Print Audit Secure

Print Audit Secure Installation and Setup Guide 1-2

Version: 7

Date: 03-Dec-2018 16:11

Table of Contents

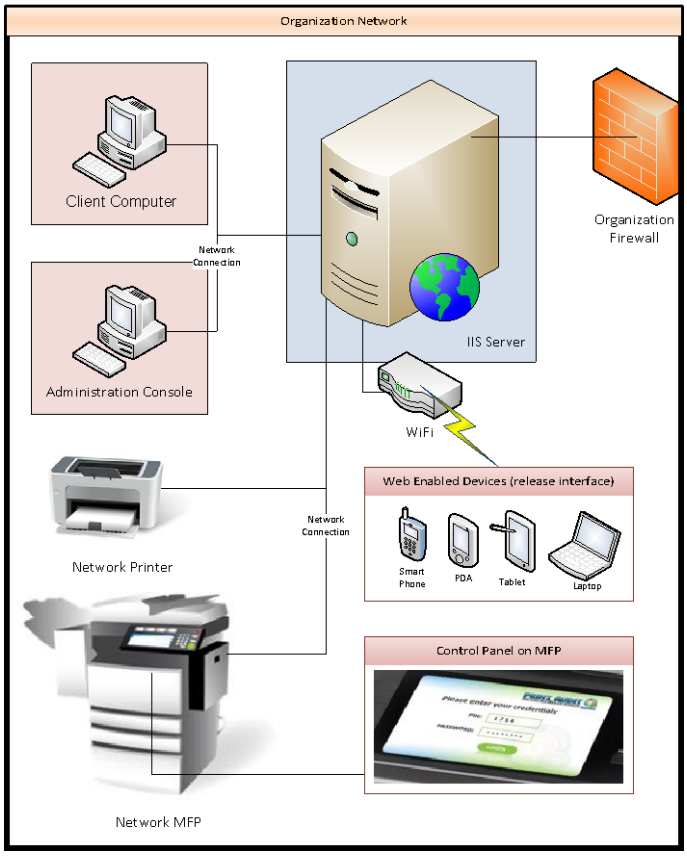
Print Audit Secure is a stand-alone application which provides secure printing and follow me capabilities, to help manage document output on your network.

Print Audit Secure ensures that print jobs are not printed until you are at the MFP, ready to pick them, eliminating wasted pages from being left at the output tray. And with follow me printing capabilities, Print Audit Secure allows users to bypass line-ups at the printer by enabling them to release their job at any compatible MFP on the network.

1. Components

Installed Components

Print Audit Secure – Network Servers and Workflow



Click to enlarge

Secure Client

The Secure Client is installed on every workstation where print jobs are to be secured for later release. The Secure Client collects information from every secured job printed at the workstation, and communicates with the Print Audit Secure Server.

Secure Server

The Secure Server handles all user authentication, job transaction calculation and tracking, document release and routing, and administrative tools. One Secure Server is required in every Print Audit Secure deployment.

Secure Release Options

PC based release

Registered users who have submitted jobs through a Secure enabled workstation can use any PC with a network connection to connect to the host Print Audit Secure Server to select and release print jobs. This would include the users local workstation used to submit jobs.

The Release Function is enabled simply by accessing the designated URL for Print Audit Secure and entering the user credentials. Unlike the administrative Print Management access defined earlier in this document, users will only be able to view and manage their own print jobs.

Smartphone release

Similar to the PC release method, smartphones with network access and a web browser can be used to release user print jobs via a mobile optimized version of the Secure web portal. Secure is compatible with most modern mobile phones, including Android, iPhone and Blackberry devices.

Web-based MFP release

User Print Release in Print Audit Secure may be enabled through multiple compatible devices. Among these are any PC workstation in the client network, smart phones with internet access and other devices such as many Multi-Functional Printers ("MFP's") that either have a compatible web browser capability or that have been enabled with Print Audit Secure embedded software.

MFP embedded control panel release

Any MFP device that has a web browser interface option may be compatible for user print release. Use of this option is subject to configuration options available with the MFP and may require additional software options from the dealer or vendor for this MFP device. The common setup for this type of device is to define the Print Audit Secure server URL as a common "Favorite".

Minimum system requirements

Secure Server

- 32 or 64–bit versions of Microsoft Windows Server 2003, 2008, 2008R2, 2012R2 or Windows 7
- IIS version 6 or newer
- Dot NET framework 4.0 or newer
- SQL Server 2005, 2008, 2012, 2014 – Full or Express
- Active Directory
- If also using Print Audit 6, version 6.5.0 or newer is required

Secure Client

- Windows XP or newer
- If also using Print Audit 6, version 6.5.0 or newer is required
- Microsoft Installer 2.0 or newer

Secure Web Release Station

- Compatible with all modern browsers such as Chrome, Internet Explorer 7 or newer, Firefox, or Safari

Secure Mobile Release

- Optimized for Android 2.2 and newer, IPhone, and most modern smartphones

3. Server Installation

Summary of System Setup

The following list is a summary of the deployment steps that need to be completed, to set up and configure Print Audit Secure. Each of these steps is covered in the following pages of this Installation and Setup Guide.

1. Install the Print Audit Secure Server software.
2. The first time you go to the Print Audit Secure website you will need to set an Administrator username and password.
3. Set your preferred configuration under Setup -> Configuration.
4. Activate your license key (or request a trial license).
5. Enter or import the printers that you want to designate as Secure. We recommend adding only the devices that you want to include in one Printer Compatibility group.
6. Create a Printer Compatibility group and add the devices from step 5.
7. Repeat steps 4 and 5 until all of the printers you want to designate as Secure have been added.
8. Install the Print Audit Secure Client on the workstations.

Before you Install

Active Directory

Print Audit Secure uses Active Directory to authenticate users. Print Audit Secure Administrators are pulled from a separate group in Active Directory.

Before installing Print Audit Secure this group must be created and populated with all users that should have administrative access to Secure.

Security with the Web Release Station

By default, the Print Audit Secure server operates under HTTP, not HTTPS, so it is unsecured. This means that any login information used on the web page is sent to the server in clear text. If this is a concern for you there are steps you can follow to encrypt this information.

1. **Create an SSL certificate.**
    a. Create a simple self-signed certificate. For information on this please visit the link below and start at the IIS Manager section. With this approach, as you can see from the example, is that when you try to go to the secure server the browser will display an error page saying that it cannot verify the certificate.
        i. http://learn.iis.net/page.aspx/144/how-to-set-up-ssl-on-iis-7/
    b. Setup a certification authority on your server, if you do not already have one on the domain, and generate a certificate from that. It will act as a valid certificate on the domain.
    c. Acquire a third party certificate.
2. **Configure the Print Audit Secure web application to use SSL.**
    a. Open the IIS Manager
    b. Click on Default Web Site
    c. Under Edit Site click on Bindings
    d. Click the Add button
    e. Under Type select https and keep IP address set to All Unassigned
    f. Select the certificate under SSL certificate
    g. Click Ok
3. **Ensure SSL Settings are not set to Require SSL.**

SQL Database installation

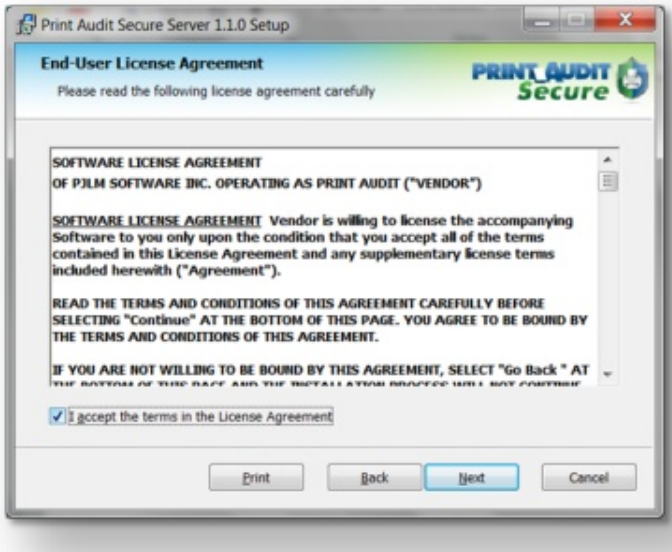
There are several guides available to assist you with installing and configuring SQL for use with Print Audit Secure . Please download the appropriate SQL database documentation for your deployment.

Secure Server Installation: Step-by-Step

Print Audit Secure is a software application that allows jobs to be placed into a virtual print queue, enabling users to conveniently release them on demand at any printer via web enabled devices such as workstations, tablet PCs or mobile device. The jobs will be stored in the Print Audit Secure database until the user who printed the jobs releases them or a Print Audit Secure Administrator cancels them. End users connect to this server through a web browser on any web enabled workstation or mobile device to release their print jobs. The Print Audit Secure Server hosts the Secure application and the database.

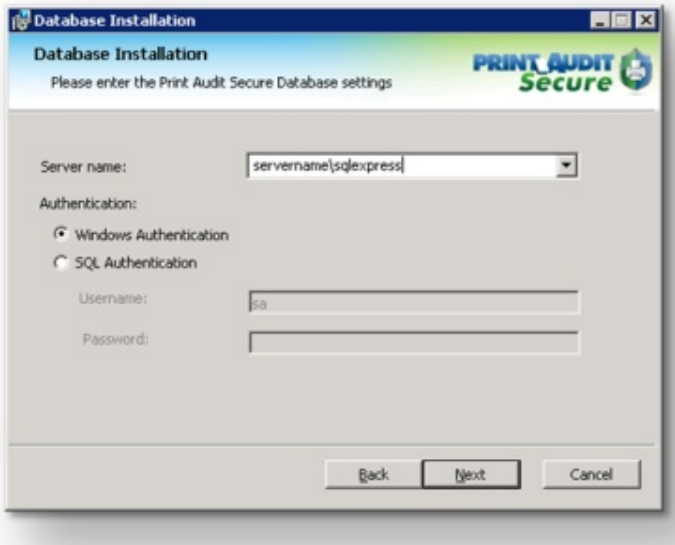
1. Download the SecureServerSetup.exe file from www.printaudit.com.
2. Double click on the SecureServerSetup.exe file to begin the installation.
3. Click the Next button on the Welcome screen

4. Check "I accept the terms in the License Agreement" and click the Next button.

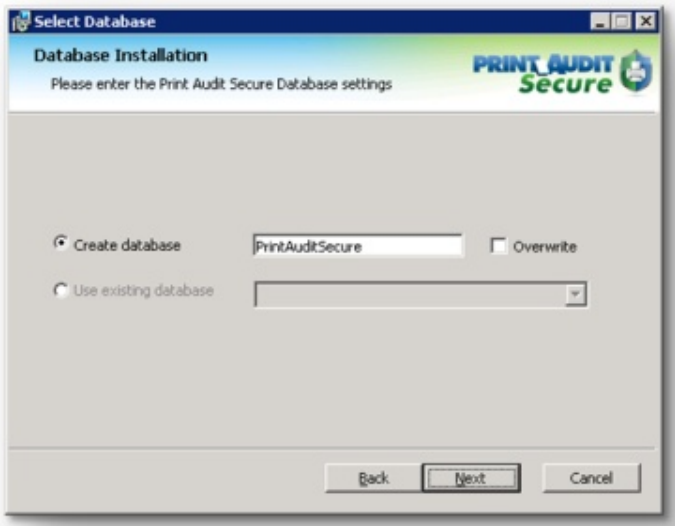


5. Select the location you would like to install Print Audit Secure to or to accept the default click Next.

6. Select the name of the server where the database will be installed. For the Express version of SQL Server, enter a backslash and then the SQL Server instance name (by default: SQLExpress). Then, Select either Windows Authentication or SQL authentication for the database. SQL Authentication is recommended. If you select SQL Authentication enter the username and password of a user that has administrative rights to the SQL Server. Click Next.



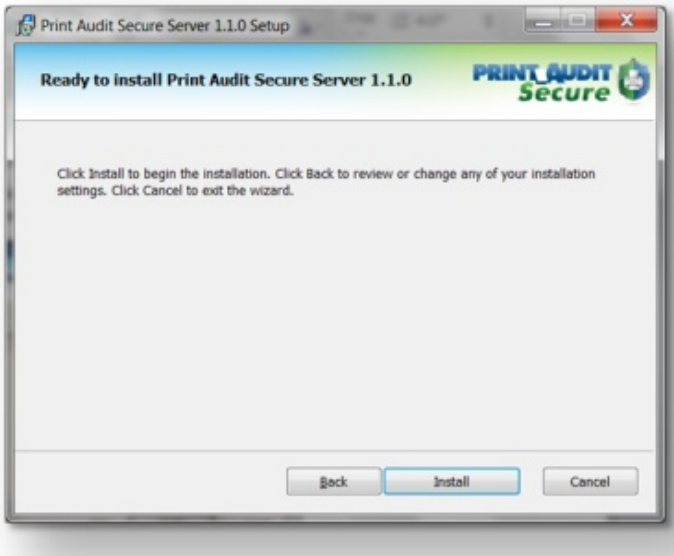
7. If this is the first time you have installed Print Audit Secure, select Create database and click Next. If you have an existing database choose Use existing database and select the database name. If you have an existing database and would like to create a new one with the same name, choose Create database and check Overwrite. This will remove all your current settings.



8. Select the Website name you would like Print Audit Secure to use. We recommend using the Default Web Site. Click Next.

9. Click the Install button to install Print Audit Secure on your server.

NOTE: You do not need to reboot after the install on the server, however, it is recommended that you reboot this computer as soon as possible.



10. Click Finish to exit the Setup Wizard.


Print Audit Secure Client 1.1.0 Setup
Completed the Print Audit Secure Server 1.1.0 Setup Wizard
Click the Finish button to exit the Setup Wizard.
PRINT AUDIT Secure
Back
Finish
Cancel

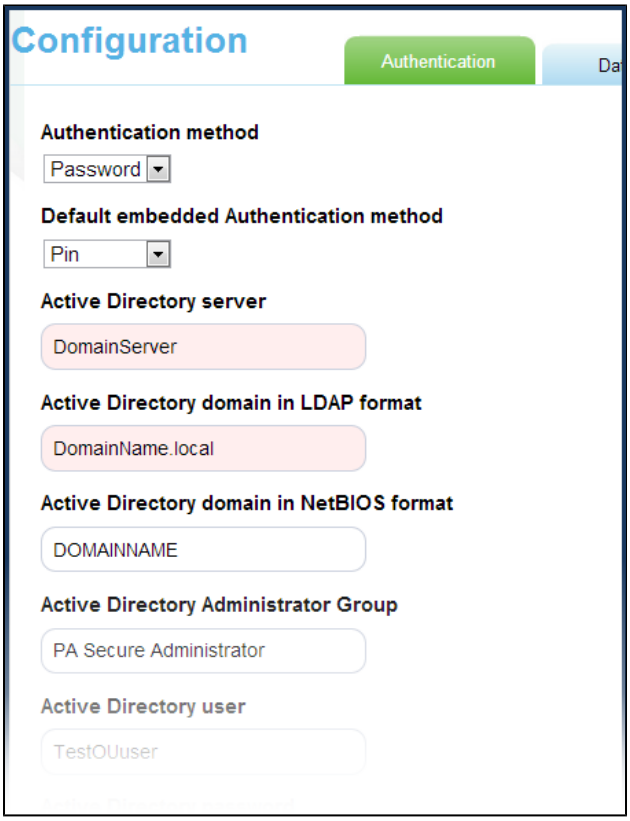
4. Configuration

Authentication settings

Immediately after installing Print Audit Secure, there must first be an authentication method setup for the server.

1. Open a web browser and go to http://<SECURESERVERNAME>/pasecure
2. The following page will appear, with a prompt to configure Print Audit Secure with the Active Directory settings for the environment. Click Ok to be automatically directed to the Authentication tab under *Setup -> Configuration page.*

> **Important!**
>
> You must enter the required information for these fields before continuing with the server configuration.



Authentication method

Select the authentication method that will be used to release any Secured print jobs.

1. **Password** – The password is the users Active Directory password used for authenticating to the domain.
2. **Pin** – The Pin comes from an Active Directory attribute that is associated to the users' profiles.
3. **Swipe** – To authenticate with a swipe card, the card number must be entered in an Active Directory attribute.

Default Embedded Authentication Method

If Print Audit Secure will be used in conjunction with a Print Audit Secure Embedded solution, select the default authentication method that will be used to release Secure jobs. As with the above configuration, the selection is Password, Pin, or Swipe authentication.

Active Directory Server

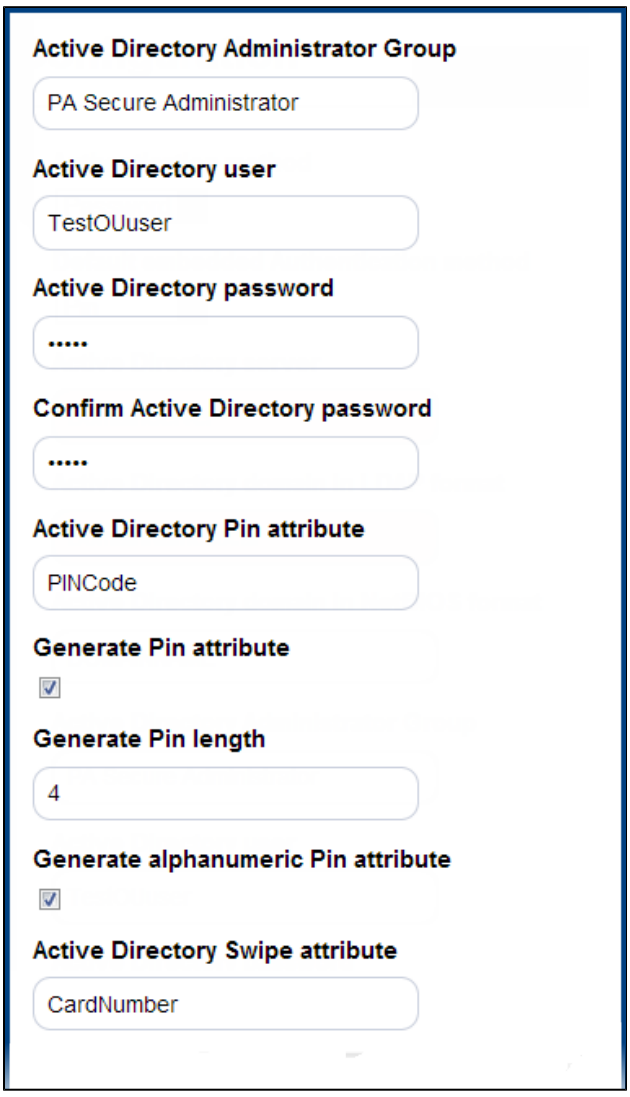
Enter the name of the Active Directory server.

Active Directory domain in LDAP format

Enter the name of the Active Directory domain in LDAP format.

Active Directory domain in NetBIOS format

Enter the name of the Active Directory domain in NetBIOS format.



Active Directory Administrator Group

Enter the Active Directory group name of users that should have administrative access to the Print Audit Secure server.

Active Directory user/password

Enter the name of an Active Directory user who has the authority to read and write to Active Directory. Enter the password for this user. Enter the password again to confirm it is correct.

Active Directory Pin attribute/length

If PIN was selected as the authentication method in step 3, enter the name of the Active Directory attribute that stores the users' PIN codes.

Generate Pin attribute/length

Check this box to enable users to generate a Pin at the Web Release Station or at MFPs. For more information on this functionality, refer to the **Self-generated PINs** section that appears further in this document. Note: this may not be supported on all embedded solutions.

Active Directory Swipe attribute

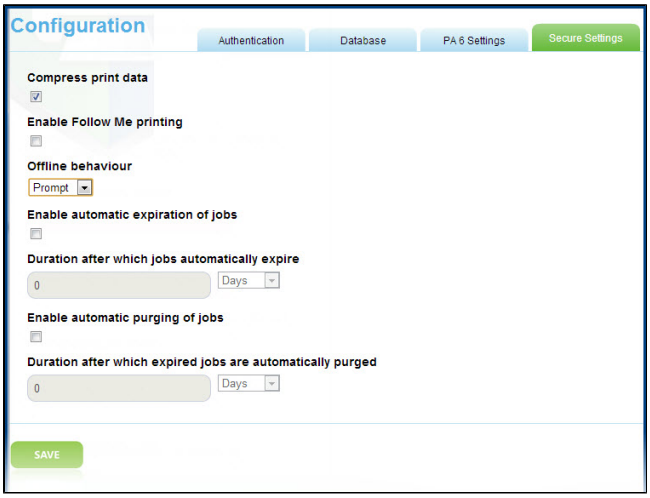
If swipe was selected as the authentication method in step 3, enter the name of the Active Directory attribute that stores the users' swipe card numbers.

Click the Save button, to save these authentication settings.

Print Audit Secure Settings

Log into the Secure server and from the top menu, select >Setup >Configuration and then click the Secure Settings tab.

Compress print data



To compress the print job data file that is stored on the Secure server, check this box. It is important to select this option if you will be sending large files to the Secure server as there is a 2 GB limit on the size of the print job.

Enable Follow Me printing

Check this box to enable Follow Me printing.

When Follow Me printing is enabled, your users may release their secure print job to an alternate MFP, rather than the one to which the user originally printed.

Offline behavior

Choose how to manage disconnected or "Offline" jobs, which only occurs if, for some reason, the Print Audit Secure Client is not able to connect to the Print Audit Secure Windows service on the server, at the time a print job is created.
Allow - Print jobs will print as they would if Secure is not installed.
Disallow - No printing to secure printers will be allowed.
Prompt - Users are prompted at the workstation to cancel, or print the job unsecured.

Enable automatic expiration of jobs

Expired jobs are removed from the secure print queue and are no longer visible or available for release. It is recommended that you enable automatic expiry of jobs to prevent the queue from becoming congested with abandoned jobs that will not be released.

To automatically expire jobs of a specified age, check this box.

Duration after which jobs automatically expire

Enter the length of time in days, hours, or minutes, after which the jobs should expire.

Enable automatic purging of jobs

When a secure print job expires, or is cancelled by the user, statistical information about that job is retained by Print Audit Secure for reporting purposes. The automatic purging of jobs will remove cancelled and expired jobs completely. Plan only to purge jobs if they are no longer required for statistic reporting. Purging jobs does not affect any pending jobs being held for secure release.

To automatically purge expired jobs from Print Audit Secure check this box.

Duration after which expired jobs are automatically purged

Enter the length of time, in days, hours, or minutes, after which the jobs should be purged.

> **Important!**
>
> Once jobs have been purged from Print Audit Secure there is no way to recover them. Purged jobs will not be included in the job statistics report.

Click the Save button to save these settings.

5. Licensing

Activation

To access the Print Audit Secure Licensing page, log into the Print Audit Secure server, and from the Top menu, select

>Setup >Licensing.

The licensing page is used to activate your license key or request a trial license.

If you have purchased seats of the Print Audit Secure, choose this radio button and enter the Company and License Key.

Request a trial license

If you have not purchased the software but would like to evaluate Print Audit Secure, select this radio button, complete all fields and click Submit.

The trial license enables the secure tracking of up to 5 printers for 15 days.

6. Managing Printers

Printer Manager

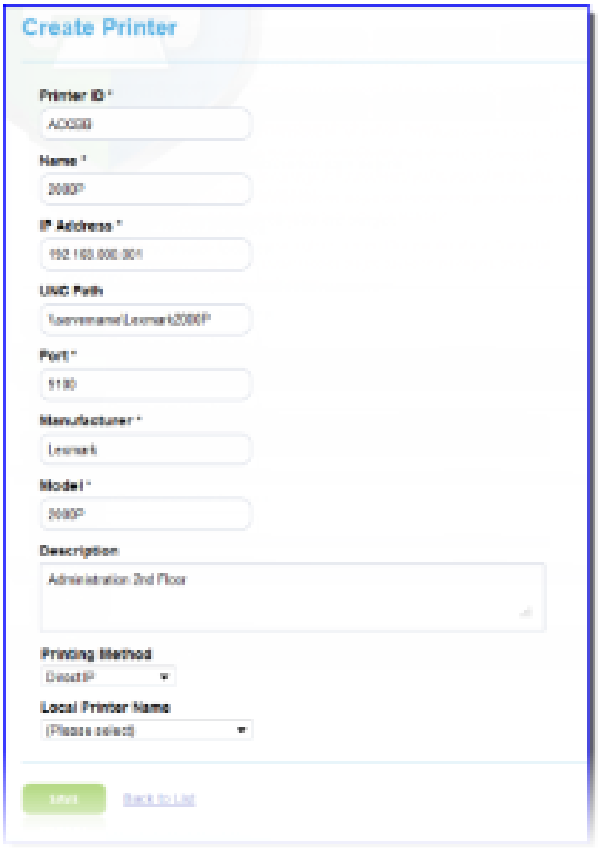
The Printer Manager manages printers that are designated as secure printers. Print Audit Secure is compatible with all networked printers. Printers can be either imported from a comma separated values (CSV) file or manually entered individually.

Import printers from a CSV file

Print Audit Secure will accept a CSV file to import printers.

1. Create a CSV file that contains the list of printers - CSV File Format: (printer ID), (name of the device), (IP address), (port), (manufacturer), (model name), (UNC path), (description of the device), (Printing Method - Direct IP or Windows Spooler), (Local Printer Name). Note: UNC Path, description of the device, Printing Method, and Local Printer Name are optional.
2. Go to www.YOURSERVERNAME\printauditsecure (http://www.YOURSERVERNAME\printauditsecure). Log into the Print Audit Secure Administrator
3. Click on Setup, and then select Printer Manager.
4. Click the Import button and find the CSV file with the printers which will be designated as secure.
5. Click Open then the Ok button.

Add a printer manually



In the Secure Administrator, click on Setup, and then select Printer Manager.

Click on the Create New button.

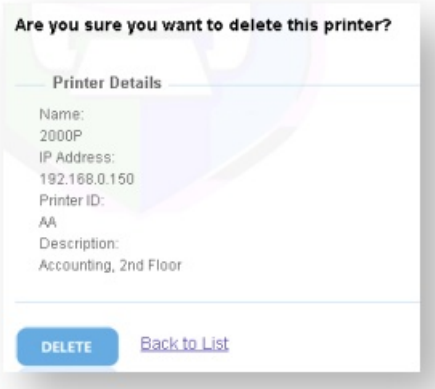
1. **Printer ID** - Enter a Printer ID that is between 3 and 50 characters long. This is a required field. It is recommended to use a similar naming convention for all secure devices, such as an abbreviation of where the device is physically located, or some other unique identifier.
2. **Name** - Enter the name of the device. This is a required field.
3. **IP Address** -Enter the IP address of the device. This is a required field
4. **UNC path** - Enter the UNC path. This field is optional.
5. **Port** - The default is 9100, but can be modified if required. The port will be determined by whichever port the printer is set to use. This is a required field.
6. **Manufacturer/Model/Description** - Enter the Manufacturer name and Model Name. These are required fields. The Description of this device is not a required field
7. **Printing Method** - Select from the drop down menu to determine how the print job will be released to the printer.

8. **Local Printer Name** - This drop down list will contain a list of printers defined on the server, and when used with Windows Spooler as the Printing Method, will release jobs to the spooler , to that printer.
    a. Direct IP:, The job will be sent to the printer using TCP/IP and the defined IP address and port.
    b. Windows Spooler: Print Audit Secure will spool the job to the printer selected under Local Printer Name

Edit a printer

1. In the Print Audit Secure Administrator, click on Setup, then Printer Manager.
2. Click the Edit link beside the device which is to be modified.
3. Make the required changes. Click the Save button.

Remove a Printer



A printer cannot be removed if there are any pending jobs still secured on the server. You must delete all the secured print jobs to the printer prior to deleting it. When you remove a printer from Print Audit Secure printer list, any print jobs sent to this printer will no longer be secured.

1. In the Print Audit Secure Administrator, click on Setup, then Printer Manager.
2. Click the Delete button next to the device which is to be removed.

3. Click the Delete button on confirmation page to remove this group.
4. A confirmation is provided, explaining that the printer has been removed.

Compatible Printer Groups

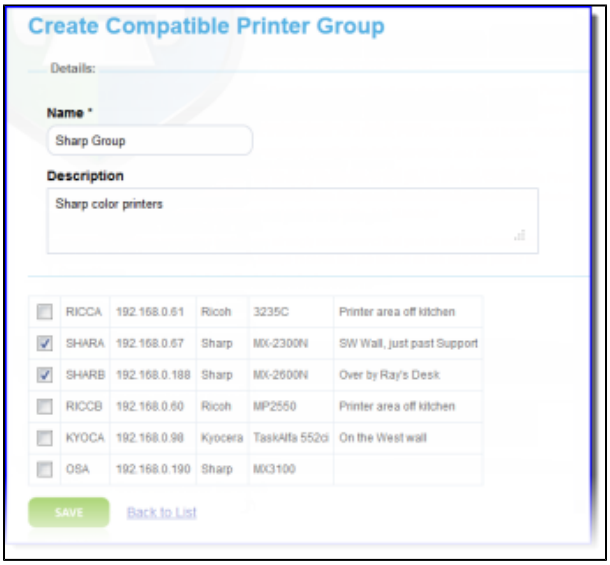
The Print Audit Secure Compatible Printer Groups are used to group similar devices together, so that users can release jobs to any compatible device. When selecting devices for your Compatible Printer Groups, it is important to ensure that the printer drivers within a group are compatible. Compatible drivers are required in order to make sure that a print job that was sent to one printer will print out as expected on another device. Compatible drivers will ensure that the printers within the group can translate the datastream in the print job. Printers can be placed in more than one Printer Compatibility Group.
When Compatible Printer Groups are defined, the user will be able to identify in the Web Release Station, the jobs that are compatible with the printer where they wish to release their job.

Recording jobs in the Print Audit 6 database

When using Print Audit Secure with Print Audit 6, remember that the job is always recorded in the Print Audit 6 database with the original printer attributes (printer name, color usage, job validation, etc) rather than those associated with the final printout.

For example, if an original job was sent to a printer as a color job, but the device where it was released is monochrome only, the job will still be charged and recorded in the Print Audit 6 database as a color job. This will also hold true for jobs with finishing attributes, such as stapling, which are released to a device that does not support the originally requested finishing option.

Create a Compatible Printer Group



1. Log into the Print Audit Secure Administrator. In the top menu, select Setup, then select Compatible Printer Groups.

2. Click the Create New button.
3. Enter a Name for the Compatible Printer Group. This is a required field and can be up to 50 characters long.
4. Enter a Description for the Printer Group. The description can be up to 100 characters long.
5. Select the devices from the list that belong in this group. Click the Save button.

Edit a Compatible Printer Group

There is an option to edit the Compatible Printer Group Name, Description, and add or remove devices for this group.

1. In the Print Audit Secure Administrator, go to the Compatible Printer Groups.
2. Click the Edit button next to the Compatible Printer Group you want edit.
3. Make the required changes.
4. Click the Save button.

Remove a Compatible Printer Group

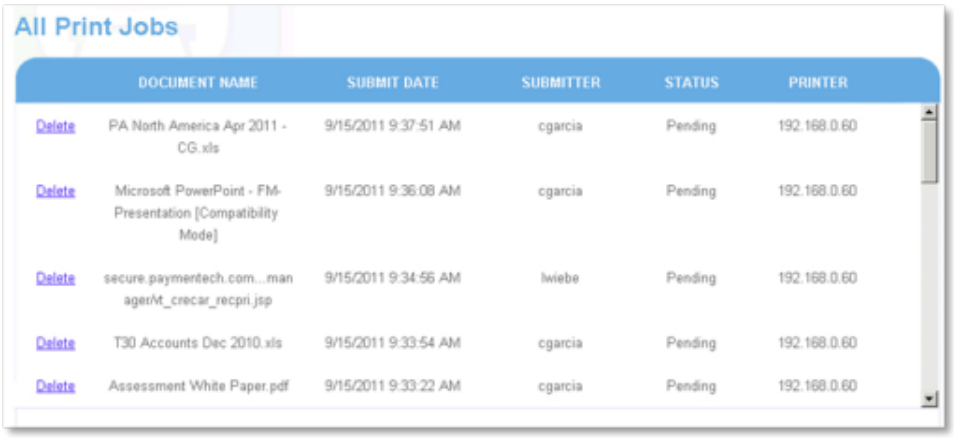
Once you remove a Compatible Printer Group, it will be permanently removed from Print Audit Secure. All the printers that were in the group will not be removed, however, they will no longer show as compatible with the other devices that were in this group. If you would like to reinstate this group you will need to create a new Printer Compatibility Group.

To remove a Compatible Printer Group:

1. In the Print Audit Secure Administrator, go to the Compatible Printer Group Manager.
2. Click the Delete button next to the Compatible Printer Group you want remove.
3. Click the Delete button on confirmation page to remove this group.
4. You will receive a confirmation that the Compatible Printer Group has been removed

7. Managing Print Jobs

Manage All Print Jobs



The Print Job Manager is a way for Print Audit Secure Administrators to cancel any pending jobs that have not been released. Once logged into the Print Audit Secure Administrator, you will see a list of pending jobs, the name of the document, the date it was submitted, the user who submitted the job, the status of the job and original printer that the job was submitted to.

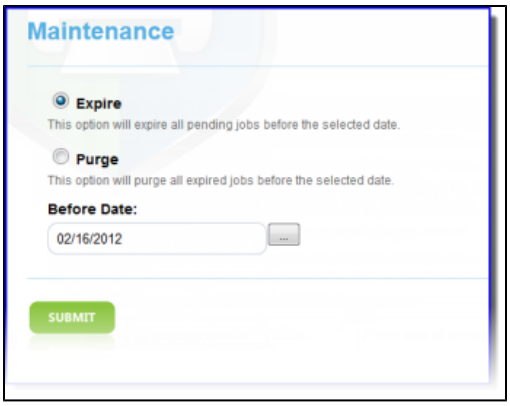
1. Log into the Print Audit Secure Administrator. From the top menu select Manage Print Jobs, then select All print jobs.
2. To Delete any job, click the Delete button next to the print job you would like to remove and then Select Delete on the confirmation page. Once the job has been cancelled it will be permanently removed from Print Audit Secure
3. To return to the job list without deleting the job, select Back to List.

Manage My Print Jobs

Print Audit Secure Administrators will always log into the Print Audit Secure Server. To release your own jobs as an Administrator you must go to My Print Jobs.

1. Log into the Print Secure Server.
2. Click on Manage Print Jobs, My Print Jobs.
3. Enter the Print ID of the device you want to release the job to.
4. If the printer you choose is compatible with the original printer you sent the job to you will have the option to release or cancel the job. If the original printer is not compatible with the original printer you sent the job to you will only have the option to cancel the job.

Maintenance



The Maintenance page allows an administrator to mass expire and purge jobs at any time. Expiring and purging jobs will affect the Print Statistics report; expired jobs will be considered a cancelled job and purged jobs will never be reported on.

Once print jobs have been expired or purged, there is no way to undo the change.

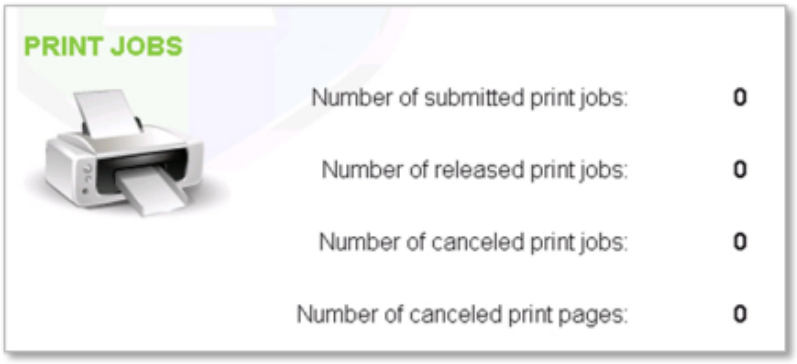
1. Log into the Print Audit Secure Administrator. Click on Manage Print Jobs and select Maintenance.
2. Choose either Expire or Purge.
3. Enter the date that you would all jobs older than to expire or purge. Click the Submit button.
4. You will receive a message confirming this, click the Ok button.

Printing Statistics

There are three reports that are available. (If you are not using Print Audit Secure in conjunction with Print Audit 6 the Cost Savings and Environmental Impact sections are not accessible.)

Print Jobs

This report shows a summary of the total number of jobs sent to the Print Audit Secure server, the number jobs released and the number of jobs canceled. If you are also using Print Audit 6 then you are also able to see the number of pages that have been canceled.



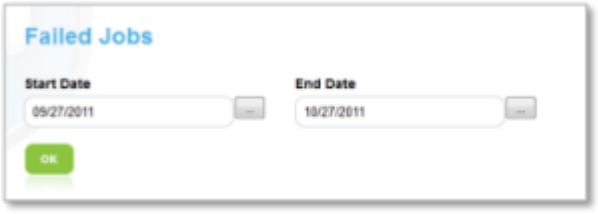
Cost Savings

This section of the report is only available when using Print Audit 6 in conjunction with Print Audit Secure. It shows the total cost savings from unreleased print jobs.

Environmental Impact

This report is only available when using Print Audit 6 in conjunction with Print Audit Secure. It shows the environmental impact your company has made by not releasing unwanted jobs. For example, on average 8,333 unreleased pages will save one tree.

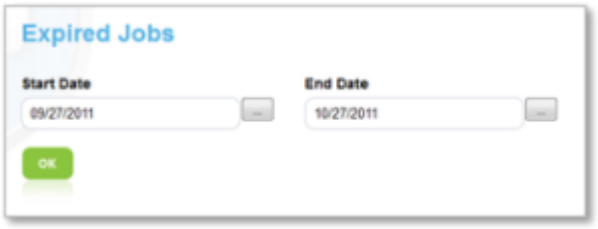
Failed Jobs



Failed jobs are any jobs that were successfully sent to the Secure server but were not successfully released from the printer. These jobs will not be removed from Print Audit Secure until they have been successfully released.

1. Log into the Print Audit Secure Server. Click on Reporting and then Failed Jobs.
2. Select your Start Date and your End Date.
3. Click the OK button. A list of failed jobs will show below.

Expired Jobs



Expired jobs are print jobs that have been expired by the Print Audit Administrator or automatically expired because they have been in the Secure server longer than the time period specified by the Print Audit Secure Administrator.

1. Log into the Print Audit Secure Server. Click on Reporting and then Expired Jobs.
2. Select your Start Date and your End Date.
3. Click the OK button. A list of expired jobs will show below.

Step-by-Step Instructions

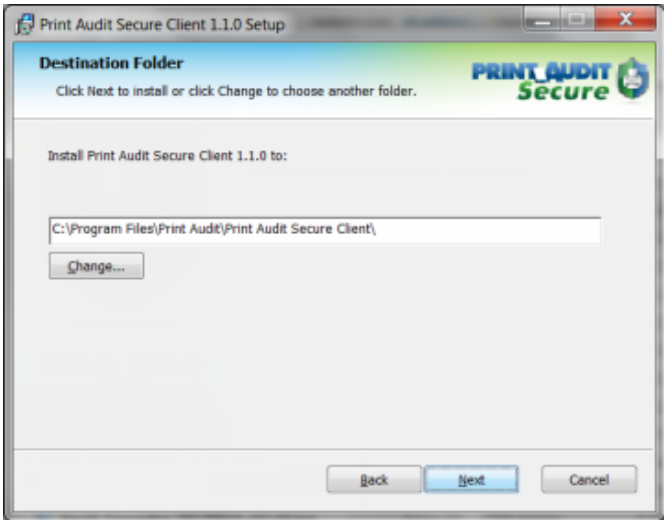
1. Download the SecureClientSetup.exe file from www.printaudit.com

2. Double click on the SecureClientSetup.exe file to begin the installation.

3. On the "Welcome to Print Audit Secure Client Setup Wizard" window click Next.

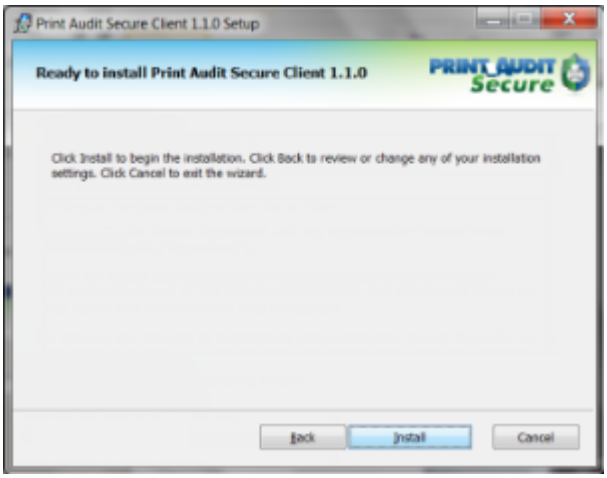
4. Read the End User License Agreement and select the checkbox if you accept. Click Next.

5. Select the location where you want to install the Secure Client or choose the default location by clicking Next.



6. Configure the Secure Client to communicate with the Print Audit Secure web server and click Next. (http://*servername*/pasecure/webservices replacing servername with the name of the Print Audit Secure Server.)

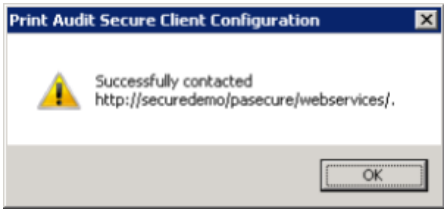
7. Click Install.



8. Once the setup wizard has completed the install click Finish.

9. Verify that the client and server can communicate.

- Click Start > All Programs > Print Audit Secure > Secure Client Config
- Click the Test URL button in the bottom left of the Print Audit Secure Client Configuration window.
- You should receive a dialogue box saying successfully contacted http://*servername*/pasecure/webservices/. Click OK.



Self-generated PINs

Users may be provided the ability to generate a PIN through the PIN generating capabilities at the Web Release Station, or at supported embedded MFPs.

Administrative Configuration

The Administrator must enable the generation of PINS by selecting the Generate Pin Attribute checkbox on the Secure Server Configuration page. The length of the Pin can also be configured here. Please note, the generated Pin will be numeric.

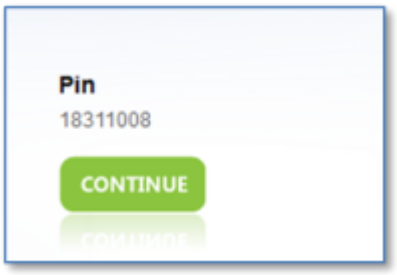
Web Release Station workflow

Once the Administrator has configured the option to generate a Pin attribute, a user who does not have a Pin, can generate a Pin by us the Web Release Station. At the Web Release Station, the user will select the Forgot pin option

The user will then be prompted to log in using Active Directory credentials


Username
Password
LOGIN

Upon successful log in, a numeric Pin will be generated by Print Audit Secure and presented to the user.



The user then has Pin access to the release jobs.

Embedded MFP workflow

When a user attempts to use an unregistered swipe card Print Audit Secure detects that the card is not registered and the user will be redirected to the username/password authentication page. The user will see the message,

“Please enter your credentials in order to register swipe card.”

The user then enters their credentials and presses the login button. The swipe card will then be registered to that user.

The user has two minutes or until machine times out, whichever comes first, to complete entering their credentials. After entering their credentials, normal authentication will occur.

11. Appendix

Installation Note 1 – Active directory error

In the event that an error was made in defining Active Directory login information, and the result is a blank display with no connection, it may be necessary to change settings and restart the application . This may require changes to the configuration for the application and only should be accomplished by a trained installation technician.

Open app.config from the Config folder of the installed application and change:

<add key="LdapServer" value="<value>"/> to <add key="LdapServer" value=""/>

<add key="LdapDomain" value="<value>"/> to <add key=" LdapDomain " value=""/>

<add key="NetBiosDomain" value="<value>"/> to <add key=" NetBiosDomain " value=""/>

(Remove the value from the value tag).

Save the changes.

Restart IIS on the server.

12. IIS Configuration/Setup for Print Audit Secure Server

Please note that this document is meant as an aid to installing and configuring IIS /. NET 4 for use with Print Audit Secure Server rather than a step by step guide. The actual sequence of steps will depend on the components installed on the server and the order in which they have been installed. Modifications to an existing IIS installation should be done by a qualified administrator.

Installing .NET version 4

Print Audit 6 Secure Server requires .NET Framework version 4. Please note that .NET should be installed prior to installing IIS. If it is not installed first, it may be necessary to use the " aspnet_regiis -ir" registration utility.

IIS 6 (Server 2008)

.NET version 4 isn't included by default with Server 2008. It can be downloaded from Microsoft's web site.

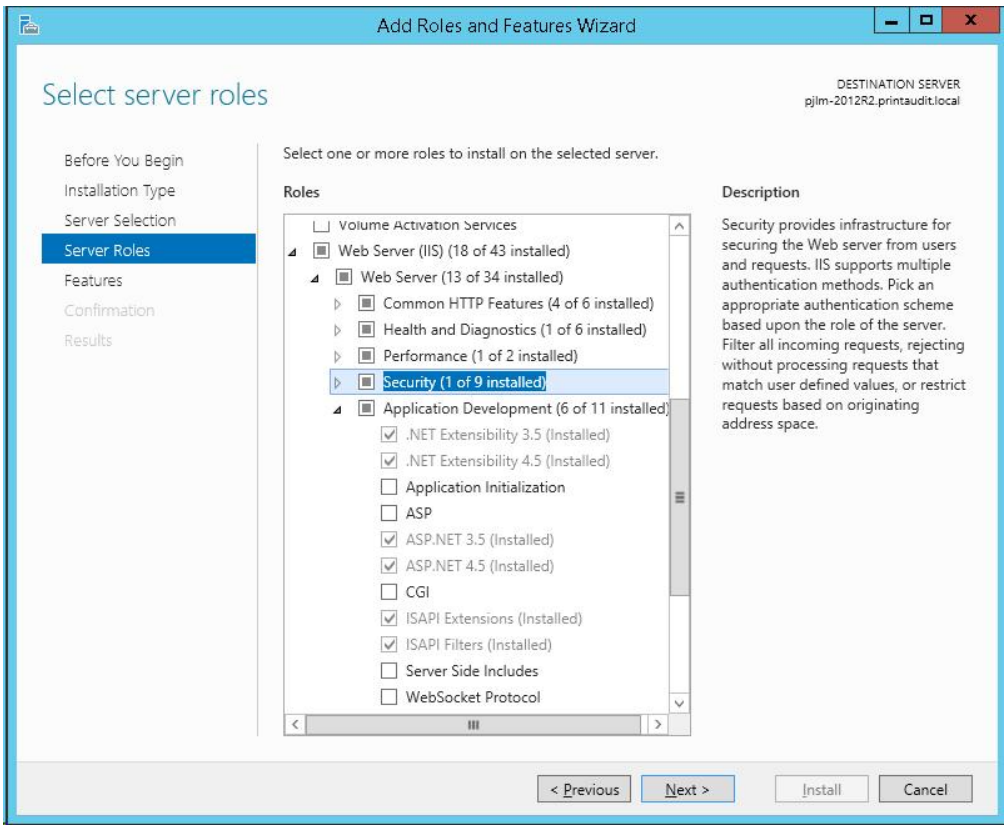
IIS 7 or higher (Server 2012 and higher)

.NET version 4 is added as a Feature using the "Add Roles and Features Wizard".

Installing IIS Components

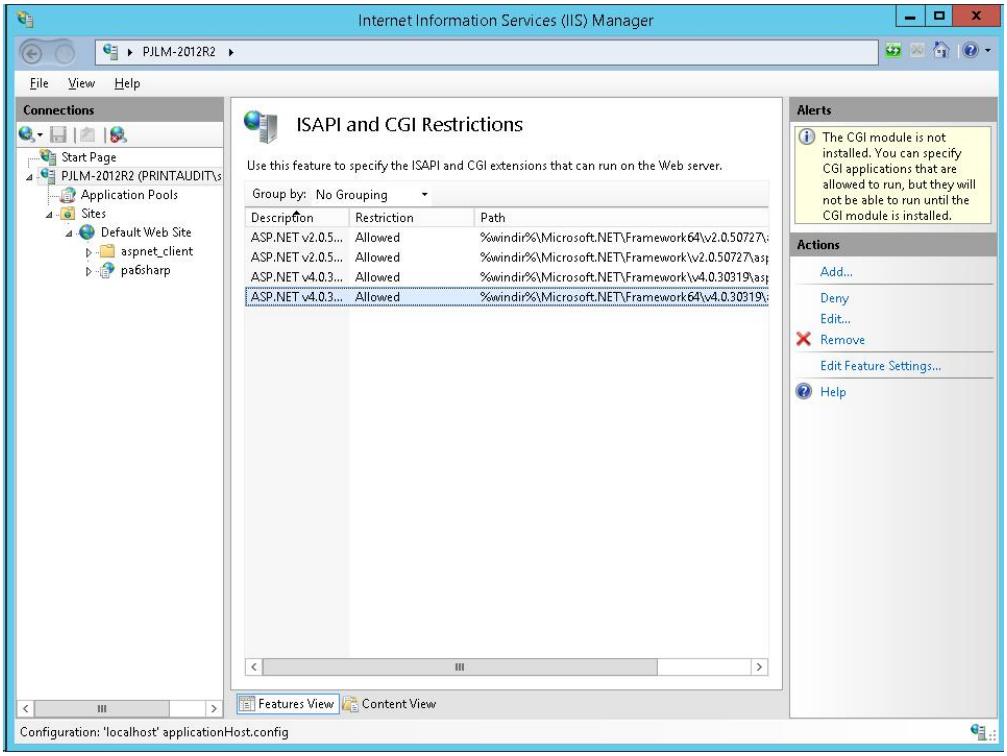
Print Audit 6 Secure Server requires that IIS version 6 or higher be installed first. The following components are required above the base IIS installation:

Application Development



Allowing the ASP.NET Version 4 Extension

The ASP.NET version 4 extension needs to be allowed before it can be used. This is done using the Internet Information Services (IIS) Manager under "ISAP and CGI Restrictions".



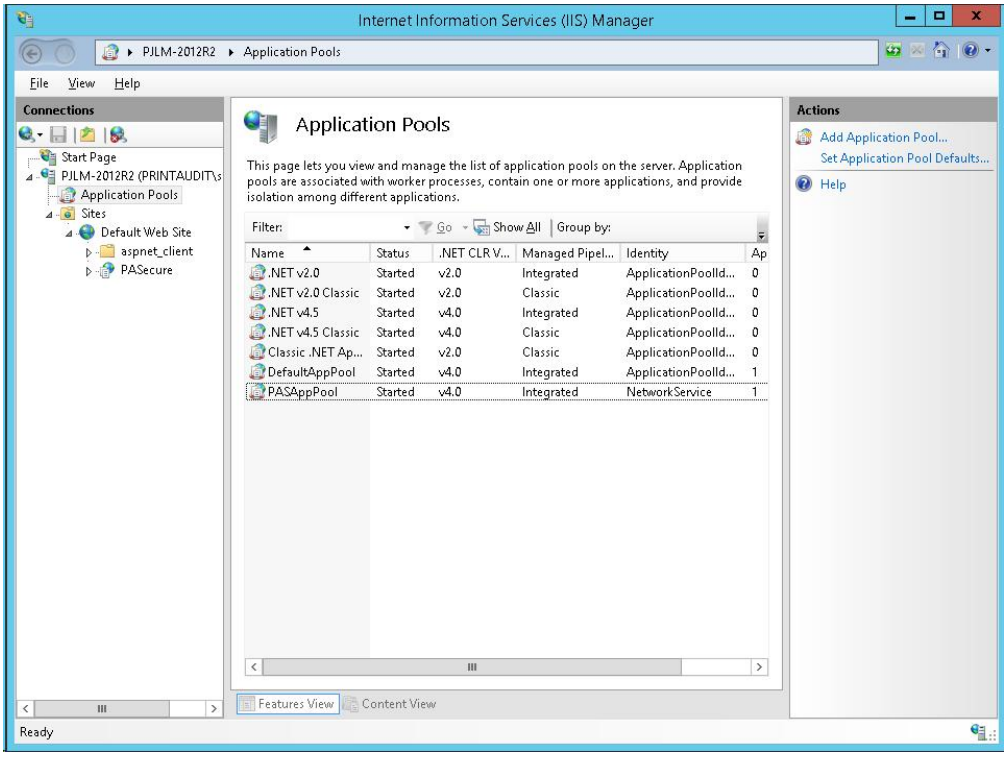
Please Note: The Print Audit 6 Secure Server Setup Wizard is designed to configure settings in IIS when it is run. However, depending the environment, it may be necessary to verify or modify those settings. The examples presented in this guide are based on the default installation options. Please contact your System Administrator for additional details should changes to these defaults be required in your environment.

Verifying Application Pools

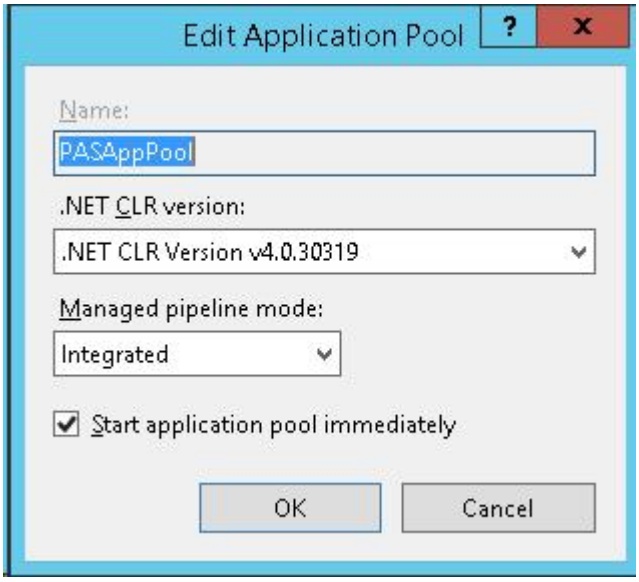
Application Pools in IIS allow different ASP.NET applications running on the web server to be isolated from each other. Errors in one application pool will not affect other applications running in other application pools. Print Audit 6 Secure Server installs an application pools - PASAppPool - running under .NET Framework v4.0.30319.

To verify that the Application Pool has been installed and configured correctly:

1. Open the Internet Information Services (IIS)Manager.



2. Under the IIS server name, "Application Pools".
3. Double click on the Application Name.



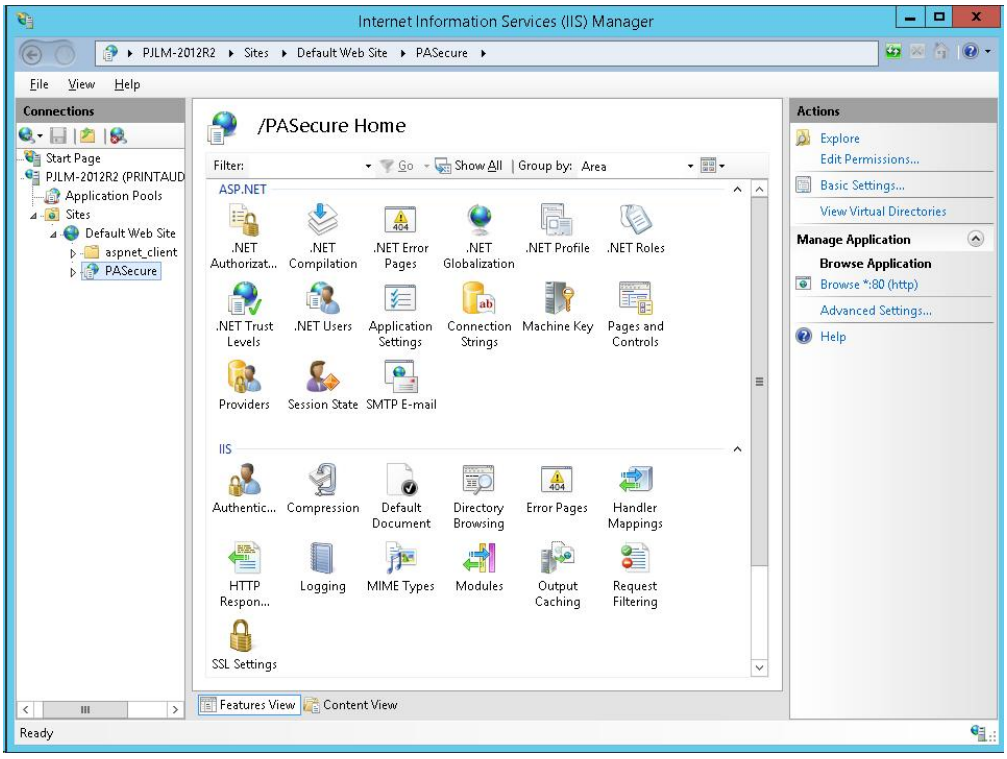
4. Use the dropdown ".NET Framework version" to select the appropriate version.

Verifying Application Pools used by Print Audit 6 Secure Server

The Print Audit 6 Secure Server creates a web site under "Default Web Site" by default - PASecure

To verify the Application pool used by a site:

1. Open the Internet Information Services (IIS) Manager.



2. Locate the web site under "Sites" and highlight it. By default, the Print Audit Secure Server sites are under "Default Web Site".
3. Under "Action" (located on the right hand side of the IIS Manager), click on "Basic Settings..."