the **Internet Information Services (IIS) Manager** window, double-click on the name of the server where you installed the certificate.
3. Single-click on the plus sign (+) to the left of the word "Sites".
4. Click once on **Default Web Site**.
5. In the **Actions** panel on the right, click **Bindings...**
6. In the **Site Bindings** pop-up window, click the **Add** button.
7. In the **Add Site Binding** window, select the following from the drop-down selections:
 - For Type, select **https**.
 - For IP address, select **All Unassigned**, or the IP address of the site.

- For Port, type **443**.
 - For SSL Certificate, select the SSL certificate you installed.
8. Click the **OK** button.
 9. Select the *https* entry and click **Edit** to open the **Edit Site Binding** popup.
 10. Tick the **Disable Legacy TLS** box, then click **OK** to close the popup.
 11. Close the **Site Bindings** window.
 12. Expand **Default Web Site**. Click on ENPSWEBACCESS3.
 13. In the center panel, double-click on **SSL Settings**.
 14. Check **Require** and click **Apply**.
 15. Close the **Internet Information Services (IIS) Manager**.

You should now be able to access ENPS Mobile services only via secure HTTPS, for example <https://enpsmobile.newsguys.com/enpswebaccess3>). Test to confirm that you cannot log in using an HTTP URL.

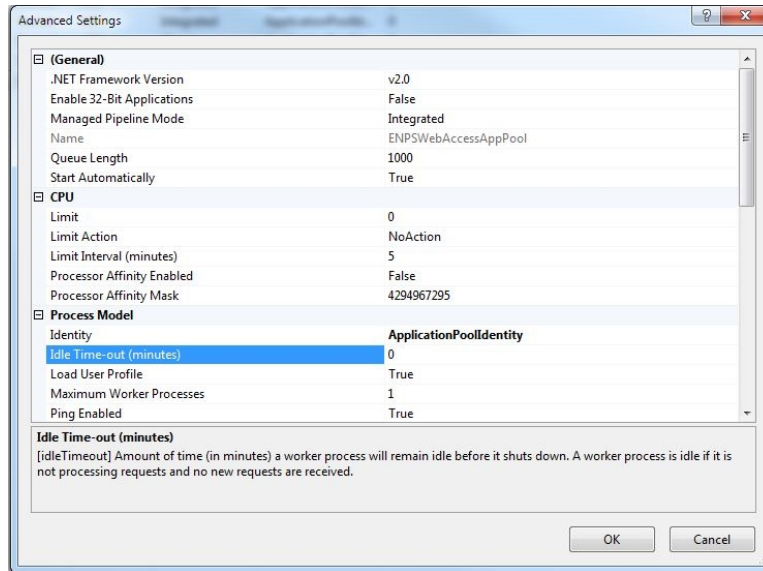
Configure Application Pools with Advanced Settings

Configure the Application Pool with advanced settings.

ENPS Web Access Application Pool Advanced Settings

To configure the ENPS Web Access Application Pool's Advanced Settings, follow these steps:

1. Open **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, expand the server name and select **Application Pools**.
3. In the Features View on the right, select **ENPSWebAccess3AppPool** and right-click on it.
4. Select **Advanced Settings**.
5. In the pop-up window, set the value of **Process Model > Idle Time-out (minutes)** to 0.

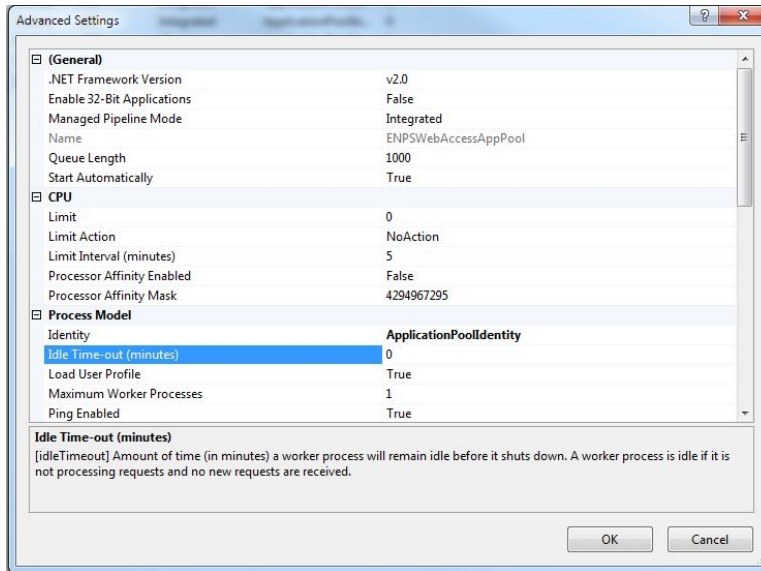


6. Click **OK**.

NOM Web Service Application Pool Advanced Settings

To configure the NOM Web Service Application Pool's Advanced Settings, follow these steps:

1. Open **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, expand the server name and select **Application Pools**.
3. In the Features View on the right, select **NOMWebServiceAppPool** and right-click on it.
4. Select **Advanced Settings**.
5. In the pop-up window, set the value of **Process Model > Idle Time-out (minutes)** to 0.

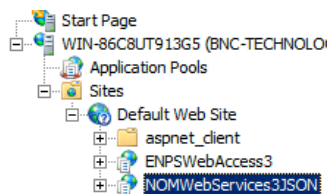


6. Click **OK**.

Configure the Web Service Host

To configure the Web Service Host, follow these steps:

1. Open **Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, expand the server name and select **Sites > Default Web Site** and select **NOMWebservices3JSON**.



3. In the Features View on the right, double-click **Application Settings** to open a list of settings.



4. Edit the settings in the list as appropriate by double-clicking each setting and entering a new value. The table below describes each setting.

Key	Value
CentralServer	Name of your ENPS Central Server. If the Web Service Host cannot resolve the hostname you will need to enter the IP address instead.
CentralServerBackup	Name or IP address of another ENPS server in your enterprise. Ideally, this should be an ENPS server local to the site where ENPS Mobile is being installed.
ClientValidationEnabled*	true
CustomReportsMaximumResultSetLength	10000
CustomReportsPageSize	20
CustomReportsPaging	false
DebugNotifications	false
ISHttpPort*	10505
LocalHttpPort*	10505
LogToENPSEvents	When set to True, logs when users attempt to log in to ENPS. For more information, see the User Login Events section.
PreserveLoginUri*	true
RTUDisconnectTimeout	00:02:00
serviceLoginUserId	ADMINISTRATOR
ServiceRealTime RecordQueueFrequency	Determines how frequently real-time updates for an open object (Rundown, Story, etc.) are sent to the Mobile client. The default value is 5 seconds (00:00:05). Decreasing this value will allow updates to be seen more quickly,

	but will place a higher load on the Mobile client/browser. Increasing this value will do the reverse. You may need to experiment with this to find the setting that best meets your needs.
signalIRMatchQueue	.\private\$\signalIRMatchQueue
TestFlightNotifications	false
UnobtrusiveJavaScriptEnabled*	true
UseWebService*	false
webpages:Enabled*	false
Webpages:Version*	2.0.0.0
WireSummaryLength*	250
*Do not change the default values for these keys unless instructed to do so by ENPS Support.	

5. Test the Web Service Host by opening a browser and opening the following URL (change the URL to `http` if you are not using SSL):

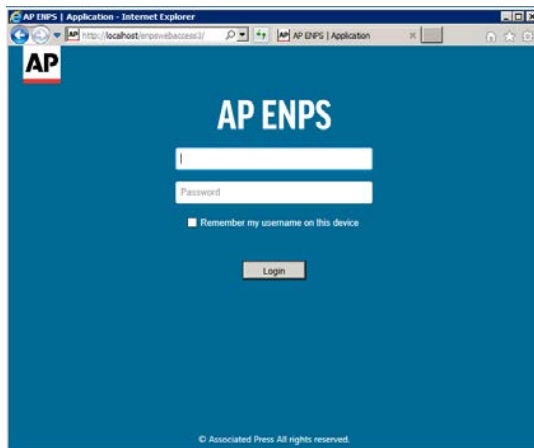
```
https://<NameOfYourMobileServer-
>/NomWebServices3JSON/NomWebService.svc
```

The following page must then load properly for you to continue with the installation. If this page does not load, first verify the installation steps in this chapter. If you continue to have difficulty, refer to the [Troubleshooting](#) steps.



6. Test the Mobile Gateway by opening a browser and opening the following URL (change the URL to http if you are not using SSL):

`https://<NameOfYourMobileServer>/enpswebaccess3`



If this page does not load, first verify the installation steps in this chapter. If you continue to have difficulty, refer to the [troubleshooting](#) steps.

Do not test logging in without first updating the *defaultDomain* and *serviceAddress* settings as noted in the next chapter.

Synchronize ENPS Global Tables in ENPS Mobile

To ensure that any changes made to the ENPS global tables are automatically replicated to ENPS Mobile, an ENPS System Administrator needs to add an entry to the Services table in System Maintenance as follows.

Field	Value
ID	Machine name of the Web Service Host computer.
Description	User-friendly description of the Web Service Host.
Type	<i>WebServiceJSON</i>
URL	https://<NameOfYourMobileServer>/nomwebservice3JSON/nomwebservice.svc

NOTE: The Type column will only contain the option for *WebServiceJSON* if you are using the System Maintenance client included with ENPS 7 or later. If you are accessing System Maintenance via the ENPS version 6 menu system, you may select *WebService*.

Once this step is complete, you will not need to restart IIS on the Mobile Server any time you make a change to one of the ENPS global tables.

Next steps

The Mobile Server is now installed!

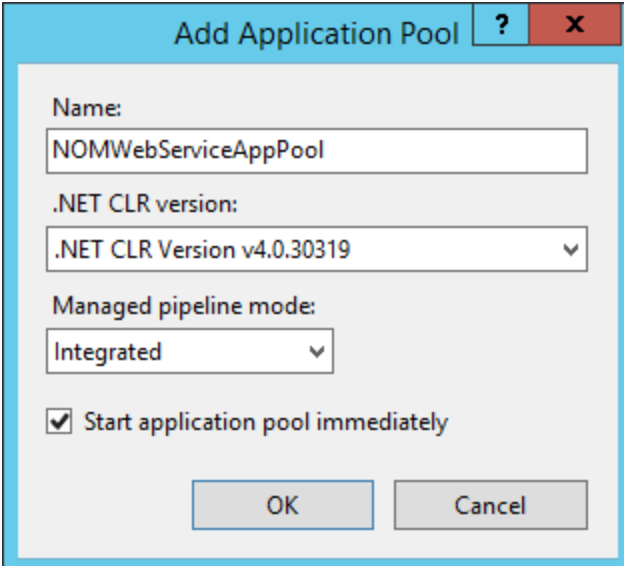
Proceed to the "Configuring ENPS Mobile" on page 75 section to configure settings for the Mobile Gateway.

Installing on Windows Server 2019

1. To configure Role Services:
 - a. Start **Server Manager** and select **Manage**. Select **Add Roles and Features**.
 - b. Ensure that *Role-based or feature-based installation* is selected and click **Next**.
 - c. Ensure that *Select a server from the server pool* is selected and that your Mobile server is highlighted in the window below. Click **Next**.
 - d. Select the following Roles (if not already selected):

NOTE: Be sure to select **Add Features** if the dialog appears.

- File and Storage Services > File and iSCSI Services > File Server
 - Web Server (IIS)
- e. For **Web Server Role (IIS) > Role Services**, select **Management Tools > IIS 6 Management Compatibility** and select the following:
- **IIS 6 Metabase Compatibility**
 - **IIS 6 Management Console**
 - **IIS 6 Scripting Tools** (Click **Add Features**)
 - **IIS 6 WMI Compatibility**
- Click **Next**.
- f. Click **Next**.
- g. For Features, expand **.NET Framework 4.6 Features** and select **ASP.NET 4.6**. Also select **WCF Services > HTTP Activation**. Click **Next**.
- h. Click **Install**.
- i. Click **Close** when installation is complete.
2. In **Server Manager**, select **Tools > Internet Information Services (IIS) Manager**. In the **Connections** pane expand the server name. Right-click on **Application Pools** and select **Add Application Pool**.



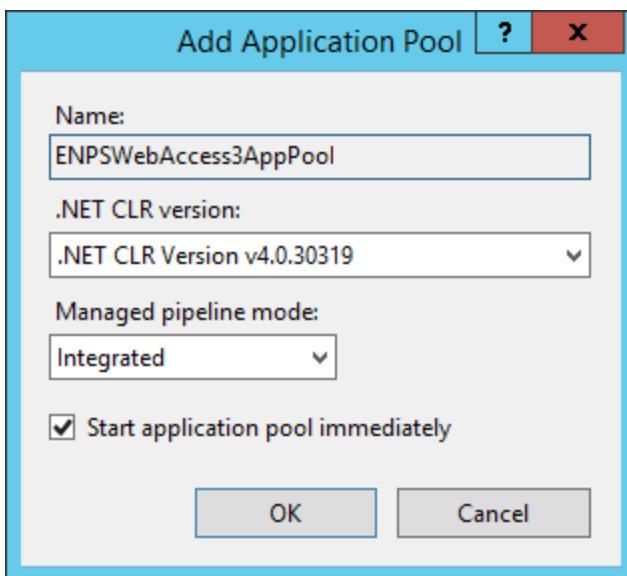
The screenshot shows the "Add Application Pool" dialog box. The title bar includes a question mark icon and a close button (X). The dialog contains the following fields and options:

- Name:** A text box containing "NOMWebServiceAppPool".
- .NET CLR version:** A dropdown menu currently set to ".NET CLR Version v4.0.30319".
- Managed pipeline mode:** A dropdown menu currently set to "Integrated".
- Start application pool immediately**
- Buttons: **OK** and **Cancel**.

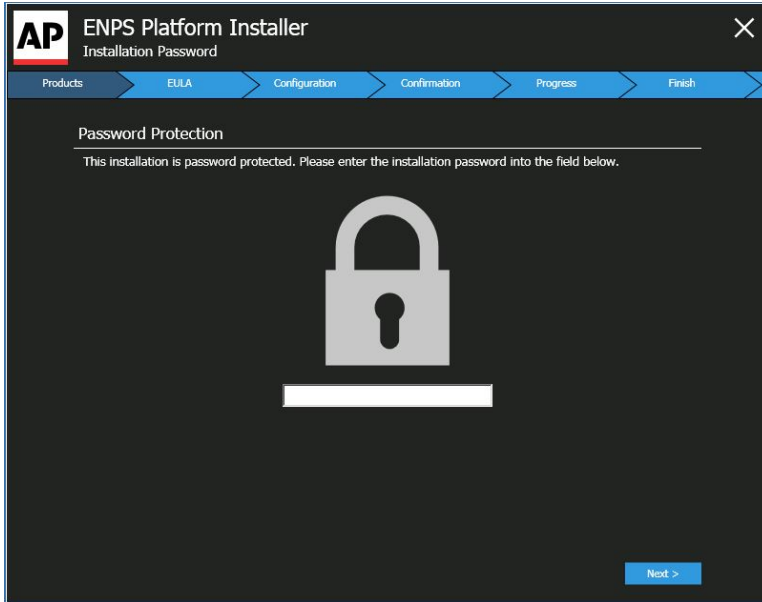
3. In the **Name** field enter "NOMWebServiceAppPool". For **.NET CLR version**, select *.NET CLR Version v4.0.30319*. Click **OK**.

NOTE: If you are installing version 9 on your existing Mobile 2 server, name the AppPool **NOMWebService3AppPool**. This will prevent it from conflicting with your mobile 2 setup which is using "NOMWebServiceAppPool".

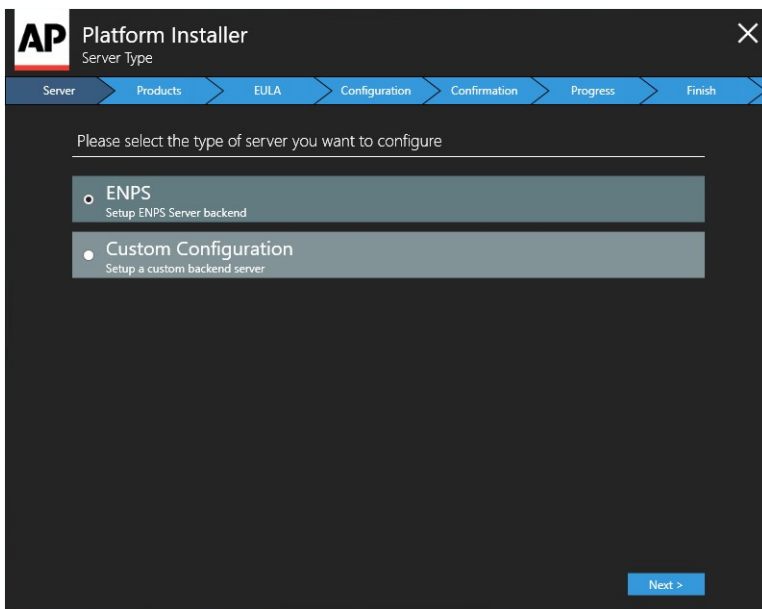
4. Right-click **Application Pools** and select *Add Application Pool* again. In the **Name** field, enter "ENPSWebAccess3AppPool". For the **.NET CLR version**, select *.NET CLR Version v4.0.30319*.



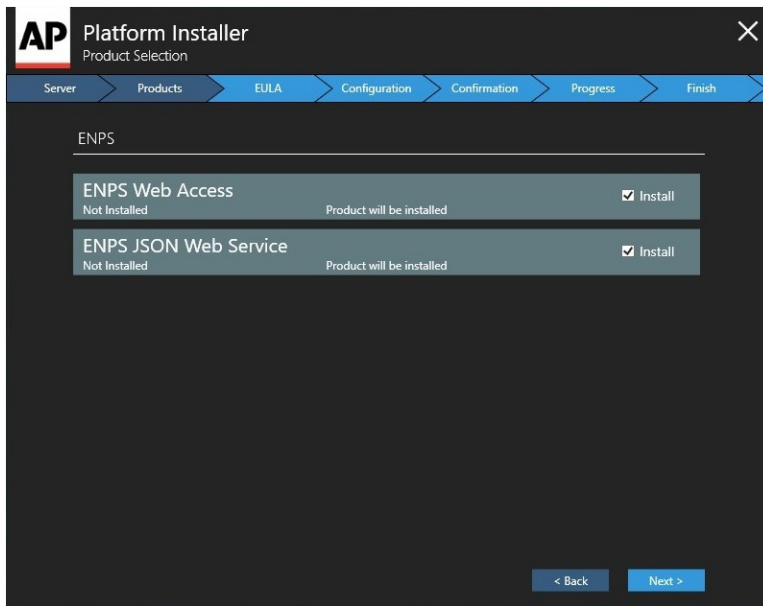
5. Download the ENPS Platform Installer from the ENPS Mobile Download page.
6. **If you are using ENPS 7.3 or later, you may skip this step.** If you are using an ENPS version prior to 7.3, copy the files `G_FIELDDEF` and `G_LANGEN` from the installation package to the `\COMMON\G_SUPPORT` folder on the ENPS Central Server's `WORK` drive. Restart the NOM on the Central Server.
7. Open the ENPS Platform Installer. The **Password Protection** screen appears. Enter your password and click the **Next** button.



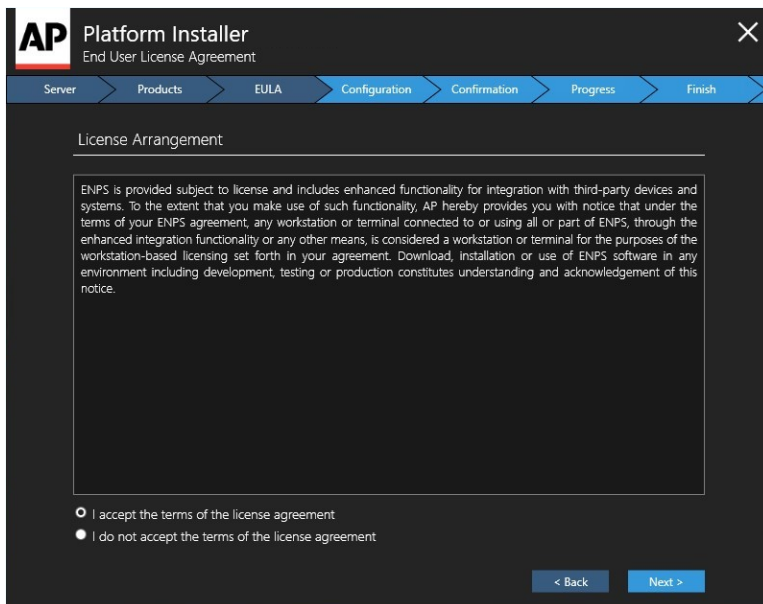
8. In the **Server Type** screen, select *ENPS Web Applications Server* and then click the **Next** button.



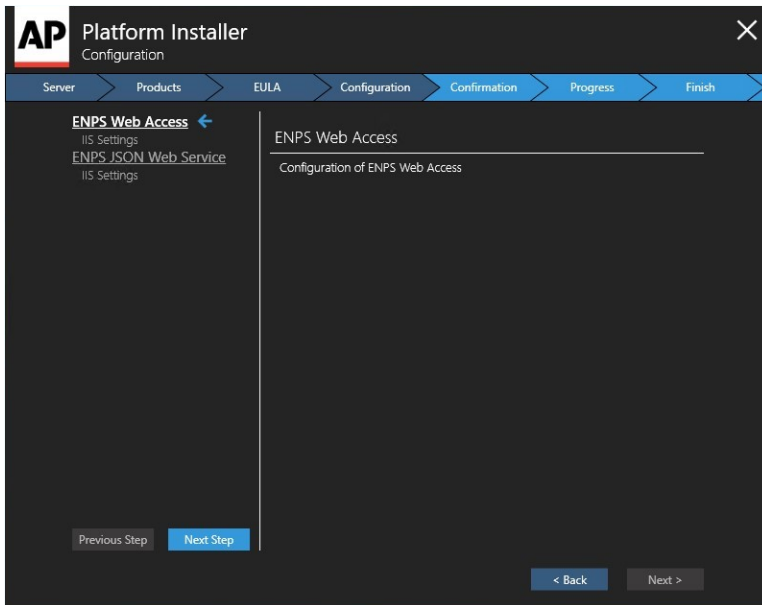
- In the **Product Selection** screen, select the **Install** checkboxes next to **ENPS Web Access** and **ENPS JSON Web Service**, then click the **Next** button.



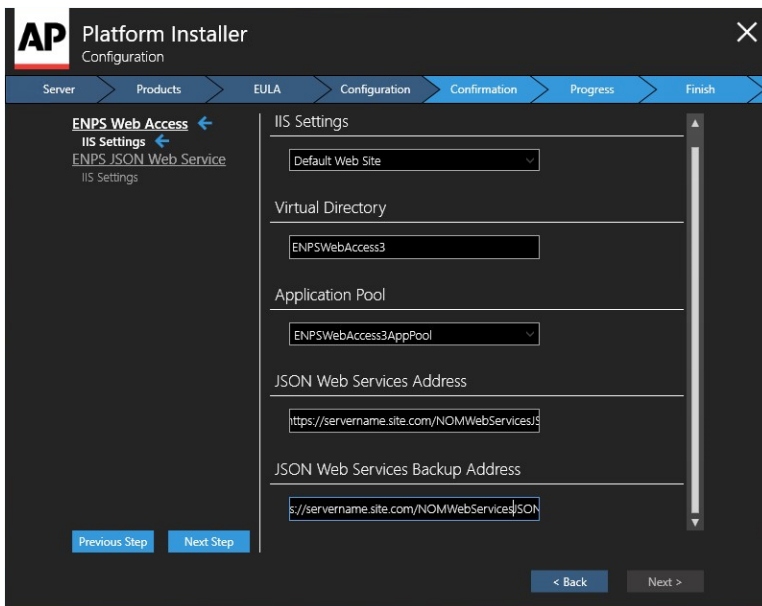
- In the **End User License Agreement** screen, select the radio button for **I accept the terms of the license agreement**, then click the **Next** button.



- The **Configuration** screen appears. In the first configuration screen, you do not need to make any selections. Click the **Next Step** button on the **left** panel of the **Configuration** screen to continue.



12. The **IIS Settings** screen for **ENPS Web Access** will appear. In the **IIS Settings** screen, select the following:

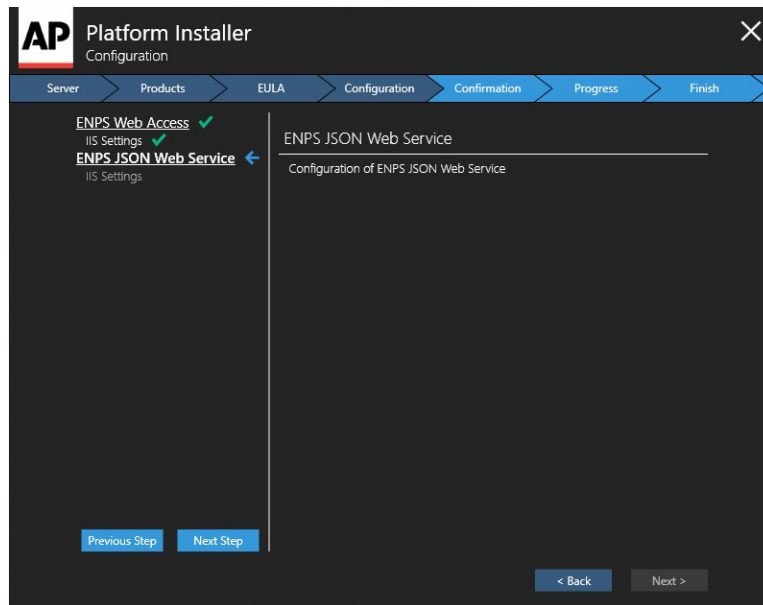


- **IIS Settings.** Select *Default Web Site*.
- **Virtual Directory.** Select *ENPSWebAccess3*.
- **Application Pool.** Select *ENPSWebAccess3AppPool*.
- **JSON Web Services Address.** Enter your server name followed by */NOMWebServices3JSON*. For example, if your JSON Web Services server is

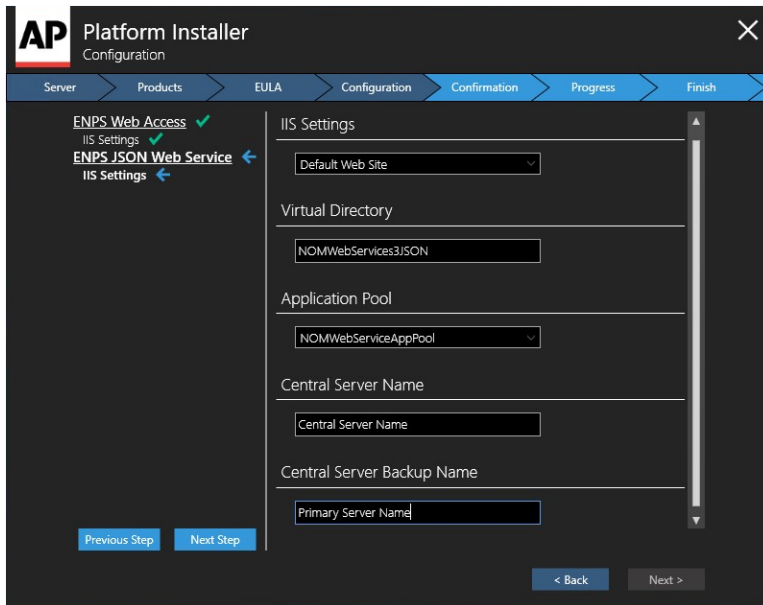
located at <https://servername.site.com>, enter <https://servername.site.com/NOMWebServices3JSON>.

- **JSON Web Services Backup Address.** If the site has a backup JSON address then enter it in this field. Otherwise, enter the same address as the main **JSON Web Services Address** entered above.

Click the **Next Step** button on the **left** side of the screen to continue.



13. The **IIS Settings** screen for **ENPS JSON Web Service** will appear. In the **IIS Settings** screen, select the following:

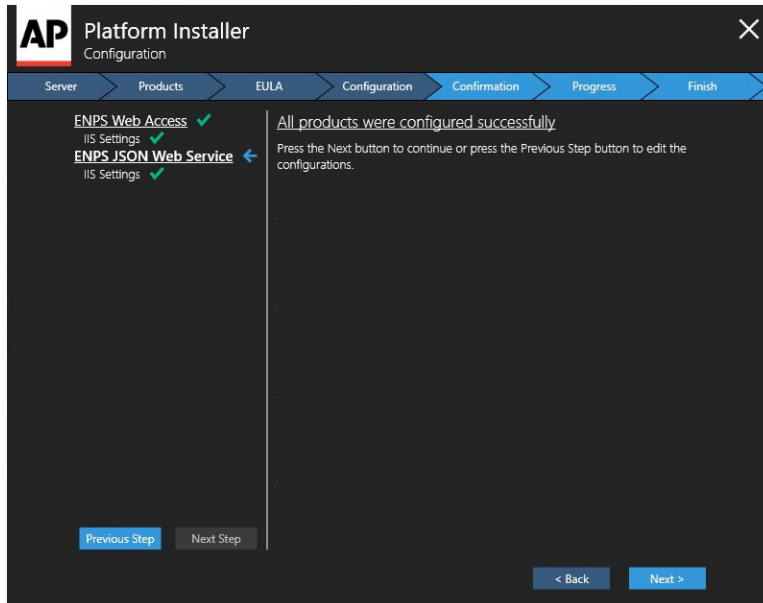


- **IIS Settings.** Select *Default Web Site*.
- **Virtual Directory.** Select *NOMWebservices3JSON*.
- **Application Pool.** Select *NOMWebServiceAppPool*.
- **Central Server Name.** Enter the name of your Central Server. If your enterprise uses only a single Primary-Buddy pair, this is the Primary Server.
- **Central Server Backup Name.** Name or IP address of another ENPS server in your enterprise. This should be an ENPS server local to the site where ENPS Mobile is being installed.

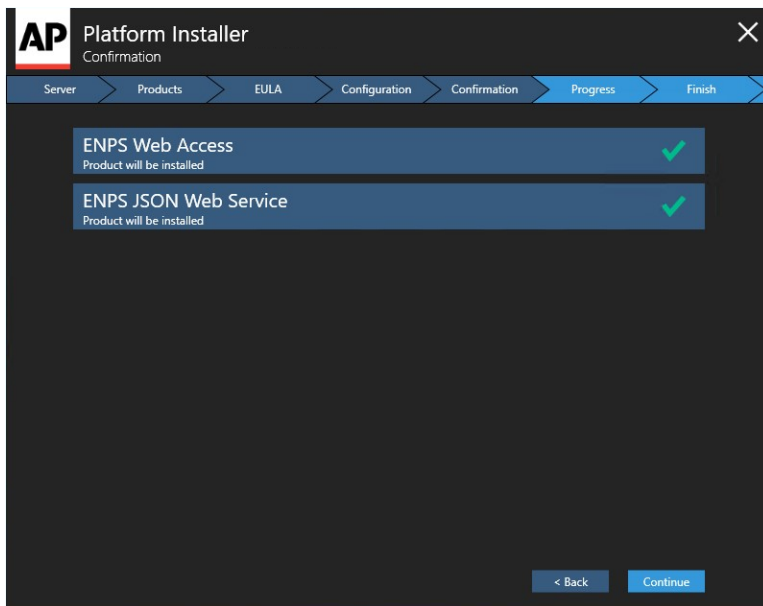
WARNING: Incorrectly setting the **Central Server Name** and **Central Server Backup Name** can cause significant issues in the event of the Central Server failing.

Please contact ENPS Support if you are not sure that you have entered the correct values in these two fields.

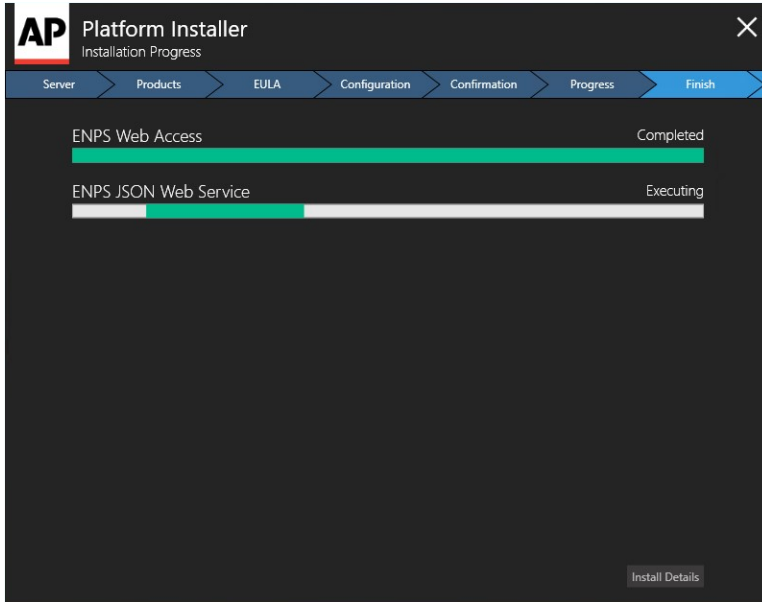
Click the **Next Step** button on the **left** side of the screen to continue.



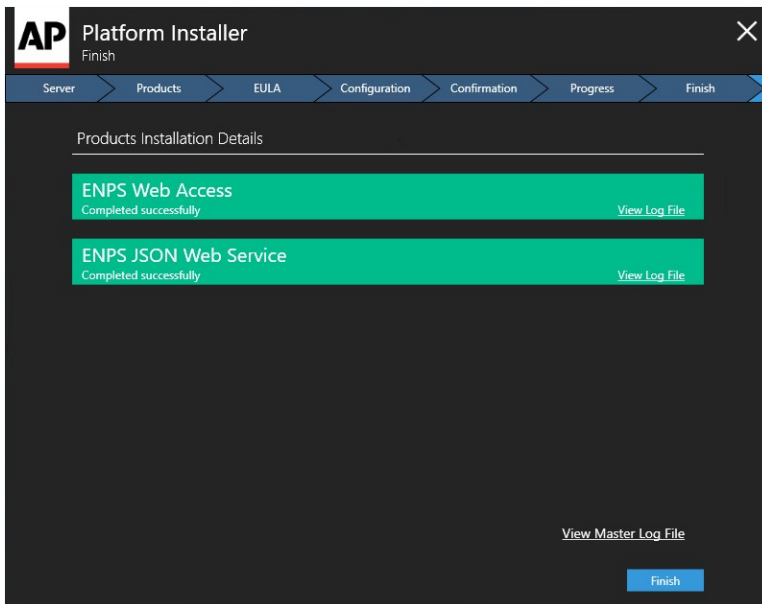
- The **Confirmation** screen will appear. The **Confirmation** screen will display a list of the products you selected and have configured for installation, indicated by green checkmarks. Click the **Continue** button to begin the installation.



- The **Installation Progress** screen will appear. Progress bars will be shown for each product you are installing.

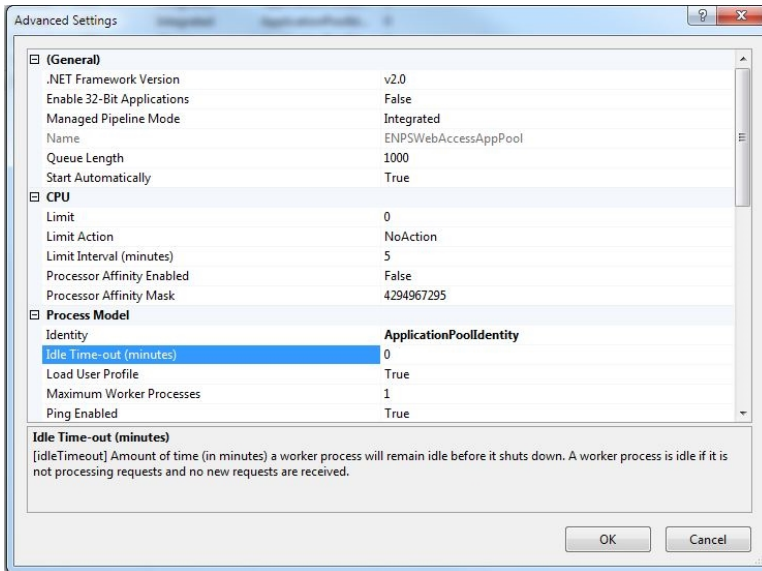


- When the installation is complete, the **Install Details** screen will appear. Select this and you will see the **Finish** screen. The **Finish** screen displays the **Product Installation Details**, which indicate if a product has been installed successfully or if the installation failed. If all products have installed successfully, select the **Finish** button.



- If you are using SSL and have installed your certificate (as described in [Part Three of Appendix A](#)), enable SSL for ENPS Mobile. If you are not using SSL, you can skip to step 18, but note that this is **NOT** recommended.

- a. In the **Internet Information Services (IIS) Manager** window, select the name of the server where you installed the certificate.
 - b. In the left pane of the **Internet Information Services (IIS) Manager** window, double-click on the name of the server where you installed the certificate.
 - c. Single-click on the plus sign (+) to the left of the word "Sites".
 - d. Click once on **Default Web Site**.
 - e. In the **Actions** panel on the right, click **Bindings...**
 - f. In the **Site Bindings** pop-up window, click the **Add** button.
 - g. In the **Add Site Binding** window, select the following from the drop-down selections:
 - For Type, select **https**.
 - For IP address, select **All Unassigned**, or the IP address of the site.
 - For Port, type **443**.
 - For SSL Certificate, select the SSL certificate you installed.
 - h. Click the **OK** button.
 - i. Close the **Site Bindings** window.
 - j. Expand **Default Web Site**. Click on `ENPSWEBACCESS3`.
 - k. In the center panel, double-click on **SSL Settings**.
 - l. Check **Require** and click **Apply**.
 - m. Close the **Internet Information Services (IIS) Manager**.
 - n. You should now be able to access ENPS Mobile services **only** via secure HTTPS (ex: `https://enpsmobile.newsguys.com/enpswebaccess3`). Test to confirm.
18. Edit the Application Pool Advanced Settings:
- a. Open **Internet Information Services (IIS) Manager**.
 - b. In the **Connections** pane, expand the server name and select **Application Pools**.
19. In the Features View on the right, select **ENPSWebAccess3AppPool** and right-click on it.
- a. Select **Advanced Settings**.
 - b. In the pop-up window, find **Idle Time-out (minutes)** and change the value in the right column to 0.

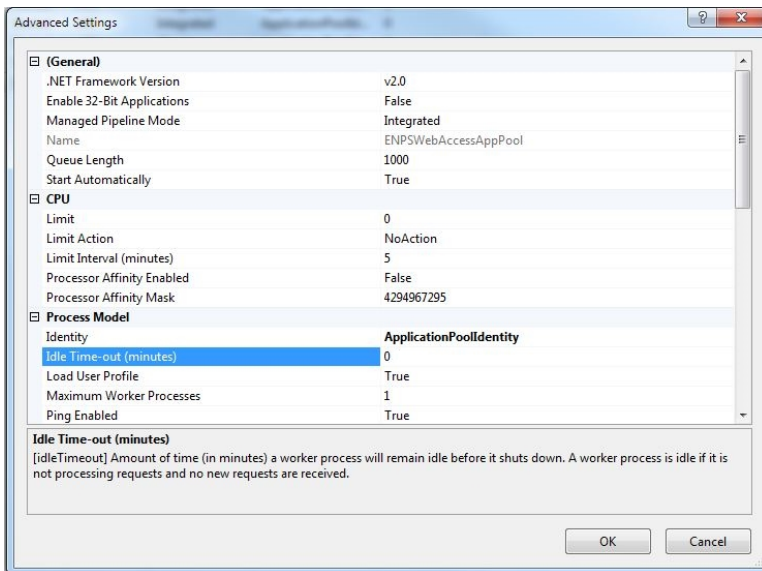


20. Click **OK**.

21. In the Features View on the right, select **NOMWebServiceAppPool** and right-click on it.

a. Select **Advanced Settings**.

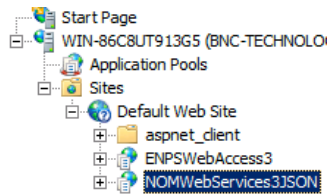
b. In the pop-up window, find **Idle Time-out (minutes)** and change the value in the right column to 0.



22. Click **OK**.

23. Edit the configuration settings for the Web Service Host:

- a. Open **Internet Information Services (IIS) Manager**.
- b. In the **Connections** pane, expand the server name and select **Sites > Default Web Site** and select **NOMWebservices3JSON**.



Application
Settings

24. In the Features View on the right, double-click **Application Settings**. The table below describes the settings on this screen. To edit a setting, double-click it.

Key	Value
CentralServer	Name of your ENPS Central Server. If the Web Service Host cannot resolve the hostname you will need to enter the IP address instead.
CentralServerBackup	Name or IP address of another ENPS server in your enterprise. Ideally, this should be an ENPS server local to the site where ENPS Mobile is being installed.
ClientValidationEnabled*	True
ISHttpPort*	10505
LocalHttpPort*	10505
LogToENPSEvents	When set to True, logs when users attempt to log in to ENPS. For more information, see the User Login Events section.
PreserveLoginUri*	True

serviceAddress	<p>Path to the Web Service Host. The default address MUST be changed to the actual name of the server.</p> <p>If you are using SSL, "CHANGEME" should be changed to the URL in the SSL certificate. If you are not using SSL, change the https to http.</p> <p>https://CHANGEME/NOMW ebservices3JSON</p>
ServiceRealTimeRecordQueueFrequency	<p>Determines how frequently real-time updates for an open object (Rundown, Story, etc.) are sent to the Mobile client. The default value is 5 seconds (00:00:05).</p> <p>Decreasing this value will allow updates to be seen more quickly, but will place a higher load on the Mobile client/browser. Increasing this value will do the reverse. You may need to experiment with this to find the setting that best meets your needs.</p>
UnobtrusiveJavaScriptEnabled*	True
UseWebService*	False
webpages:Enabled*	False
Webpages:Version*	2.0.0.0
WireSummaryLength*	250
*Do not change the default values for these keys unless instructed to do so by ENPS Support.	

25. Test the Web Service Host by opening a browser and opening the following URL (change to "http" if you are not using SSL):

```
https://<NameOfYourMobileServer>/NomWebServices3JSON/No
mWebService.svc
```

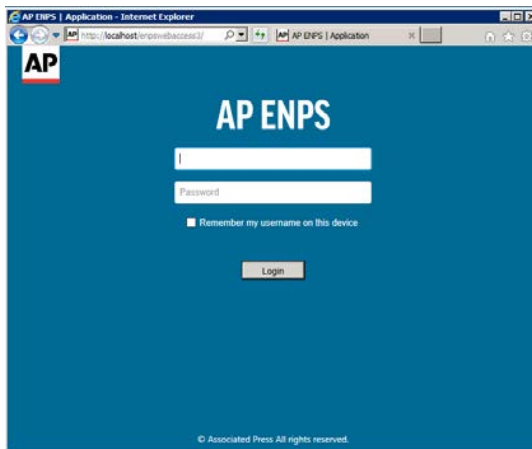
You should see the following page:



This page must load properly for you to continue with the installation. If this page does not load, first verify the installation steps in this chapter. If you continue to have difficulty, refer to the [troubleshooting](#) steps.

Test the Mobile Gateway by opening a browser and opening the following URL (change to "http" if you are not using SSL):

`https://<NameOfYourMobileServer>/enpswebaccess3`



If this page does not load, first verify the installation steps in this chapter. If you continue to have difficulty, refer to the [troubleshooting](#) steps.

Do not test logging in without first updating the *defaultDomain* and *serviceAddress* settings as noted in the next chapter.

26. To ensure that any changes made to the ENPS global tables are automatically replicated to ENPS Mobile, an ENPS System Administrator needs to add an entry to the Services table in System Maintenance as follows:

Field	Value
ID	Machine name of the Web Service Host computer.
Description	User-friendly description of the Web Service Host.
Type	<i>WebServiceJSON</i>
URL	https://<NameOfYourMobileServer>/nomwebservice3JSON/nomwebservice.svc

NOTE: The Type column will only contain the option for *WebServiceJSON* if you are using the System Maintenance client included with ENPS 7 or later. If you are accessing System Maintenance via the ENPS version 6 menu system, you may select *WebService*.

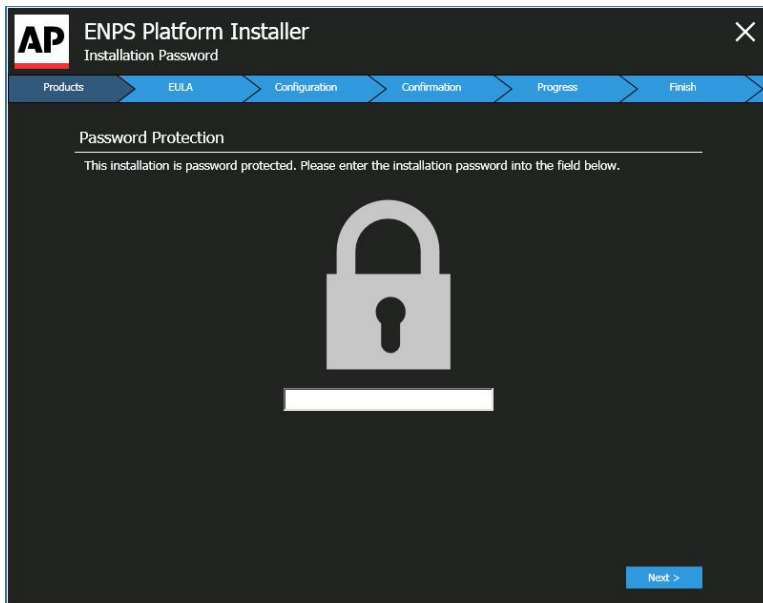
Once this step is complete, you will not need to restart IIS on the Mobile Server any time you make a change to one of the ENPS global tables.

27. Proceed to the next section to configure settings for the Mobile Gateway.

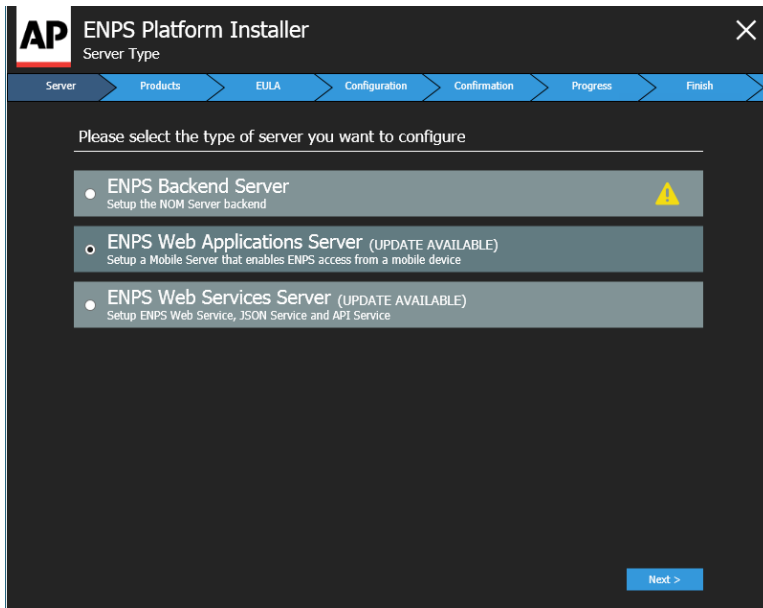
Upgrading on Windows Server 2019

1. Download the ENPS Platform Installer from the ENPS Mobile Download page.
2. Open the ENPS Platform Installer. The **Password Protection** screen appears. Enter

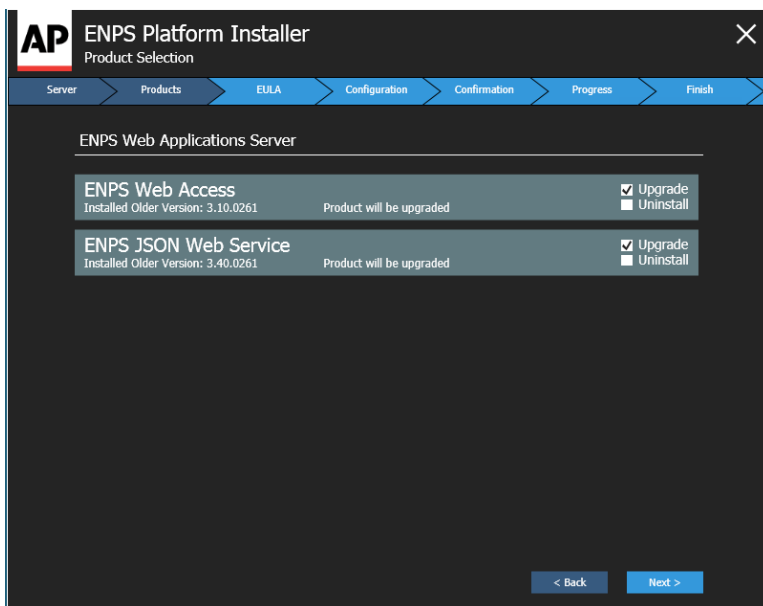
your password and click the **Next** button.



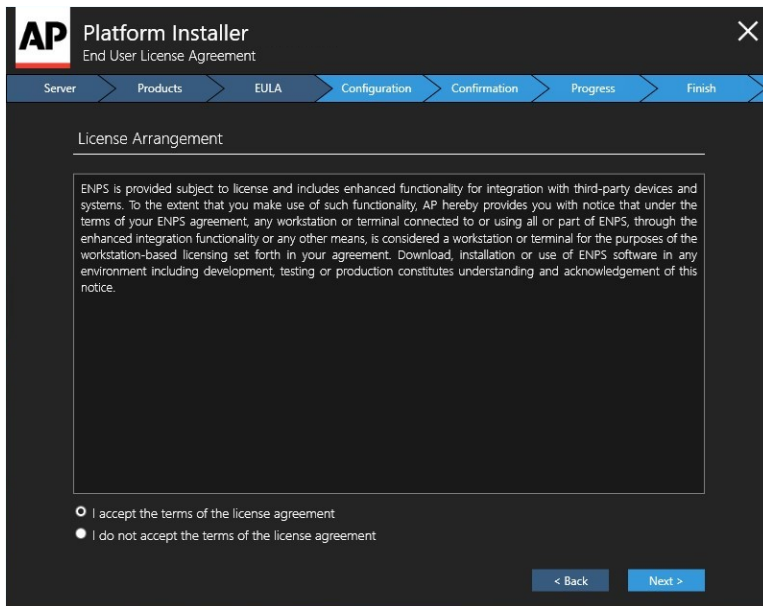
3. In the **Server Type** screen, select **ENPS Web Applications Server (UPDATE AVAILABLE)** and then click the **Next** button.



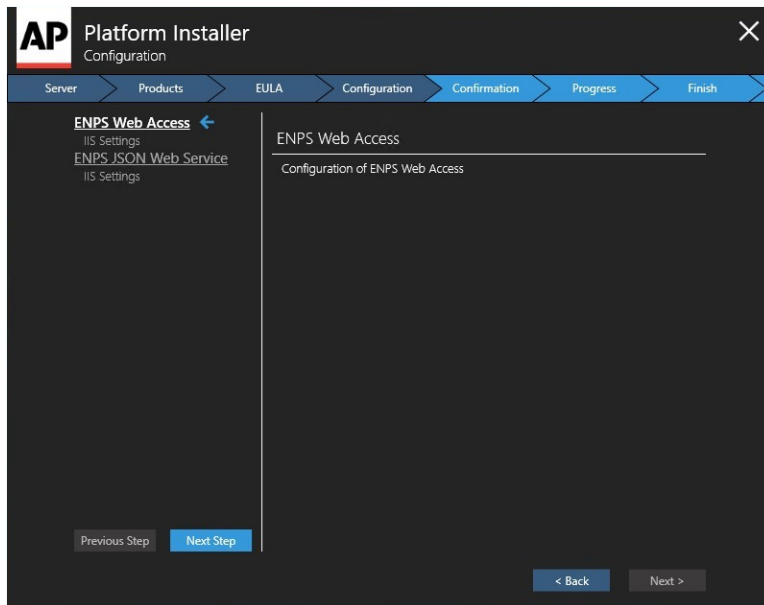
4. In the **Product Selection** screen, select the **Upgrade** checkboxes next to **ENPS Web Access** and **ENPS JSON Web Service**, then click the **Next** button.



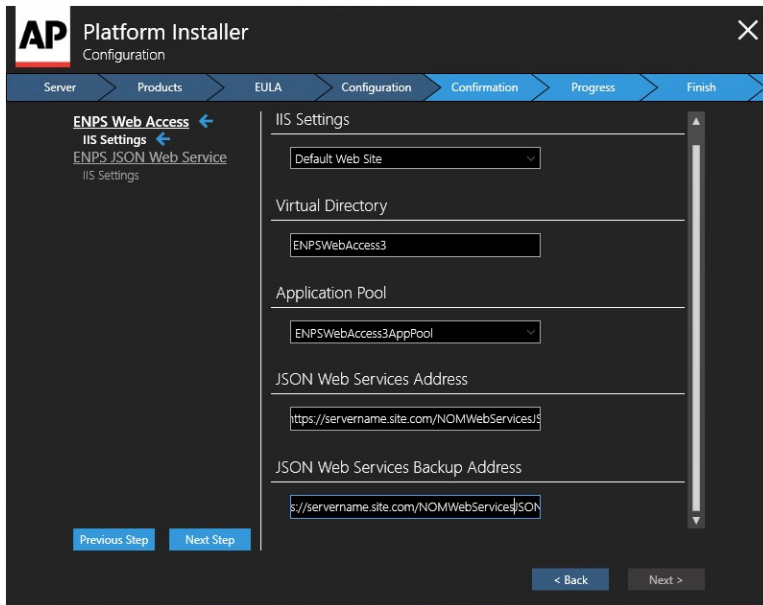
5. In the **End User License Agreement** screen, select the radio button for *I accept the terms of the license agreement*, then click the **Next** button.



6. The **Configuration** screen appears. In the first configuration screen, you do not need to make any selections. Click the **Next Step** button on the left panel of the **Configuration** screen to continue.



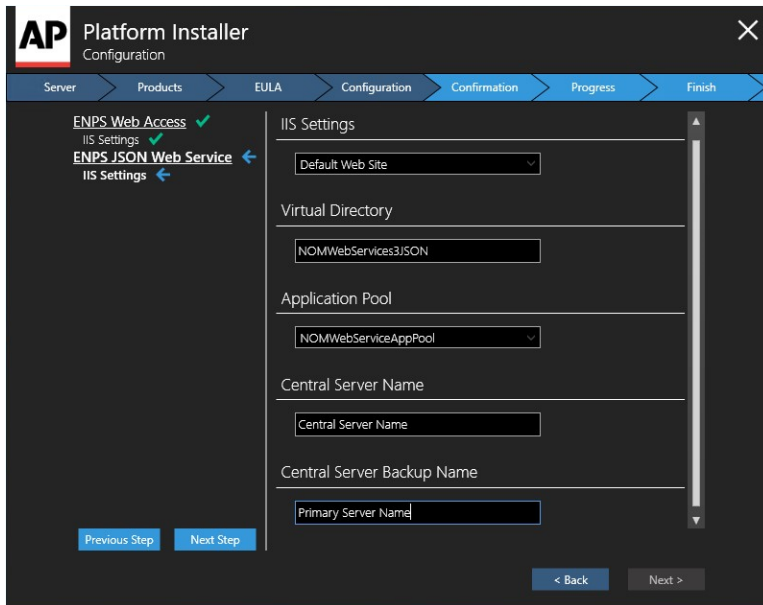
7. The **IIS Settings** screen for **ENPS Web Access** will appear. In the **IIS Settings** screen, select the following:



- **IIS Settings.** Select *Default Web Site*.
- **Virtual Directory.** Select *ENPSWebAccess3*.
- **Application Pool.** Select *ENPSWebAccess3AppPool*.
- **JSON Web Services Address.** Enter your server name followed by */NOMWebServices3JSON*. For example, if your JSON Web Services server is located at `https://servername.site.com`, enter `https://servername.site.com/NOMWebServices3JSON`.
- **JSON Web Services Backup Address.** If the site has a backup JSON address then enter it in this field. Otherwise, enter the same address as the main **JSON Web Services Address** entered above.

Click the **Next Step** button on the **left** side of the screen to continue.

8. The **IIS Settings** screen for **ENPS JSON Web Service** will appear. In the **IIS Settings** screen, select the following:



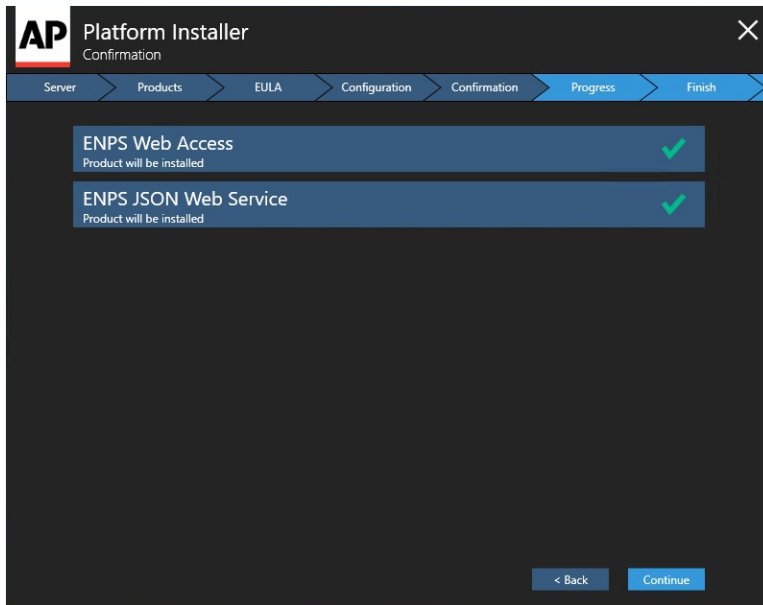
- **IIS Settings.** Select *Default Web Site*.
- **Virtual Directory.** Select *NOMWebservices3JSON*.
- **Application Pool.** Select *NOMWebServiceAppPool*.
- **Central Server Name.** Enter the name of your Central Server. If your enterprise uses only a single Primary-Buddy pair, this is the Primary Server.
- **Central Server Backup Name.** Name or IP address of another ENPS server in your enterprise. This should be an ENPS server local to the site where ENPS Mobile is being installed.

WARNING: Incorrectly setting the **Central Server Name** and **Central Server Backup Name** can cause significant issues in the event of the Central Server failing.

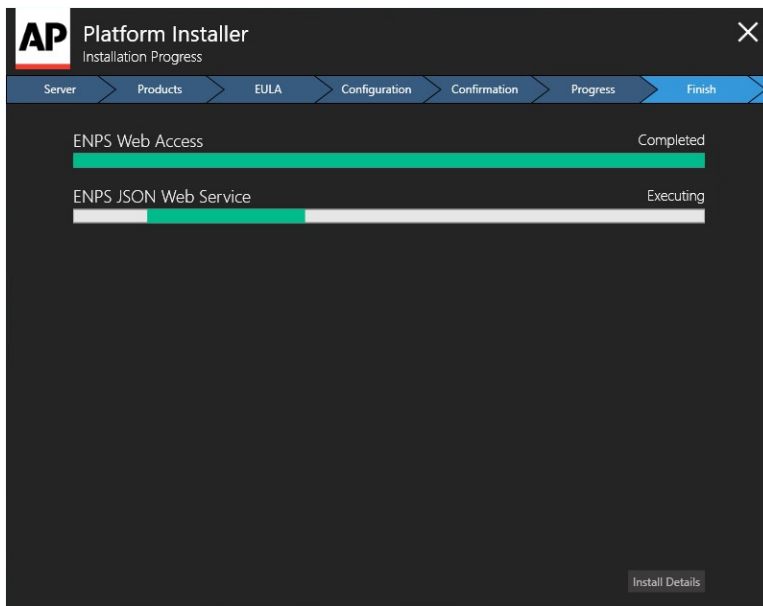
Please contact ENPS Support if you are not sure that you have entered the correct values in these two fields.

Click the **Next Step** button on the **left** side of the screen to continue.

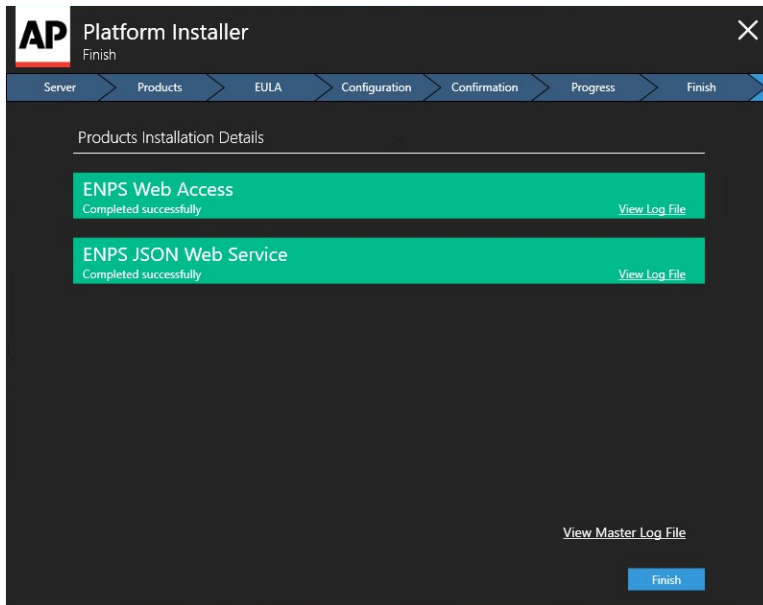
9. The **Confirmation** screen will appear. The **Confirmation** screen will display a list of the products you selected and have configured for an upgrade, indicated by green checkmarks. Click the **Continue** button to begin the upgrade.



10. The **Installation Progress** screen will appear. Progress bars will be shown for each product you are upgrading.



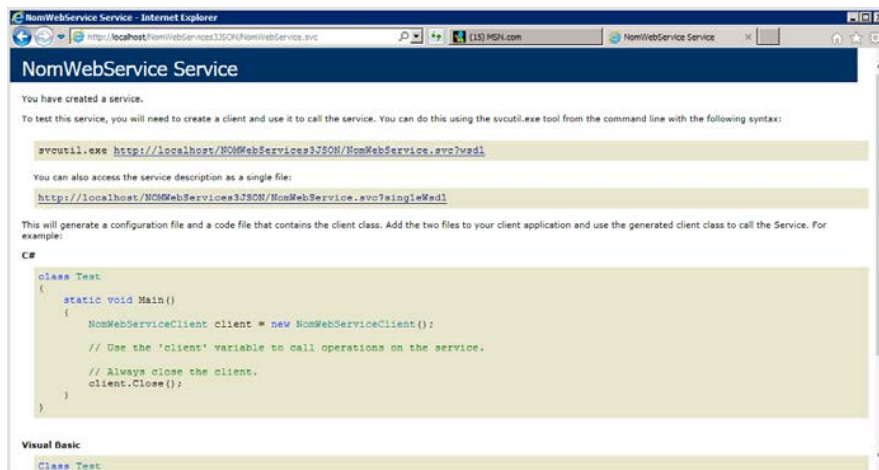
11. When the upgrade is complete, click the **Install Details** button and the **Finish** screen will appear. The **Finish** screen displays **Product Installation Details**, which indicate if a product has been upgraded successfully or if the upgrade failed. If all products have upgraded successfully, select the **Finish** button.



12. It is recommended that you double-check your **Application Settings** at this point. You can do so by referring to *numbers 10, 11 and 18–22* in the **Installing on...** section.
13. Test the Web Service Host by opening a browser and opening the following URL (change to "http" if you are not using SSL):

`https://<NameOfYourMobileServer>/NomWebServices3JSON/NomWebService.svc`

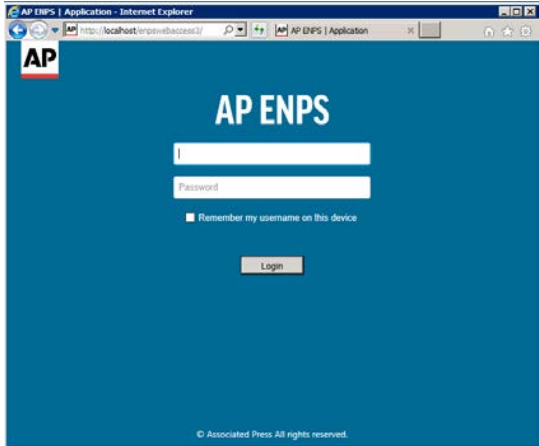
You should see the following page:



This page must load properly for you to continue with the installation. If this page does not load, first verify the installation steps in this chapter. If you continue to have difficulty, refer to the *troubleshooting* steps.

Test the Mobile Gateway by opening a browser and opening the following URL (change to "http" if you are not using SSL):

`https://<NameOfYourMobileServer>/enpswebaccess3`



If this page does not load, first verify the installation steps in this chapter. If you continue to have difficulty, refer to the [troubleshooting](#) steps.

Do not test logging in without first updating the *defaultDomain* and *serviceAddress* settings as noted in the next chapter.

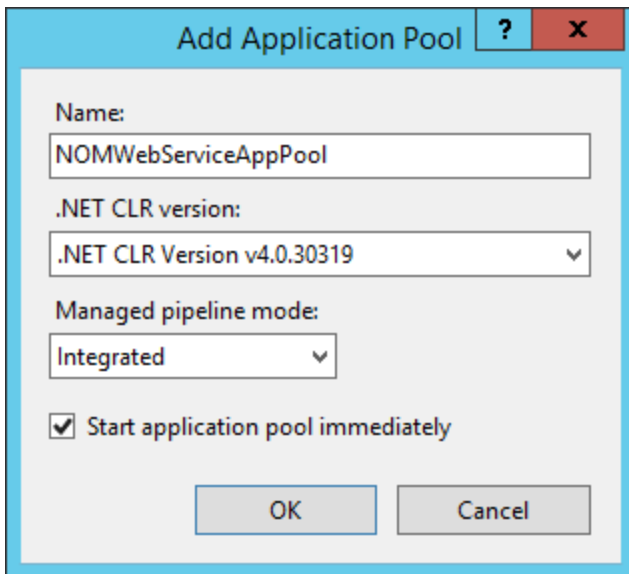
Installing on Windows Server 2016

1. To configure Role Services:
 - a. Start **Server Manager** and select **Manage**. Select **Add Roles and Features**.
 - b. Ensure that *Role-based or feature-based installation* is selected and click **Next**.
 - c. Ensure that *Select a server from the server pool* is selected and that your Mobile server is highlighted in the window below. Click **Next**.
 - d. Select the following Roles (if not already selected):

NOTE: Be sure to select **Add Features** if the dialog appears.

- **File and Storage Services > File and iSCSI Services > File Server**
- **Web Server (IIS)**

- e. For Features, expand **.NET Framework 4.6 Features** and select **ASP.NET 4.6**. Also select **WCF Services > HTTP Activation**. Click **Next**.
 - f. Click **Next**.
 - g. For **Web Server Role (IIS) > Role Services**, select **Management Tools > IIS 6 Management Compatibility** and select the following:
 - **IIS 6 Metabase Compatibility**
 - **IIS 6 Management Console**
 - **IIS 6 Scripting Tools** (Click **Add Features**)
 - **IIS 6 WMI Compatibility**Click **Next**.
 - i. Click **Install**.
 - j. Click **Close** when installation is complete.
2. In **Server Manager**, select **Tools > Internet Information Services (IIS) Manager**. In the **Connections** pane expand the server name. Right-click on **Application Pools** and select **Add Application Pool**.

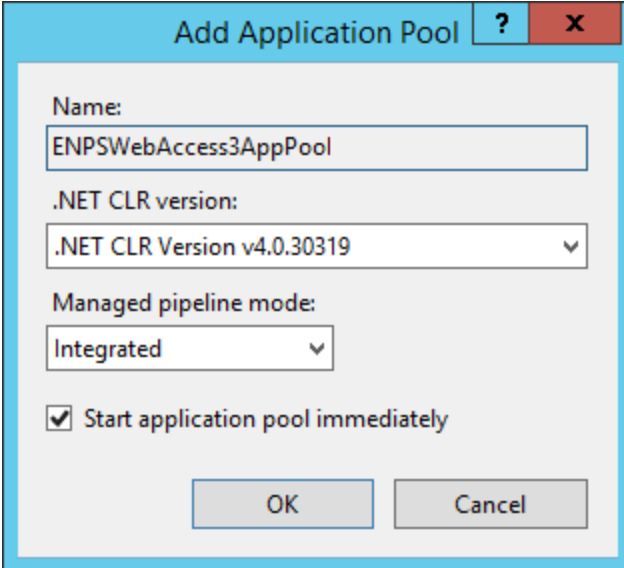


3. In the **Name** field enter "NOMWebServiceAppPool". For **.NET CLR version**, select **.NET CLR Version v4.0.30319**. Click **OK**.

• **NOTE:** If you are installing version 9 on your existing Mobile 2 server, name

the AppPool **NOMWebService3AppPool**. This will prevent it from conflicting with your mobile 2 setup which is using "NOMWebServiceAppPool".

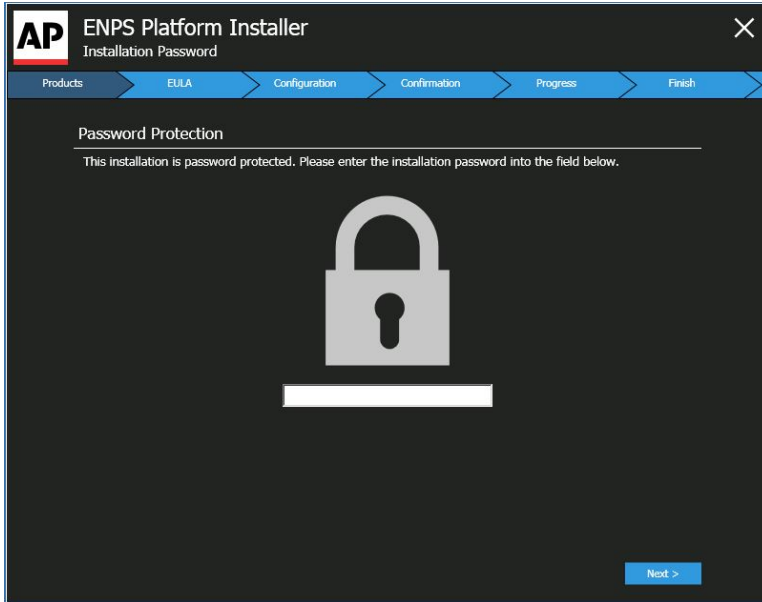
- Right-click **Application Pools** and select *Add Application Pool* again. In the **Name** field, enter "ENPSWebAccess3AppPool". For the **.NET CLR version**, select *.NET CLR Version v4.0.30319*.



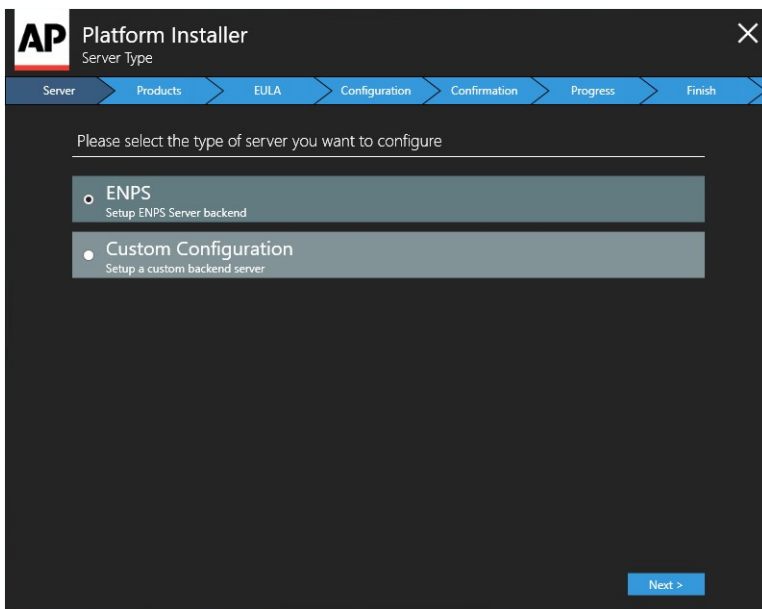
The screenshot shows a dialog box titled "Add Application Pool". It has a light blue header with a question mark and a close button. The main area is white with a light blue border. It contains the following fields and controls:

- Name:** A text box containing "ENPSWebAccess3AppPool".
- .NET CLR version:** A dropdown menu showing ".NET CLR Version v4.0.30319".
- Managed pipeline mode:** A dropdown menu showing "Integrated".
- Start application pool immediately**
- At the bottom, there are two buttons: "OK" and "Cancel".

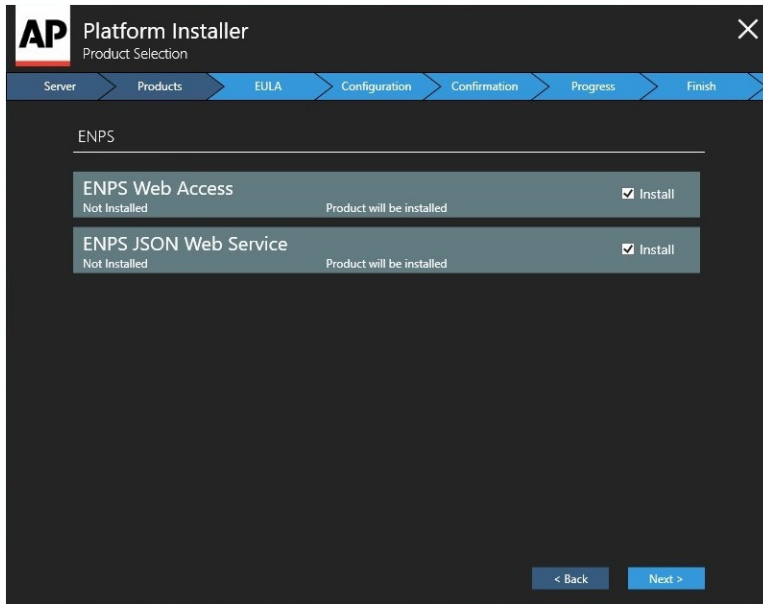
- Download the ENPS Platform Installer from the ENPS Mobile Download page.
- If you are using ENPS 7.3 or later, you may skip this step.* If you are using an ENPS version prior to 7.3, copy the files `G_FIELDDEF` and `G_LANGEN` from the installation package to the `\COMMON\G_SUPPORT` folder on the ENPS Central Server's `WORK` drive. Restart the NOM on the Central Server.
- Open the ENPS Platform Installer. The **Password Protection** screen appears. Enter your password and click the **Next** button.



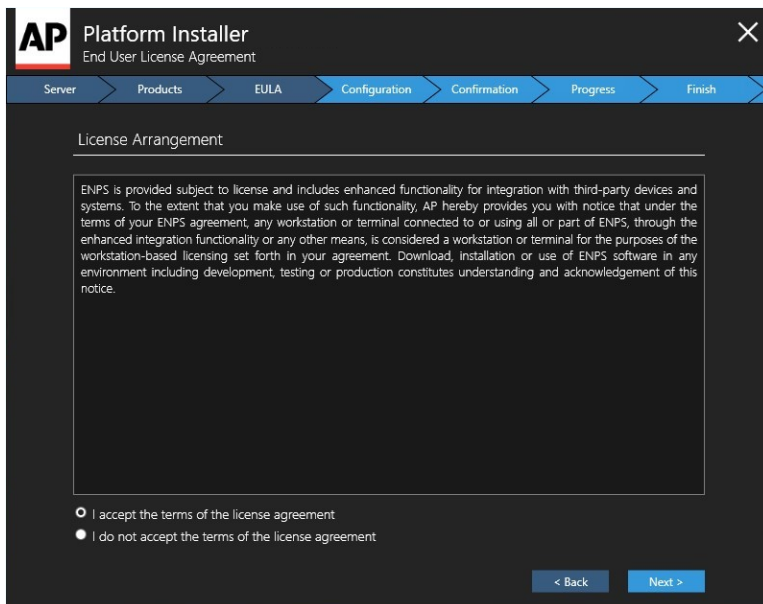
8. In the **Server Type** screen, select *ENPS Web Applications Server* and then click the **Next** button.



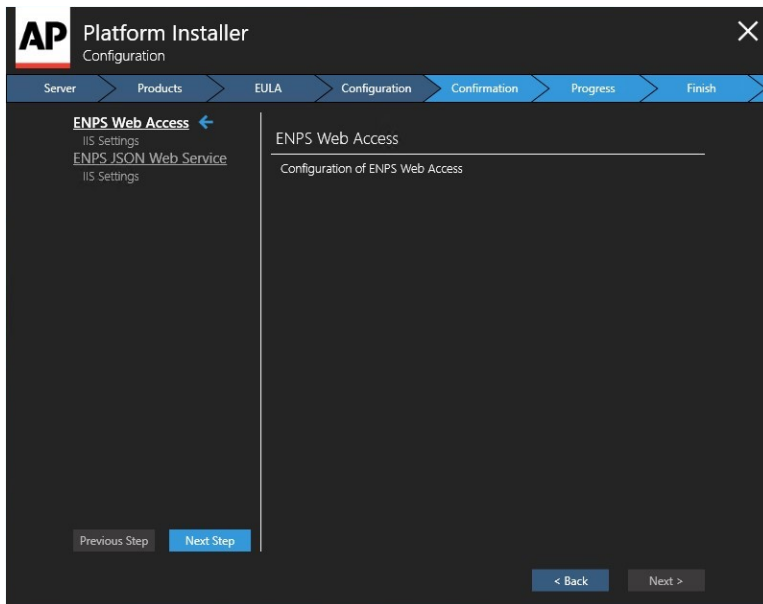
9. In the **Product Selection** screen, select the **Install** checkboxes next to **ENPS Web Access** and **ENPS JSON Web Service**, then click the **Next** button.



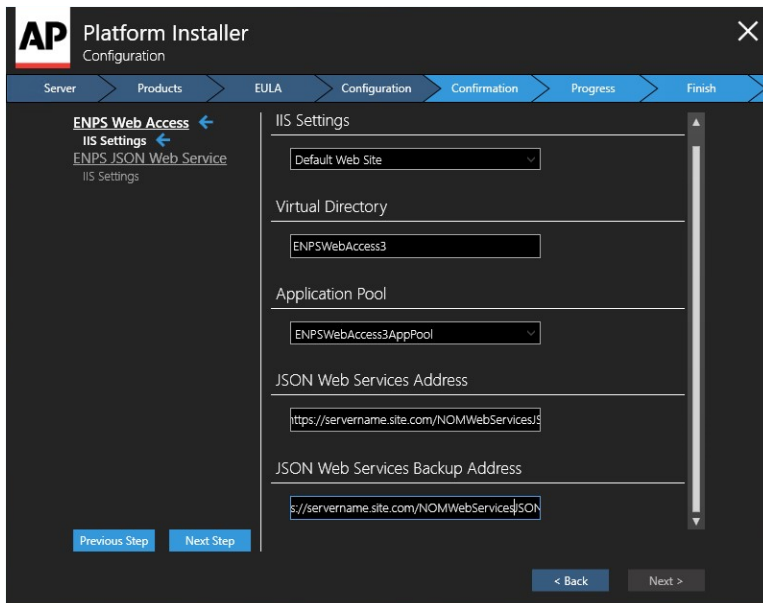
10. In the **End User License Agreement** screen, select the radio button for **I accept the terms of the license agreement**, then click the **Next** button.



11. The **Configuration** screen appears. In the first configuration screen, you do not need to make any selections. Click the **Next Step** button on the **left** panel of the **Configuration** screen to continue.



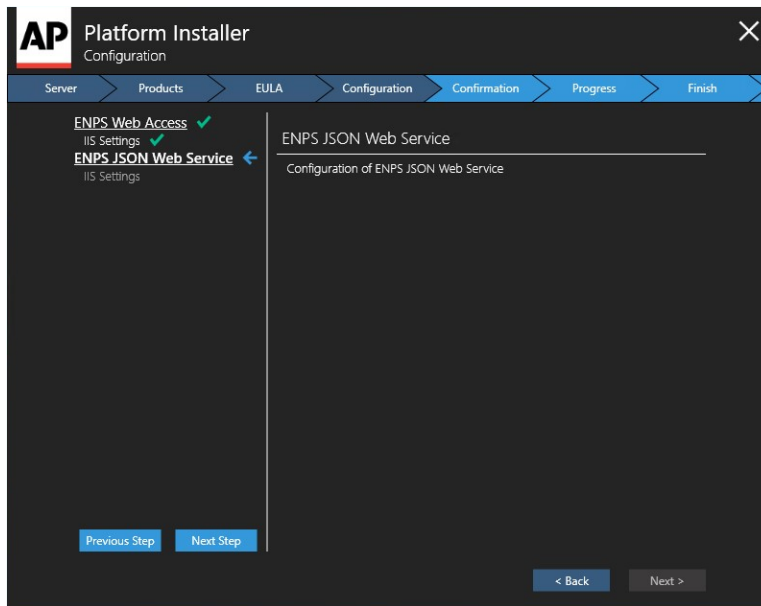
12. The **IIS Settings** screen for **ENPS Web Access** will appear. In the **IIS Settings** screen, select the following:



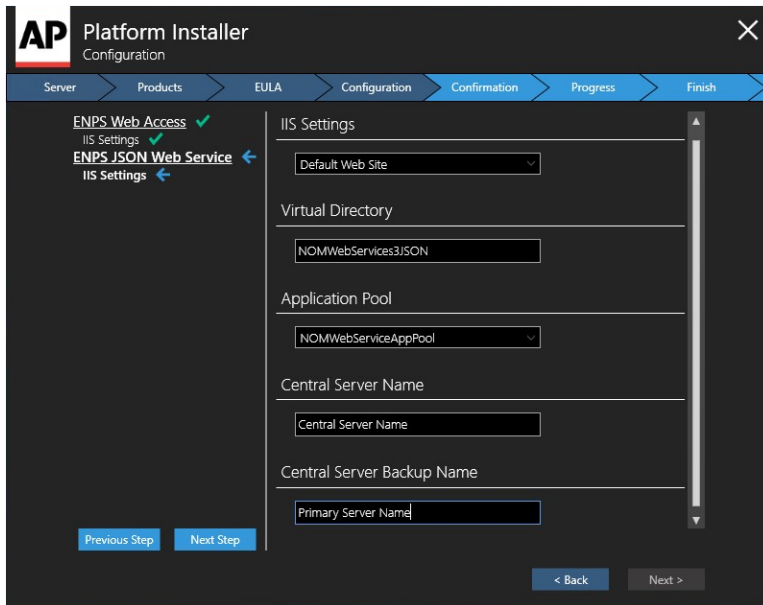
- **IIS Settings.** Select *Default Web Site*.
- **Virtual Directory.** Select *ENPSWebAccess3*.
- **Application Pool.** Select *ENPSWebAccess3AppPool*.

- **JSON Web Services Address.** Enter your server name followed by `/NOMWebServices3JSON`. For example, if your JSON Web Services server is located at `https://servername.site.com`, enter `https://servername.site.com/NOMWebServices3JSON`.
- **JSON Web Services Backup Address.** If the site has a backup JSON address then enter it in this field. Otherwise, enter the same address as the main **JSON Web Services Address** entered above.

Click the **Next Step** button on the **left** side of the screen to continue.



13. The **IIS Settings** screen for **ENPS JSON Web Service** will appear. In the **IIS Settings** screen, select the following:

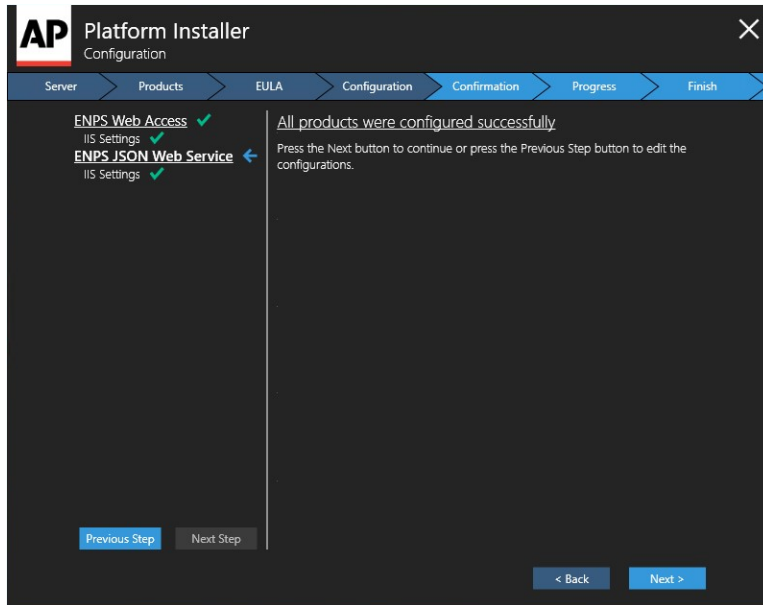


- **IIS Settings.** Select *Default Web Site*.
- **Virtual Directory.** Select *NOMWebservices3JSON*.
- **Application Pool.** Select *NOMWebServiceAppPool*.
- **Central Server Name.** Enter the name of your Central Server. If your enterprise uses only a single Primary-Buddy pair, this is the Primary Server.
- **Central Server Backup Name.** Name or IP address of another ENPS server in your enterprise. This should be an ENPS server local to the site where ENPS Mobile is being installed.

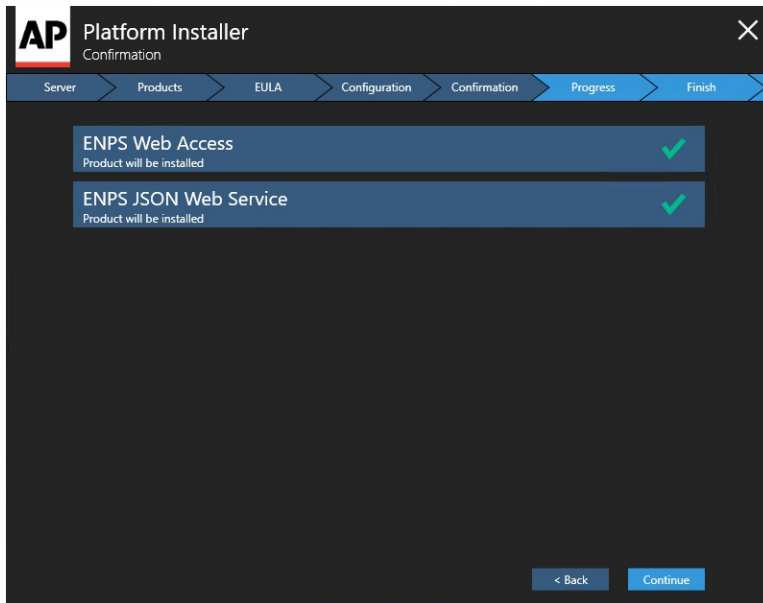
WARNING: Incorrectly setting the **Central Server Name** and **Central Server Backup Name** can cause significant issues in the event of the Central Server failing.

Please contact ENPS Support if you are not sure that you have entered the correct values in these two fields.

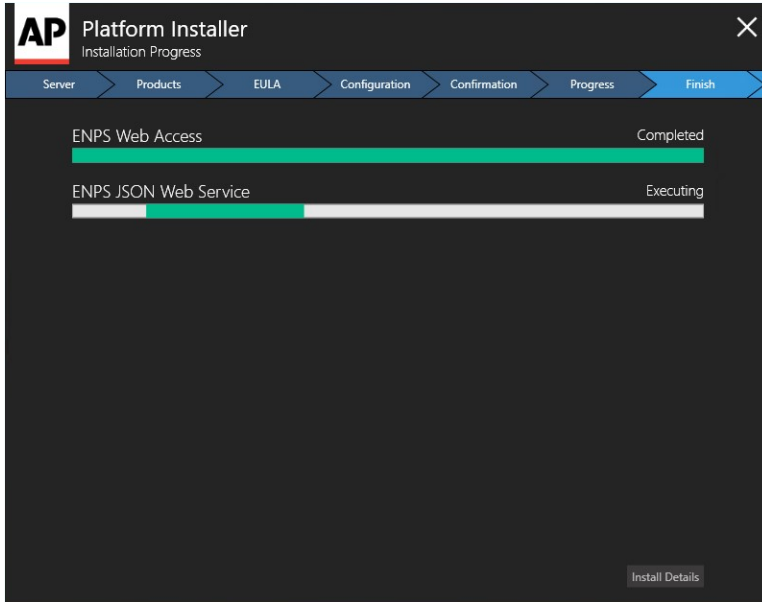
Click the **Next Step** button on the **left** side of the screen to continue.



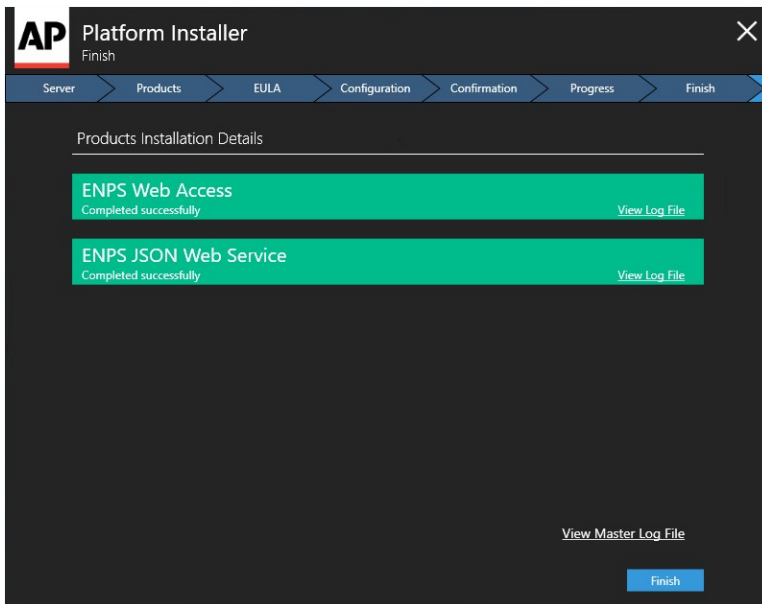
14. The **Confirmation** screen will appear. The **Confirmation** screen will display a list of the products you selected and have configured for installation, indicated by green checkmarks. Click the **Continue** button to begin the installation.



15. The **Installation Progress** screen will appear. Progress bars will be shown for each product you are installing.

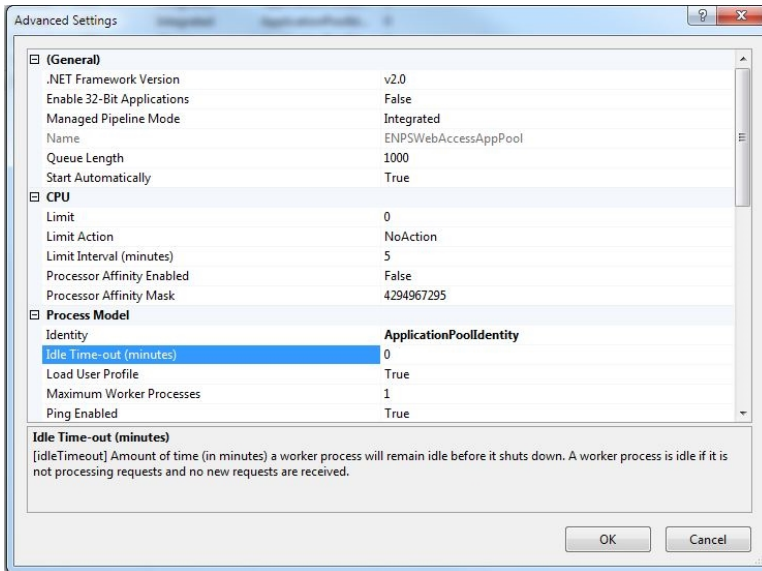


- When the installation is complete, the **Install Details** screen will appear. Select this and you will see the **Finish** screen. The **Finish** screen displays the **Product Installation Details**, which indicate if a product has been installed successfully or if the installation failed. If all products have installed successfully, select the **Finish** button.



- If you are using SSL and have installed your certificate (as described in [Part Three of Appendix A](#)), enable SSL for ENPS Mobile. If you are not using SSL, you can skip to step 18, but note that this is **NOT** recommended.

- a. In the **Internet Information Services (IIS) Manager** window, select the name of the server where you installed the certificate.
 - b. In the left pane of the **Internet Information Services (IIS) Manager** window, double-click on the name of the server where you installed the certificate.
 - c. Single-click on the plus sign (+) to the left of the word "Sites".
 - d. Click once on **Default Web Site**.
 - e. In the **Actions** panel on the right, click **Bindings...**
 - f. In the **Site Bindings** pop-up window, click the **Add** button.
 - g. In the **Add Site Binding** window, select the following from the drop-down selections:
 - For Type, select **https**.
 - For IP address, select **All Unassigned**, or the IP address of the site.
 - For Port, type **443**.
 - For SSL Certificate, select the SSL certificate you installed.
 - h. Click the **OK** button.
 - i. Close the **Site Bindings** window.
 - j. Expand **Default Web Site**. Click on `ENPSWEBACCESS3`.
 - k. In the center panel, double-click on **SSL Settings**.
 - l. Check **Require** and click **Apply**.
 - m. Close the **Internet Information Services (IIS) Manager**.
 - n. You should now be able to access ENPS Mobile services **only** via secure HTTPS (ex: `https://enpsmobile.newsguys.com/enpswebaccess3`). Test to confirm.
18. Edit the Application Pool Advanced Settings:
- a. Open **Internet Information Services (IIS) Manager**.
 - b. In the **Connections** pane, expand the server name and select **Application Pools**.
19. In the Features View on the right, select **ENPSWebAccess3AppPool** and right-click on it.
- a. Select **Advanced Settings**.
 - b. In the pop-up window, find **Idle Time-out (minutes)** and change the value in the right column to 0.

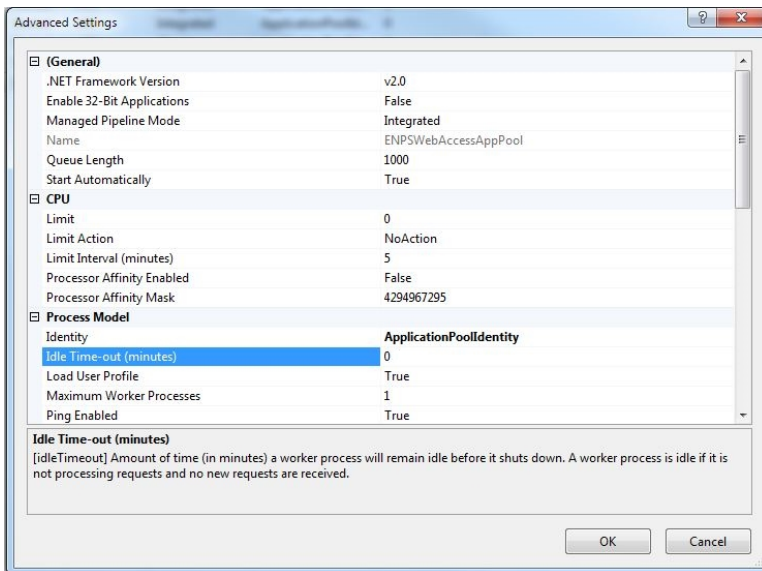


20. Click **OK**.

21. In the Features View on the right, select **NOMWebServiceAppPool** and right-click on it.

a. Select **Advanced Settings**.

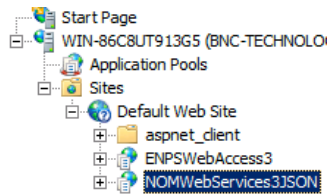
b. In the pop-up window, find **Idle Time-out (minutes)** and change the value in the right column to 0.



22. Click **OK**.

23. Edit the configuration settings for the Web Service Host:

- a. Open **Internet Information Services (IIS) Manager**.
- b. In the **Connections** pane, expand the server name and select **Sites > Default Web Site** and select **NOMWebservices3JSON**.



Application
Settings

24. In the Features View on the right, double-click **Application Settings**. The table below describes the settings on this screen. To edit a setting, double-click it.

Key	Value
CentralServer	Name of your ENPS Central Server. If the Web Service Host cannot resolve the hostname you will need to enter the IP address instead.
CentralServerBackup	Name or IP address of another ENPS server in your enterprise. Ideally, this should be an ENPS server local to the site where ENPS Mobile is being installed.
ClientValidationEnabled*	True
ISHttpPort*	10505
LocalHttpPort*	10505
LogToENPSEvents	When set to True, logs when users attempt to log in to ENPS. For more information, see the User Login Events section.
PreserveLoginUrl*	True

serviceAddress	<p>Path to the Web Service Host. The default address MUST be changed to the actual name of the server.</p> <p>If you are using SSL, "CHANGEME" should be changed to the URL in the SSL certificate. If you are not using SSL, change the https to http.</p> <p>https://CHANGEME/NOMW ebservices3JSON</p>
ServiceRealTimeRecordQueueFrequency	<p>Determines how frequently real-time updates for an open object (Rundown, Story, etc.) are sent to the Mobile client. The default value is 5 seconds (00:00:05).</p> <p>Decreasing this value will allow updates to be seen more quickly, but will place a higher load on the Mobile client/browser. Increasing this value will do the reverse. You may need to experiment with this to find the setting that best meets your needs.</p>
UnobtrusiveJavaScriptEnabled*	True
UseWebService*	False
webpages:Enabled*	False
Webpages:Version*	2.0.0.0
WireSummaryLength*	250
*Do not change the default values for these keys unless instructed to do so by ENPS Support.	

25. Test the Web Service Host by opening a browser and opening the following URL (change to "http" if you are not using SSL):

```
https://<NameOfYourMobileServer>/NomWebServices3JSON/No
mWebService.svc
```

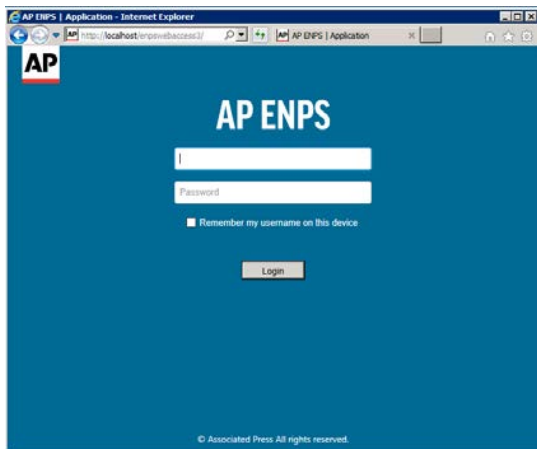
You should see the following page:



This page must load properly for you to continue with the installation. If this page does not load, first verify the installation steps in this chapter. If you continue to have difficulty, refer to the [troubleshooting](#) steps.

Test the Mobile Gateway by opening a browser and opening the following URL (change to "http" if you are not using SSL):

`https://<NameOfYourMobileServer>/enpswebaccess3`



If this page does not load, first verify the installation steps in this chapter. If you continue to have difficulty, refer to the [troubleshooting](#) steps.

Do not test logging in without first updating the *defaultDomain* and *serviceAddress* settings as noted in the next chapter.

26. To ensure that any changes made to the ENPS global tables are automatically replicated to ENPS Mobile, an ENPS System Administrator needs to add an entry to the Services table in System Maintenance as follows:

Field	Value
ID	Machine name of the Web Service Host computer.
Description	User-friendly description of the Web Service Host.
Type	<i>WebServiceJSON</i>
URL	https://<NameOfYourMobileServer>/nomwebservices3JSON/nomwebservice.svc

NOTE: The Type column will only contain the option for *WebServiceJSON* if you are using the System Maintenance client included with ENPS 7 or later. If you are accessing System Maintenance via the ENPS version 6 menu system, you may select *WebService*.

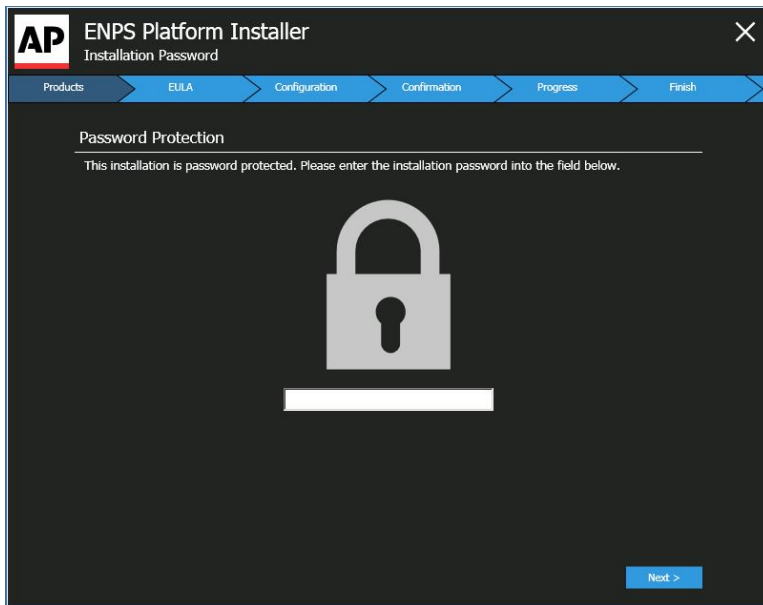
Once this step is complete, you will not need to restart IIS on the Mobile Server any time you make a change to one of the ENPS global tables.

27. Proceed to the next section to configure settings for the Mobile Gateway.

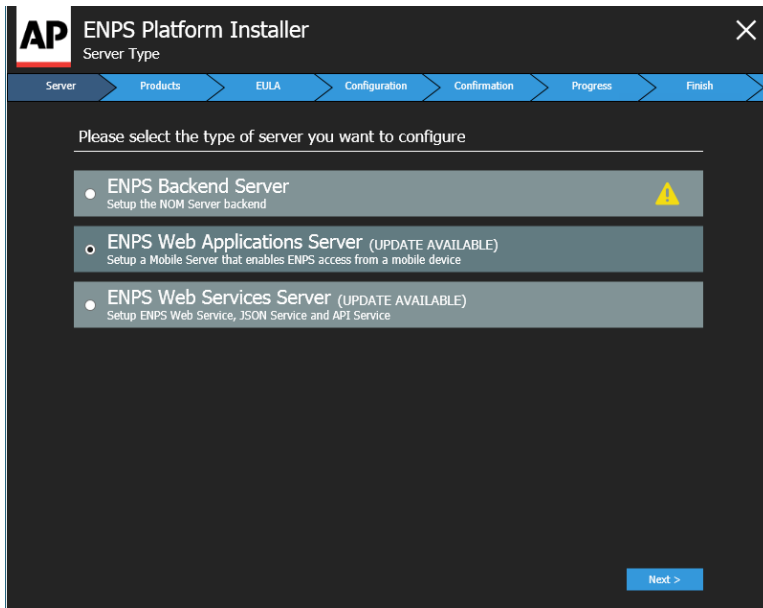
Upgrading on Windows Server 2016

1. Download the ENPS Platform Installer from the ENPS Mobile Download page.
2. Open the ENPS Platform Installer. The **Password Protection** screen appears. Enter

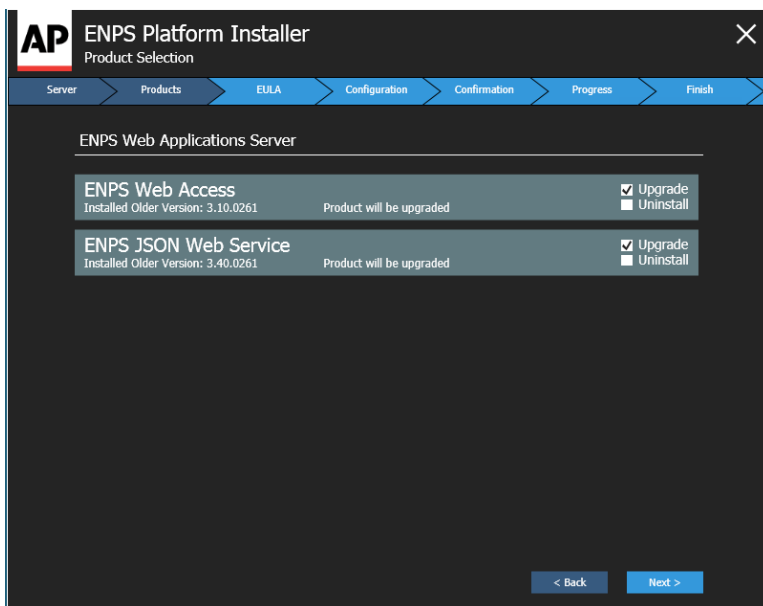
your password and click the **Next** button.



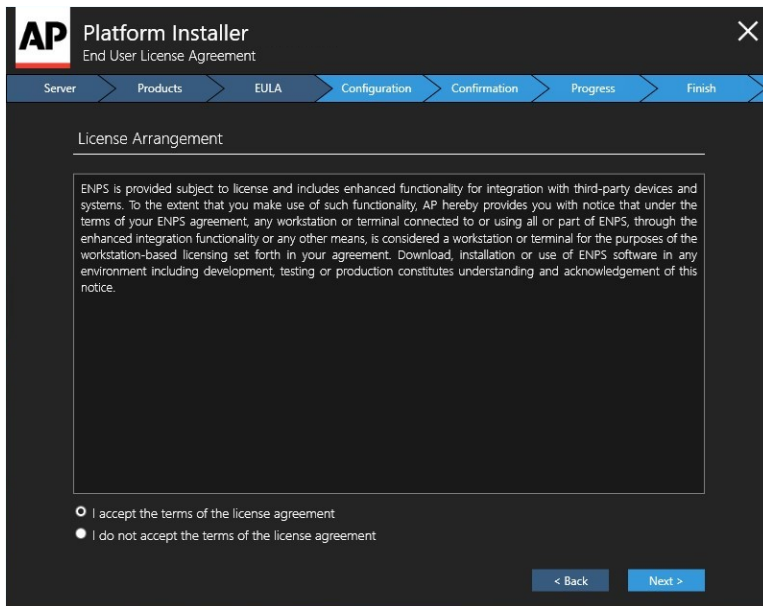
3. In the **Server Type** screen, select **ENPS Web Applications Server (UPDATE AVAILABLE)** and then click the **Next** button.



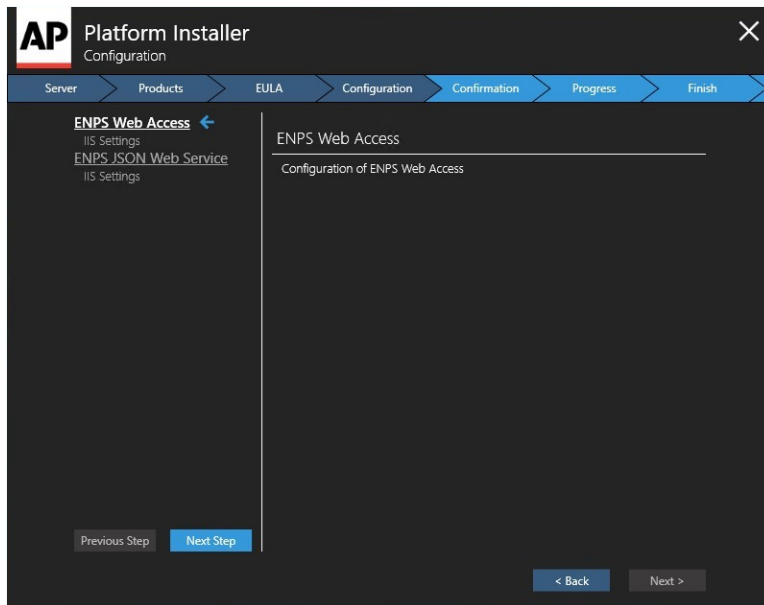
4. In the **Product Selection** screen, select the **Upgrade** checkboxes next to **ENPS Web Access** and **ENPS JSON Web Service**, then click the **Next** button.



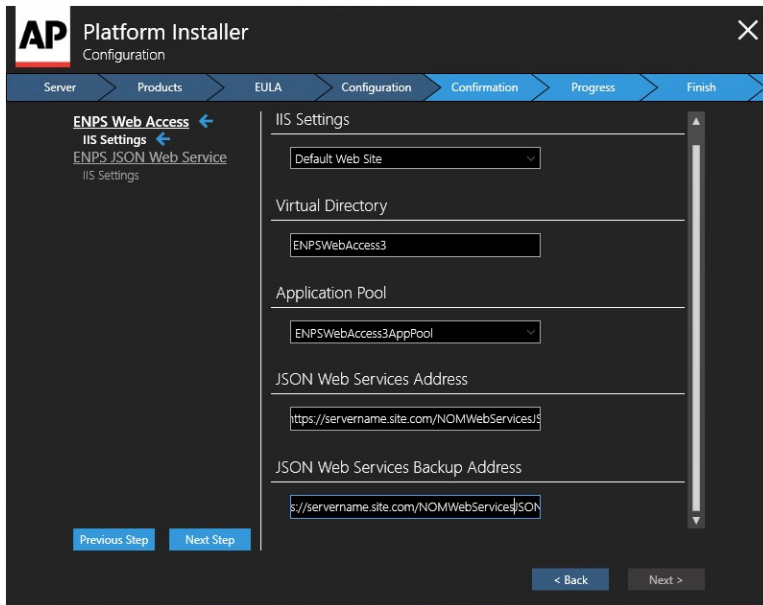
5. In the **End User License Agreement** screen, select the radio button for *I accept the terms of the license agreement*, then click the **Next** button.



6. The **Configuration** screen appears. In the first configuration screen, you do not need to make any selections. Click the **Next Step** button on the **left panel** of the **Configuration** screen to continue.



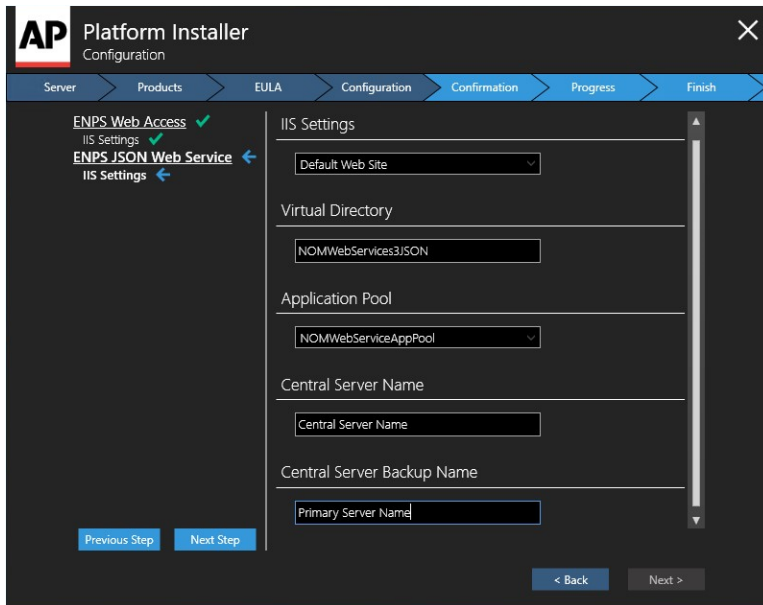
7. The **IIS Settings** screen for **ENPS Web Access** will appear. In the **IIS Settings** screen, select the following:



- **IIS Settings.** Select *Default Web Site*.
- **Virtual Directory.** Select *ENPSWebAccess3*.
- **Application Pool.** Select *ENPSWebAccess3AppPool*.
- **JSON Web Services Address.** Enter your server name followed by */NOMWebServices3JSON*. For example, if your JSON Web Services server is located at *https://servername.site.com*, enter *https://servername.site.com/NOMWebServices3JSON*.
- **JSON Web Services Backup Address.** If the site has a backup JSON address then enter it in this field. Otherwise, enter the same address as the main **JSON Web Services Address** entered above.

Click the **Next Step** button on the **left** side of the screen to continue.

8. The **IIS Settings** screen for **ENPS JSON Web Service** will appear. In the **IIS Settings** screen, select the following:



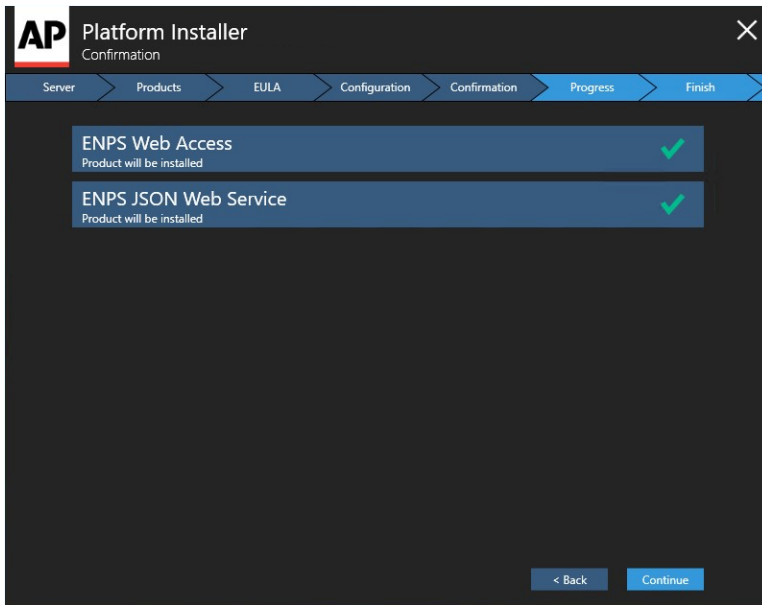
- **IIS Settings.** Select *Default Web Site*.
- **Virtual Directory.** Select *NOMWebservices3JSON*.
- **Application Pool.** Select *NOMWebServiceAppPool*.
- **Central Server Name.** Enter the name of your Central Server. If your enterprise uses only a single Primary-Buddy pair, this is the Primary Server.
- **Central Server Backup Name.** Name or IP address of another ENPS server in your enterprise. This should be an ENPS server local to the site where ENPS Mobile is being installed.

WARNING: Incorrectly setting the **Central Server Name** and **Central Server Backup Name** can cause significant issues in the event of the Central Server failing.

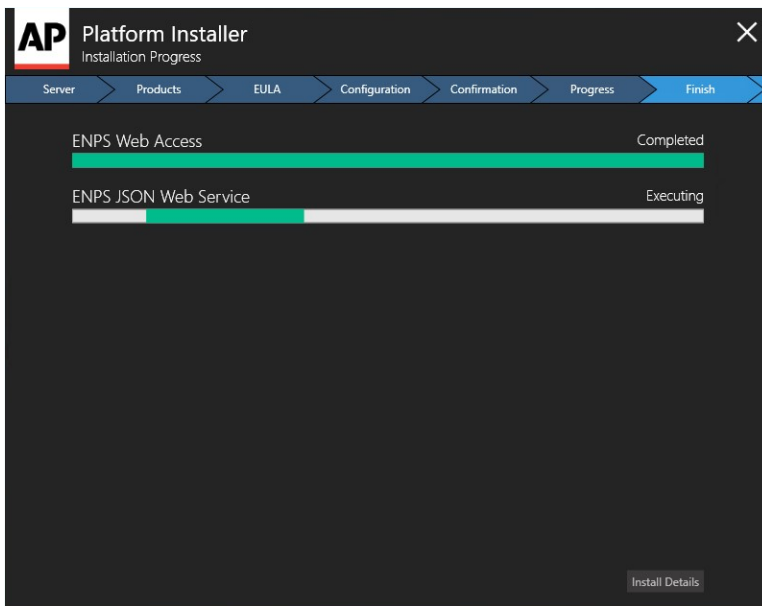
Please contact ENPS Support if you are not sure that you have entered the correct values in these two fields.

Click the **Next Step** button on the **left** side of the screen to continue.

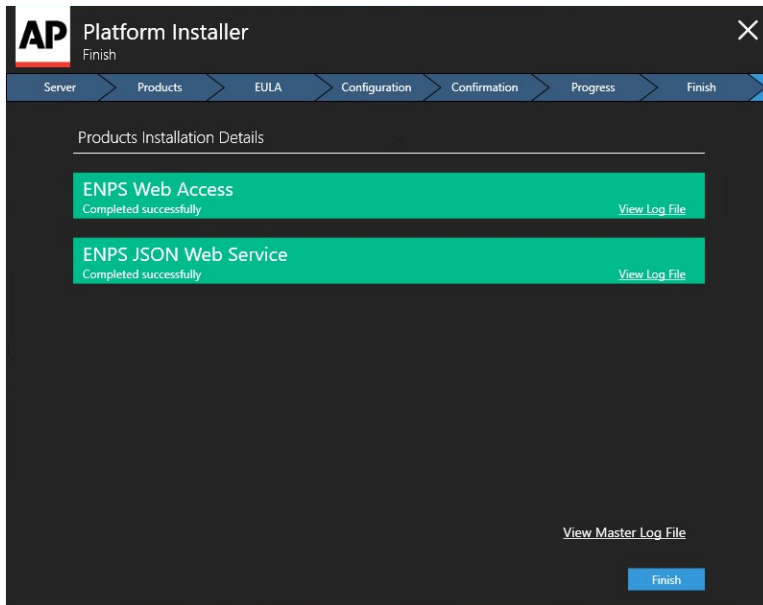
9. The **Confirmation** screen will appear. The **Confirmation** screen will display a list of the products you selected and have configured for an upgrade, indicated by green checkmarks. Click the **Continue** button to begin the upgrade.



10. The **Installation Progress** screen will appear. Progress bars will be shown for each product you are upgrading.



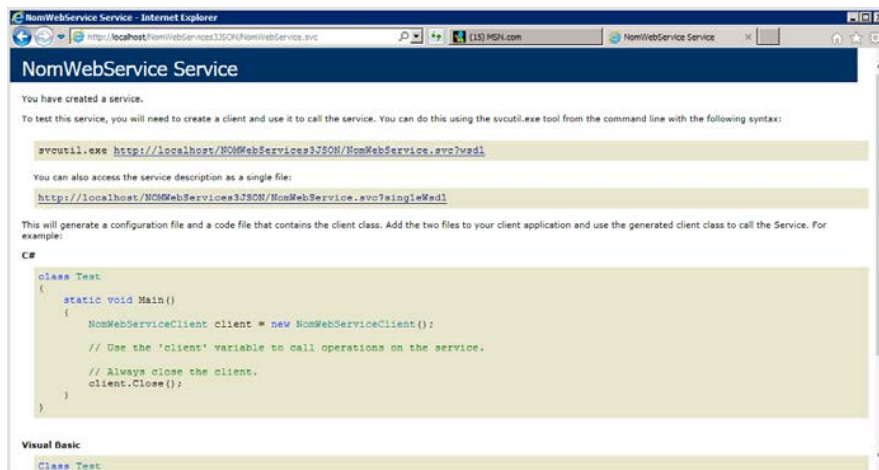
11. When the upgrade is complete, click the **Install Details** button and the **Finish** screen will appear. The **Finish** screen displays **Product Installation Details**, which indicate if a product has been upgraded successfully or if the upgrade failed. If all products have upgraded successfully, select the **Finish** button.



12. It is recommended that you double-check your **Application Settings** at this point. You can do so by referring to *numbers 10, 11 and 18–22* in the **Installing on...** section.
13. Test the Web Service Host by opening a browser and opening the following URL (change to "http" if you are not using SSL):

`https://<NameOfYourMobileServer>/NomWebServices3JSON/NomWebService.svc`

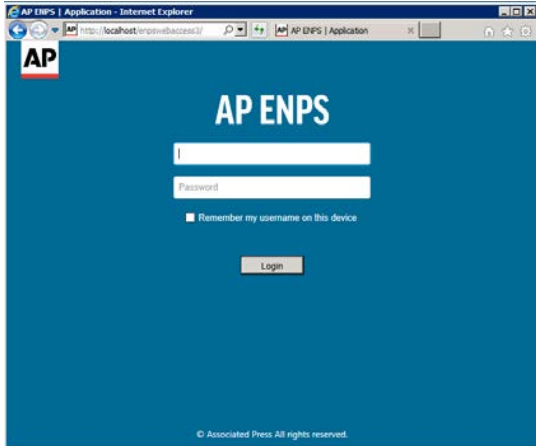
You should see the following page:



This page must load properly for you to continue with the installation. If this page does not load, first verify the installation steps in this chapter. If you continue to have difficulty, refer to the *troubleshooting* steps.

Test the Mobile Gateway by opening a browser and opening the following URL (change to "http" if you are not using SSL):

`https://<NameOfYourMobileServer>/enpswebaccess3`



If this page does not load, first verify the installation steps in this chapter. If you continue to have difficulty, refer to the [troubleshooting](#) steps.

Do not test logging in without first updating the *defaultDomain* and *serviceAddress* settings as noted in the next chapter.

Configuring ENPS Mobile

To access mobile configuration settings, open Internet Information Services (IIS):

1. Select **Roles > Web Server (IIS) > Internet Information Services (IIS) Manager**.
2. Select **Sites > Default Web Site** and select **ENPSWebAccess3**.



Application Settings

3. In the Features view, double-click the **Application Settings** icon.

The following table describes each of the settings on the Application Settings screen:

Option Name	Default Value	Description
AllowEditing	True	Allows editing of Stories via ENPS Mobile, provided the user has appropriate privileges. Additional edit permissions for ENPS Mobile can be configured through the Staff Table in System Maintenance. When set to False, the edit icon is disabled.

<p>defaultDomain</p>	<p>CHANGEME</p>	<p>The network domain where ENPS resides. Setting this allows users to login without having to provide their domain every time.</p> <p>If users need to log in with a domain other than the default, they should enter their username in either of these formats on the login screen:</p> <p><code>domain\username</code> or <code>username@domain</code></p> <p>The default value is "CHANGEME" and MUST be changed.</p>
<p>EnableCheckin</p>	<p>True</p>	<p>Allows users to check in to Stories and Planning Items.</p> <p>When set to False, the check in icon is disabled.</p>
<p>PrompterFontSize</p>	<p>15</p>	<p>Controls how large text contained within {curly brackets} is displayed in the main Story view.</p>

<p>QRCodeRightsInquiries EmailAddressQRCodeRig htsInquiries PhoneNumberQRCodeRi ghtsInquiries SiteName</p>	<p>CHANGEME</p>	<p>Information identifying your newsroom that is recorded into the QR code created in the field that tags your video at ingest time.</p> <p>If video containing this metadata is sent via satellite or other public channels, this information may be available publicly, so it is not recommend that you use personal contact information.</p>
<p>RealTimeUpdateLevel</p>	<p>1</p>	<p>Enables sending of realtime updates to Mobile users.</p> <p>Setting this to 0 disables updates.</p> <p>In the future, this will be expanded to allow for control over which type of updates are sent.</p>

RundownFont	Arial	Default font for Rundowns.
RundownFontSize	14	Default font size for Rundowns.
serviceAddress	https://CHANGEME/NOMWeb services3JSON	<p>Path to the Web Service Host.</p> <p>The default address MUST be changed to the actual name of the server.</p> <p>If you are using SSL, "CHANGEME" should be changed to the URL in the SSL certificate.</p> <p>If you are not using SSL, change the https to http.</p>
StoryFont	Arial	Default font for Stories.
StoryFontSize	10	Default font size for Stories.

<p>TranslatedLabel-Cancel</p>	<p>Cancel</p>	<p>TranslatedLabel-XXXX entries allow for translating text, labels or messages that appear on the main login page into a language other than U.S. English.</p> <p>These are set here because the user is not yet logged in when on the login page and therefore values from the main ENPS language files are not yet available.</p> <p>This applies for all entries beginning with "TranslatedLabel".</p>
-------------------------------	---------------	---

TranslatedLabel-Copyright	Associated Press All rights reserved.
TranslatedLabel-Error	ERROR:
TranslatedLabel-ErrorGettingGlobalTables	Error getting global tables.
TranslatedLabel-LoggingIn	Logging In...
TranslatedLabel-Login	Login
TranslatedLabel-LoginError	Login Error...check username and password and try again.
TranslatedLabel-LoginTimeoutMessage	Your login has timed out. This may indicate a slow internet connection. Please check your connection or contact your system administrator.
TranslatedLabel-LoginWhenApplicationStarts	Login when application starts.
TranslatedLabel-LoginCancellingLogin	Cancelling Login
TranslatedLabel-Password	Password
TranslatedLabel-PasswordError	Please check password.
TranslatedLabel-PasswordError	Please enter password.
TranslatedLabel-RememberMe	Remember my username on this device.
TranslatedLabel-UserID	UserID
TranslatedLabel-	Please enter username.

UserIDValidation		
TranslatedLabel-UserNotAuthorized	You are not authorized to use ENPS.	
TranslatedLabel-WebAccessURL	Web Access URL	
TranslatedLabel-WebserviceError	Login error...could not contact service on	
TSVCommandFontSize	14	Default font size for Production Commands and media references in the Tablet Story Viewer.
TSVPrompterFontSize	15	Controls how large text contained within {curly brackets} is displayed in the Tablet Story Viewer.
TSVRundownFont	Arial	Default font for Rundowns in the Tablet Story Viewer.
TSVRundownFontSize	14	Default font size for Rundowns in the Tablet Story Viewer.

<p>TSVShowTextBelowBlackLine</p>	<p>True</p>	<p>Controls whether Story source content (text below the Story black line) is displayed in the Tablet Story Viewer.</p> <p>Setting this to False will hide source content in the Tablet Story Viewer.</p> <p>If the option <code>TSVSkipStoriesWithoutText</code> is enabled and this option is disabled only Stories with editorial text above the black line will be shown in the Tablet Story Viewer. Stories that contain only text below the black line will be skipped.</p>
<p>TSVSkipStoriesWithoutText</p>	<p>True</p>	<p>By default, paging through the Tablet Story Viewer will skip stories that do not include editorial text above the Story black line.</p> <p>Setting this to False will not skip any Stories, regardless of their contents.</p>
<p>TSVStoryFont</p>	<p>Arial</p>	<p>Default Font for Stories in the Tablet Story Viewer.</p>

TSVStoryFontSize	14	Default font size for Stories in the Tablet Story Viewer.
TSVWebServiceConnectionTimeout	20	Number of seconds the Tablet Story Viewer will wait for a response from the Web Service Host before timing out.
UserIDSpaceReplacementCharacter	- (hyphen)	<p>If your site requires the setting <code>UserIDSpace</code> to access the regular ENPS client, this setting lets you use the same feature with ENPS Mobile.</p> <p>If you use certain reserved characters, such as periods, in your user login ID's, set this value to match the replacement character used in the ENPS staff table.</p> <p>For example, if user <code>john.doe</code> is listed in the ENPS staff table as <code>john-doe</code>, then an entry of <code>UserIDSpace=-</code> would be sufficient.</p> <p>If your site does not use these characters, or there is no difference between your user login ID's and how they are entered in the ENPS</p>

		staff table, you may wish to delete this setting.
WebserviceConnectionTimeout	20	Number of seconds ENPS Mobile will wait for a response from the Web Service Host before timing out.

Session Timeout

Session Timeout controls the number of minutes of inactivity before a user's session is terminated on the server. It is only necessary to set this on the Web Service Host.

To modify this setting:

1. Select **Roles > Web Server (IIS) > Internet Information Services (IIS) Manager**.
2. Select **Sites > Default Web Site** and select **NOMWebServices3JSON**.



Session State

3. In the Features view, double-click the **Session State** icon.
4. In the **Cookie Settings** section, enter the number of minutes for the Session timeout.

Cookie Settings

Mode:

Name:

Time-out (in minutes):

Regenerate expired session ID

5. Click **OK** to save your changes.

ENPS Server Settings for Mobile

Global Configuration Table Settings

The following global configuration settings relate to ENPS Mobile:

- *SendPushNotifications* - set to `true` to ensure that messages are sent to users of the smartphone apps.
- *MobileAPNS* - configure to ensure that alerts are delivered to iOS devices
- *MobileFCM* - configure to ensure that alerts are delivered to Android devices

The *MobileAPNS* and *MobileFCM* keys are configured by the Platform Installer. If missing, please contact the ENPS Helpdesk at support@enps.com.

Staff Table Settings

Several settings in the ENPS Staff table allow administrators to control Mobile access rights and editing permissions for individual users.

By default, all users can access both the ENPS desktop client and ENPS Mobile. This can be changed via the **Blocked Clients** column. Selecting "Desktop" will prevent the user from accessing the ENPS v6 and ENPS v7 or later desktop clients; selecting "Smartphone" will prevent the user from logging in to ENPS Mobile (on any device). The remaining options are legacy settings for use only with ENPS Mobile version 2.

Blocked Clients	<input type="checkbox"/>
Desktop	<input type="checkbox"/>
Outlook	<input type="checkbox"/>
Smartphone	<input type="checkbox"/>
WAP	<input type="checkbox"/>

- The **Smartphone Edit** column controls whether a user can edit existing content or add new lines to a Rundown via ENPS Mobile (subject to their normal ENPS permissions). By default, this column is blank, which means that the user's ability to edit depends on the value of the `AllowEditing` setting in IIS on the ENPS Mobile Gateway server. If this column is set to *Allow* or *Deny*, it will override the `AllowEditing` setting on the server for that user only. The **Web Edit** column is a legacy setting for use only with ENPS Mobile version 2.
- The **Smartphone TSV** column lets you allow or deny access to the Tablet Story Viewer for specific users. By default, all users have access to the Tablet Story Viewer. If the value in this column is set to *Allow* or left blank, the user will be able to access the Tablet Story Viewer. Setting the value to *Deny* will prevent access to the TSV. Note: there is no server-wide setting to disable the Tablet Story Viewer for all users.

NOM Configuration Settings

To ensure that users are properly alerted in real time when new messages are received, the setting "BroadcastMail=1" must be added to the NOM.INI file on all ENPS servers in an enterprise.

To do this:

1. Navigate to the `\NOM` directory on your server.
2. Locate and open the `NOM.INI` file.
3. Under the `[NOM]` section, enter the following setting: `BroadcastMail=1`
4. Close and save the `NOM.INI` file.
5. Restart the **News Object Manager** (at a time that is convenient for your newsroom).

Media Upload

ENPS Mobile Mobile users can upload media from a mobile device directly into a story. Full details are in the *Media Submission from the Field* section of the **ENPS Operations Guide**.

Language Support for Mobile Devices

Non-U.S. English sites should refer to the options with the prefix `TranslateLabel` in the Mobile Gateway settings table above for translating specific text fields in the mobile interface that appear prior to user login.

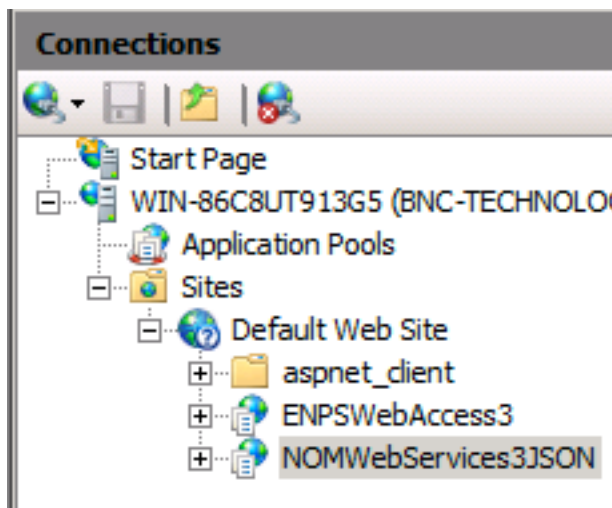
All text and labels that appear after user login are based on the standard ENPS **Language Resources** tables, which can be edited via System Maintenance.

Troubleshooting

This chapter provides you with troubleshooting information for the setup and configuration of the ENPS Mobile Server.

Verifying Settings–WebService Host

1. Open **Server Manager** and expand **Roles > Web Server (IIS) > Internet Information Services (IIS) Manager**. In the **Connections** pane, expand the server name. Verify that the `NomWebServices3JSON` virtual directory is listed under **Default Web Site**. Select **NOMWebServices3JSON**.



2. In the Features view, open **Application Settings**. Verify that the settings are correct.



Application
Settings

Refer to the [Configuring ENPS Mobile](#) chapter for more information.

3. In the Features view, select **Authentication** and verify that *Anonymous*

Authentication is enabled.



Authentication

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Verifying Settings—Mobile Gateway

1. Open **Server Manager** and expand **Roles > Web Server (IIS) > Internet Information Services (IIS) Manager**.
2. In the **Connections** pane, select **ENPSWebAccess3** and click **Application Settings**. Verify that `serviceAddress` is set to: `https://<NameOfWebServiceHost>/nomwebservices3JSON`



Application Settings

(or `http:`, if you are not using SSL)

3. Refer to the **Configuring ENPS Mobile** chapter for more information on these settings.
4. In the Features view, select **Authentication** and verify that *Anonymous*

Authentication is enabled.



Authentication

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Disabled	HTTP 401 Challenge

Not Seeing New Features and Enhancements

If you are not seeing new features and enhancements after updating your ENPS Mobile server, you will want to clear the browser cache and ensure you have the latest version of the app on all your client devices.

IIS Issues

If an error occurs during IIS installation, navigate to the Microsoft.NET folder and run the following command from the command line, where {version} is the .NET version number:

```
%systemroot%\Microsoft.NET\Framework\{version}\aspnet_regiis.exe -i
```

The system root folder is usually `C:\Windows` however running the command directly from the Microsoft.Net framework folder as mentioned above may be easiest. See the ASP.NET section below for more information.

Duplicate Values

Check that entries in ENPS global tables do not have duplicate IDs.

The System Maintenance application prevents you from creating entries with the same ID. However, entries created by hand, for example in Notepad, do not have this error checking.

ASP .NET Issues

There are a few issues that may occur with new ASP .NET installations:

You have installed ASP.NET and the .NET Framework on the server, but when you request a page from your application nothing happens and the request does not resolve.

You need to install and enable IIS on the server before you install the .NET Framework. Either you can uninstall the .NET Framework from the server, install IIS, then reinstall the .NET Framework. Or you can install IIS and use the ASP.NET IIS registration tool `Aspnet_regiis.exe` to configure the script maps that IIS uses for ASP.NET filename extensions. See below for more information.

You have installed ASP.NET and the .NET Framework with IIS installed and enabled, then uninstalled and reinstalled IIS. When you request a page from your application, nothing happens and the request does not resolve.

When you uninstalled and reinstalled IIS the script maps that IIS uses for ASP.NET were broken. Use `ASPNET_REGIIS.EXE` to configure the script maps that IIS uses for ASP.NET file name extensions. See below for more information.

You have installed and enabled IIS, installed ASP.NET and the .NET Framework, deployed your application, and requested a page, but you receive one of the following error messages:

```
Access denied to 'C:\Inetpub\wwwroot' directory. Failed to start monitoring directory changes.
```

```
Server cannot access application directory'C:\Inetpub\Wwwroot\ Virtual Directory Name \'. The directory does not exist or is not accessible because of security settings.
```

The proper permissions have not been set for the website or virtual directory. ASP.NET requires read, execute, and list access for the ASPNET account (the `Aspnet_wp.exe` process account) on the root website or on any virtual directory. These settings are necessary so that ASP.NET can access the content files and can monitor file changes.

To add read, execute, and list permissions for the ASPNET account on the root website or on a virtual directory, complete the following steps:

1. Open the folder that contains the root website, which is `C:\Inetpub\Wwwroot` by default or the virtual directory.
2. Right-click the folder and select *Properties*.
3. On the **Security** tab, click **Edit** and then select *Add*.
4. Type `ComputerName\ASPNET`. For example, on a computer named "Webdev," type `Webdev\ASPNET` and then click **OK**.
5. Allow the following permissions for the ASPNET account: Read & Execute, List Folder Contents, and Read.
6. Click **OK** to close the Properties dialog box and to save the changes.

You do not need to perform these steps if the Everyone group or the Users group has read access to the root website or virtual directory.

To repair IIS mappings for ASP.NET using `Aspnet_regiis.exe`, type the following command (including quotes) at the command prompt. Replace `{version}` with the version number of the .NET Framework installed on your server.

```
"%systemroot%\Microsoft.NET\Framework\
{version}\aspnet_regiis.exe" -i
```

For more information on `Aspnet_regiis.exe`, enter the following command:

```
"%systemroot%\Microsoft.NET\Framework\
{version}\aspnet_regiis.exe" -?
```

If you want to install ASP.NET on a domain controller there are special steps you must take to make the installation work properly. For more information, see article Q315158, "ASP.NET Does Not Work with the Default ASPNET Account on a Domain Controller" in the Microsoft Knowledge Base at <http://support.microsoft.com>.

User Login Events

When set to `True`, the `LogToENPSEvents` setting in the `NOMWebServices3JSON` *Application Settings* will log all attempts by a user to log in to ENPS Mobile.

The logs are stored as Events in **Event Viewer > App and Service Logs > ENPS Events**.

The following information associated with users is logged:

- **User ID**
- **User's IP Address**
- **User's Home Server**
- **Message.** A number that indicates a successful or unsuccessful login. The messages are as follows:
 - **5001.** Indicates successful login.
 - **5002.** Indicates the login failed.

Appendix A. Purchasing and Installing SSL Certificates

A self-signed Server Certificate-"AP Platform Certificate" is provided on installation of ENPS 9, but we strongly recommend that publicly-signed SSL certificates be used instead.

Part One: Purchasing an SSL Certificate

When you install a Secure Sockets Layer (SSL) certificate on your server, you provide an extra layer of security that ensures that the connection between the Mobile server and clients is protected from unauthorized users. It is strongly recommended to use SSL with ENPS Mobile, even when used entirely within your protected network.

Complete the following steps to obtain an SSL certificate:

1. Complete the instructions in this guide to *install* and *configure* your Web Server.
2. Generate a CSR (Certificate Signing Request) and save it to a text file. Instructions on generating a CSR can be found on various websites:

- https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=INFO235&actp=search&viewlocale=en_US&searchid=1463664287015
- https://search.thawte.com/support/ssl-digital-certificates/index?page=content&id=INFO1108&actp=search&viewlocale=en_US&searchid=1463664326022

When asked to enter the name of your website, do not enter a wildcard representing a wide domain name range, e.g. *.sitename.com. Instead, provide the name you have created specifically for the server that must be in the form of netbios.sitename.com.

3. Once you have the CSR, you need to purchase an SSL Certificate. There are many vendor websites that sell certificates. Contact your chosen vendor directly for any SSL Certificate installation or support questions.
 - <http://help.godaddy.com/article/5282>

- <https://knowledge.verisign.com/support/ssl-certificates-support/index.html>
- <https://search.thawte.com/support/ssl-digital-certificates/index.html>

Part Two: Generating a Certificate Request

To generate a certificate request, perform the following steps:

1. On the server desktop, click the **Start** button.
2. Click on **Administration Tools**.
3. From the sub-menu, click on Internet **Information Services (IIS) Manager**.
4. In the **Connections** pane on the left, click the name of your server.
5. In the middle pane, double-click on the **Server Certificates** icon (in the IIS section of the pane).
6. In the **Actions** pane on the right, single-click on **Create Certificate Request**.
7. The **Request Certificate** wizard should open.
8. Complete the form with the following information:

NOTE: You may not use the following characters in your responses:

< > ~ ! @ # \$ % ^ * / \ () ? &

- **Common Name.** The exact URL/address that your staffers will use to access your ENPS Mobile server from the field. Example: enpsmobile.wxxx.com
 - **Organization.** The name in which your domain legally registered. Must be the same name under which your domain name is registered.
 - **Organizational Unit.** Use this field to identify a group within your company. Something that is helpful for your tracking/record-keeping.
 - **City/Locality.** The full name of the city or village in which your company is registered/located. **NOTE:** Do not abbreviate.
 - **State/Province.** The full name of state or province in which your organization is located. **NOTE:** Do not abbreviate.
 - **Country.** The two-letter ISO country code for the country in which your company is legally registered.
9. Click the **Next** button.
 10. For Cryptographic service provider, from the drop-down select **Microsoft RSA SChannel Cryptographic Provider**.

11. For Bit length from the drop-down select: **2048**.
12. Click the **Next** button.
13. The server is going to create a short text file that you will copy and send to your SSL Certificate Vendor to formally request your SSL certificate. In the space, type in the full path and name for how you want the text file to be temporarily written to your server. You may click on the ellipsis button to open a "Save As" dialogue box to guide your file naming. Give it a very obvious name so you can identify it easily. If you have used the "Save As" dialogue box, click the **Open** button.
14. Click the **Finish** button.
15. Follow the directions from your SSL vendor for requesting your certificate. It will require copying the text from the file you just created.

Part Three: Installing a Server Certificate

Your SSL Certificate vendor will provide you with two files. Save them to someplace that you will remember on your ENPS Mobile server. Once you download the files, you will first install the Intermediate Certificate in your IIS 7 server. After that you will install the primary SSL Certificate. In doing so, you will complete the pending request, and then bind the certificate to your website.

Installing an SSL Certificate in IIS 7

1. On the desktop, click **Start**.
2. Click on **Administrative Tools**.
3. Click **Internet Information Services (IIS) Manager**.
4. In the left pane of the **Internet Information Services (IIS) Manager** window, click once on your server.
5. In the IIS section of the middle pane, double-click **Server Certificates**.
6. In the **Actions** pane on the right, click on **Complete Certificate Request...**
7. To locate your certificate file, click on the ellipsis (...) button.
8. In the **Open** dialogue box, from the drop-down list, select *.* as your file name extension.
9. Navigate to the files you saved and select your certificate (it might be saved as a .txt, .cer, or .crt).
10. Click the **Open** button.

11. In the **Complete Certificate Request** window, enter a Friendly name (something obvious) for the certificate file.
12. Click on the **OK** button.
13. Close the **Internet Information Services (IIS) Manager** window to complete your SSL certificate installation.

Configuring HTTPS Binding

1. In the **Internet Information Services (IIS) Manager** window, select the name of the server where you installed the certificate.
2. In the left pane of the **Internet Information Services (IIS) Manager** window, double-click on the name of the server where you installed the certificate.
3. Single-click on the plus sign (+) to the left of the word "Sites".
4. Click once on **Default Web Site**.
5. In the **Actions** panel on the right, click **Bindings...**
6. In the **Site Bindings** pop-up window, click the **Add** button.
7. In the **Add Site Binding** window, select the following from the drop-down selections:
 - For Type, select **https**.
 - For IP address, select **All Unassigned**, or the IP address of the site.
 - For Port, type **443**.
 - For SSL Certificate, select the SSL certificate you installed.
8. Click the **OK** button.
9. Close the **Site Bindings** window.
10. Expand **Default Web Site**. Click on `ENPSWEBACCESS3`.
11. In the center panel, double-click on **SSL Settings**.
12. Check **Require** and click **Apply**.
13. Close the **Internet Information Services (IIS) Manager**.
14. You should now be able to access ENPS Mobile services **only** via secure HTTPS (ex: `https://enpsmobile.newsguys.com/enpswebaccess3`). Test to confirm.

AP



support@enps.com

USA & Americas : +1.866.ENPS.911

EMEA, APAC & ROW: +44.20.7482.7707

workflow.ap.org