DATAMINE

PRODUCTION ACCOUNTING

Production Accounting 2.0.1

Installation Guide

Published: Thursday, 4 December 2025

Contents

Get Help with Production Accounting 6

Overview 7

- Production Accounting Features and Benefits 8
  - Key Features 8
  - Key Benefits 8
- System Requirements for Production Accounting 9
  - Production Accounting Application Server 9
  - Production Accounting Database Server 10
  - Production Accounting Clients 11
  - Configuration 11
  - Virtualisation 11
- System Configuration before Installing Production Accounting 12
  - Application Server 12
  - Database Server 12
  - Regional Settings 13
  - Daylight Saving Settings 14
  - Event Viewer 15
  - Service Account Permissions 16
  - Add Network Service to the Group or User Names List 17
  - Security 18
  - Microsoft .NET Framework 20
  - Internet Information Services (IIS) 21
  - Microsoft .NET Core 23
  - Microsoft URL Rewrite 24
  - Microsoft Message Queuing (MSMQ) 25
  - Microsoft Distributed Transaction Coordinator (MSDTC) 26
  - Self-signed Certificate Creation 28
  - Microsoft SQL Server 31

Production Accounting Installation 37
Integration with other Intelligent Mining Solutions applications 37
Production Accounting Installation on the Application Server 37
Production Accounting Configuration on the Application Server 37
Production Accounting Databases 38
Production Accounting Services 38
Production Accounting File Structure 39
Default Port Numbers 41
PA Framework 41
PA Core 41
Required IIS Configuration 42
Optional IIS Configuration for Non-Production Environments 49
Database Creation 50
JKMetAccount Installation 55
Edit the Web.config File 58
Edit the Bootstrap.config File 65
Edit the PA Core App.config.json and Appsettings.json Files 68
Production Accounting Notification Service 70
Production Accounting Audit Service 73
Production Accounting Logging Service 78
Production Accounting Time Service 82
Message Queue Permissions 85
IMS Integration Hub Message Queue Configuration 87
Configuration Editor Installation 89
Start up Production Accounting 90
Permissions Editor Installation 91
Production Accounting Analytics Installation 93
Analytics Installation Prerequisites 93

Set up Production Accounting Analytics 93
Internet Browser Configuration 101
Self-Signed Certificate Trust in Edge 101
Pop-ups 103
Email Notification Configuration 104
Email Notification Prerequisites 104
Enable Email Notifications 110
Upgrade Production Accounting 114
Upgrading from 2.0.0 or earlier 114
Upgrading from 1.14.0 or earlier 114
Upgrading from 1.13.2 or earlier 114
Upgrading from 1.13.1 or earlier 116
Upgrading from 1.12.4 or earlier 117
Upgrading from 1.12.3 or earlier 118
Upgrading from 1.12.0 or earlier 119
Upgrading from 1.9.1 or earlier 119
Upgrading from 1.8 or earlier 121
Disaster Mitigation and Recovery 122
Important Considerations 122
Production Accounting Maintenance 124
Recover Messages from Dead-Letter and Poison Queues 125

Get Help with Production Accounting

Online product documentation for Production Accounting is available at https://docs.dataminesoftware.com/ProductionAccounting/.

For further information about installing or using Production Accounting, check your contract with Datamine to determine whether site-specific documentation was supplied to your site.

Datamine's commitment to customer service provides our customers with access to a skilled and responsive support team. The global customer support team ensures all customer questions and issues are addressed in a timely manner and escalated as required to ensure resolution.

You should always contact Datamine support if you have an issue. Do not contact individual members of Datamine for support because your issue may not be responded to in a timely manner if that person is unavailable.

If you are a licensed Production Accounting user, you can request support via the:

- Datamine Support Email support@dataminesoftware.com.
- Support Portal https://www.dataminesoftware.com/support/

We also welcome feedback about this documentation.

Overview

This section describes Production Accounting functionality and technical requirements.

> **Important:** If you intend to copy any code snippets from this Installation Guide, open the Installation Guide in Adobe Reader or similar rather than viewing the file in an internet browser.

> **Note:** Instructions for Windows Server administration activities match Windows Server 2022.

Production Accounting Features and Benefits

Production Accounting provides a complete production accounting solution designed for mining, mineral processing, smelting, and refining operations.

Key Features

Production Accounting addresses key production accounting challenges by providing the ability to take on production data from various sources. The solution provides:

- System workflow to manage authorisation and publishing
- Validation routines for identifying data with low integrity
- Quarantine and review/reject functionality
- Web logsheets for manual data entry
- Multiple processing routines, including check-in/check-out, cascading calculations and statistical data adjustment
- Data audit trails

Key Benefits

Production Accounting provides the flexibility to cater to diverse site and business requirements, while enabling a corporation to use a single solution across its operations. Production Accounting:

- Facilitates a change in business philosophy from past accounting for mass to future accounting for metal content
- Supports proactive risk management
- Enables timely and accurate recognition of revenue
- Enhances production performance measurement
- Provides a key input for bonus scheme calculation
- Enables improved production planning and forecasting
- Produces timely and relevant production information for monthly financial reporting
- Increases accuracy in matching production costs to various parts of the production process
- Assists in the calculation of royalty payments

System Requirements for Production Accounting

Important: System specifications and disk space requirements depend on anticipated data volumes and growth. Datamine recommends a scoping study to determine exact requirements. Testing or training environments must not be set up on the same server as the production environment, in order to reduce the load on the production server and isolate it from potential issues in other environments. For high-availability solutions additional hardware is required. This should be discussed with your Datamine representatives during the implementation study/budgeting phase.

Production Accounting Application Server

CPU	6 cores
Operating System	Windows Server 2019 / 2022
Memory	32 GB RAM
Storage	50 GB (Operating System) 70 GB (software and logs) 150 GB (working directory)
Network	1 Gbit LAN network link or better to Database Server
.NET	.NET Framework 3.5 and .NET Framework 4.8 ASP.NET Core 8.0 Runtime Windows Hosting Bundle including ASP.NET Core Module (ANCM) for IIS
Utilities	• WinZip or 7-Zip • `bcp.exe` and `sqlcmd.exe` [1]
Other	• Microsoft Internet Information Services (IIS) [2] • Microsoft Distributed Transaction Coordinator (MSDTC) • Microsoft Message Queuing (MSMQ) [3] • Time zone configuration must be the same as the Database Server and Reporting Server • Server Daylight Saving setting must be correctly configured based on region and Production Accounting configuration [4]

[1] Required for configuration deployments done via the Application Server
[2] Version to suit the Operating System

[3] Version to suit the Operating System and .NET

[4] Daylight saving support is not currently available for all configurations. Please discuss daylight saving configuration requirements with a Datamine representative.

Production Accounting Database Server

CPU	8 cores
Operating System	Windows Server 2019 / 2022
Memory	32 GB RAM
Storage	50 GB (Operating System) 400 GB (databases) [1] 600 GB (working directory for backups and temporary databases used during upgrades)
RDBMS	Microsoft SQL Server 2017 / 2019 / 2022 (with supported compatibility level from 130)
Network	1 Gbit LAN network link or better to Application Server
Other	• Microsoft Distributed Transaction Coordinator (MSDTC) • SQL Server Reporting Services (SSRS) • Microsoft SQL Server Management Studio • WinZip or 7-Zip • Time zone configuration must be the same as the Application Server and Reporting Server • Server Daylight Saving setting must be correctly configured based on region and Production Accounting configuration [2]

[1] Actual storage requirements depend on the size of the Production Accounting configuration.

[2] Daylight saving support is not currently available for all configurations. Please discuss daylight saving configuration requirements with a Datamine representative.

Production Accounting Clients

Operating System	Windows 11
Memory	8 GB RAM
Browser	Microsoft Edge with pop-ups enabled

Configuration

The computer used to create and modify the Production Accounting configuration must have Microsoft Excel installed.

The computer used to deploy the Production Accounting configuration must have `bcp.exe` and `sqlcmd.exe` available. These utilities are included as part of SQL Server or the Microsoft Command Line Utilities.

These computers may be the Application Server, the Database Server, a Production Accounting Client, or a consultant's computer.

Virtualisation

Virtualisation technology is widely used with good results for Production Accounting. This includes server virtualisation, application virtualisation, and cloud-based virtual environments provided by vendors such as Microsoft, VMWare, and Amazon. We take advantage of some of these technologies in our own development environments. No conflicts have been reported; however, due to the wide variety of vendors and technologies, Datamine is unable to test all virtualisation possibilities and therefore cannot offer explicit support for any of them.

System Configuration before Installing Production Accounting

The following system configuration must be completed before installing Production Accounting.

> **Important:** Before installing Production Accounting, ensure all relevant Windows updates have been applied to the Application Server and Database Server.

Application Server

- Regional settings
- Daylight saving settings
- Event Viewer
- Network Service Permissions (optional)
- .NET Framework
- Security
- Internet Information Services (IIS)
- .NET Core
- Microsoft URL Rewrite
- Microsoft Message Queuing (MSMQ)
- Microsoft Distributed Transaction Coordinator (MSDTC)

Database Server

- Regional settings
- Daylight saving settings
- .NET Framework
- MSDTC
- Microsoft SQL Server

Regional Settings

The Application Server and the Database Server must have the same regional settings.

To confirm the regional settings:

1. Open the Windows **Control Panel**.
2. View by icons (rather than by category).
3. Select **Region**.

   The **Region** screen displays.
4. Confirm that all preferences on the **Formats** tab match on both servers.
5. Click **OK**.
6. Close the **Region** screen.

Daylight Saving Settings

Both the Application Server and the Database Server must have the correct setting for daylight saving based on region and the Production Accounting configuration.

Production Accounting 1.13.2 introduces initial updates for daylight saving support. By default, Windows enables automatic adjustment of the system time for daylight saving. Therefore, for most Production Accounting configurations, no manual adjustments to server daylight saving settings are required.

However, if your Production Accounting configuration requires hourly periods for data, daylight saving may not be supported and automatic adjustment for daylight saving may need to be disabled on the Application Server and Database Server.

> **Note:** Please discuss daylight saving configuration requirements with a Datamine representative.

To configure daylight saving time settings:

1. Open the Windows **Control Panel**.
2. View by icons (rather than by category).
3. Select **Date and Time**.

   The **Date and Time** screen displays.
4. Click **Change time zone**.

   The **Time Zone Settings** screen displays. If the selected time zone has potential daylight saving time, there is an **Automatically adjust clock for Daylight Saving Time** checkbox on the screen.
5. Configure the **Automatically adjust clock for Daylight Saving Time** setting as required. If your Production Accounting configuration uses daylight saving support functionality, ensure that the checkbox is selected. Otherwise, if not required, deselect the checkbox. Default: *Selected*.
6. Click **OK**.
7. Close the **Date and Time** screen.

Event Viewer

Production Accounting creates messages that are stored in the Windows Event Viewer. The Event Viewer must be configured on the Application Server to allow events to be overwritten.

To allow events to be overwritten in the Event Viewer:

1. Open the Windows **Control Panel** on the Application Server.
2. View by icons (rather than by category).
3. Select **Administrative Tools**.
4. Double-click **Event Viewer**.

   The **Event Viewer** screen displays.
5. Expand the **Event Viewer » Windows Logs** node.
6. Right-click the **Application** node and select **Properties** from the menu.

   The **Log Properties - Application** screen displays.
7. Select the **General** tab.
8. Select **Overwrite events as needed (oldest events first)**.
9. Click **OK**.
10. Close the **Event Viewer**.

Service Account Permissions

If Production Accounting services are to write events to the Application log, the service account on the Application Server must be given access to Event Viewer.

> **Note:** In a default installation of Production Accounting, either a domain account or the Network Service account can be the main account for accessing the required resources.

To verify that the Network Service account can access Event Viewer:

1. Open the Windows **Registry Editor** on the Application Server.
2. Expand the **HKEY_LOCAL_MACHINE » SYSTEM » CurrentControlSet » Services** node.
3. Right-click the **EventLog** node and select **Permissions** from the menu.

   The **Permissions for EventLog** screen displays.
4. Select the **NETWORK SERVICE** account.

   > **Note:** See how to add Network Service to the **Group or user names** list below if required.
5. Select the following permissions. All other permissions should be cleared.

   Full Control—Allow

   Read—Allow
6. Click **OK**.

   The **Permissions for EventLog** screen closes.
7. Expand the **HKEY_LOCAL_MACHINE » SYSTEM » CurrentControlSet » Services » EventLog** node.
8. Right-click the **Security** node and select **Permissions** from the menu.

   The **Permissions for Security** screen displays.
9. Select the **NETWORK SERVICE** account.
10. Select the following permissions. All other permissions should be cleared.

    Full Control—Allow

    Read—Allow
11. Click **OK**.

    The **Permissions for Security** screen closes.
12. Close the **Registry Editor**.

Add Network Service to the Group or User Names List

This activity is included in this Installation Guide for reference purposes only. The Network Service may need to be searched for on the local machine.

Selecting the Network Service may be required in the following activities as an alternative to using a domain account:

- Network Service Permissions
- Production Accounting File Structure
- Message Queue Configuration

If NETWORK SERVICE is not in the Group or user names list:

1. Click **Add**.

   The **Select Users or Groups** screen displays.
2. Confirm that the object types list includes **Built-in security principals**. If required:
   a. Click **Object Types**.

      The **Object Types** screen displays.
   b. Select **Built-in security principals**.
   c. Click **OK**.

      The **Object Types** screen closes.
3. Confirm that the location is the name of the local machine. If required:
   a. Click **Locations**.

      The **Locations** screen displays.
   b. Select the name of the local machine.
   c. Click **OK**.

      The **Locations** screen closes.
4. Enter **NETWORK SERVICE** in the **Enter the object names to select** field.
5. Click **Check Names**.

   The **NETWORK SERVICE** name is underlined.
6. Click **OK**.

   The **Select Users or Groups** screen closes.

Security

Complete the following activities to enhance security on the Application Server.

Disable 8dot3 name creation:

1. Open Windows **Command Prompt** with administrator permissions.
2. Run the following command.

```
fsutil behavior set disable8dot3 1
```

> **Note:** By default, Windows creates hidden file names in the 8dot3 format for files with longer names. If this registry entry is edited after the Production Accounting has been installed, to delete previously created 8dot3 hidden file names:
>
> 1. Copy the `Portal` directory.
> 2. Delete the original `Portal` directory.
> 3. Rename the copied directory to have the original name and location.

Disable NetBIOS:

1. Open the Windows **Control Panel** on the Application Server.
2. View by icons (rather than by category).
3. Select **Network and Sharing Center**.
4. Click the hyperlinked network connection name.

   The **Status** screen for the network displays.
5. Click **Properties**.
6. In the list of items that the connection uses, select **Internet Protocol Version 4**.
7. Click **Properties**.
8. Click **Advanced**.
9. Select the **WINS** tab.
10. In the **NetBIOS setting**, select *Disable NetBIOS over TCP/IP*.
11. Click **OK** to close each window, and close the **Status** screen for the network.

Disable Server Message Block (SMB):

1. Open the Windows **Control Panel** on the Application Server.
2. View by icons (rather than by category).
3. Select **Network and Sharing Center**.

4. Click the hyperlinked network connection name.

   The **Status** screen for the network displays.
5. Click **Properties**.
6. In the list of items that the connection uses, uncheck the following drivers:
   - **Client for Microsoft Networks**
   - **File and Printer Sharing for Microsoft Networks**

   > **Note:** Do not disable **File and Printer Sharing for Microsoft Networks** if files need to be copied to the Application Server; for example, for integration.
7. Click **OK**, and close the **Status** screen for the network.

Microsoft .NET Framework

Microsoft .NET Framework 4.8 must be installed on the Application Server. Required files and installation information are available from the Microsoft Download Center: https://dotnet.microsoft.com/download/dotnet-framework/net48.

Microsoft .NET Framework 3.5 must be installed on the Application Server if using the **IMSVersion** report for Production Accounting or IMS Integration Hub. Installation of Microsoft .NET Framework 3.5 is done when you set up the Internet Information Services (IIS) below.

Internet Information Services (IIS)

Production Accounting is a web application and requires a web server configured on the Application Server.

To set up IIS:

1. Open the Windows **Server Manager** on the Application Server.
2. Select **Dashboard** in the left-hand panel.
3. Select **Add roles and features** in the right-hand panel.

   The **Add Roles and Features Wizard** screen displays.
4. On the **Installation Type** page, select **Role-based or feature-based installation**.
5. On the **Server Selection** page:
   a. Select **Select a server from the server pool**.
   b. Select the local machine name in the **Server Pool** list.
6. On the **Server Roles** page, select **Web Server (IIS)**.

   The **Add Roles and Features Wizard** dialog box displays a confirmation of the features to be added.
7. Select **Include management tools (if applicable)**.
8. Click **Add Features**.

   The **Add Roles and Features Wizard** dialog box closes and **Web Server Role (IIS)** is added to the left-hand pane of the **Add Roles and Features Wizard** screen.
9. On the **Features** page:
   a. Expand the **.NET Framework 3.5 Features** node.
   b. Select **NET Framework 3.5 (includes .NET 2.0 and 3.0)**.
   c. Expand the **.NET Framework 4.8 Features** node.
   d. Select **ASP.NET 4.8**.
   e. Expand the **WCF Services** node (under the **.NET Framework 4.8 Features** node).
   f. Select **HTTP Activation** and **TCP Port Sharing**.

      > **Note:** A dialog box may display prompts to add required features for HTTP Activation. If you follow the prompts, steps **9g**, **9h**,**10f** and **10g** below are not required.

   g. Expand the **Windows Process Activation Service** node.
   h. Select **Process Model** and **Configuration APIs**.

10. On the **Web Server (IIS) » Role Services** page:
    a. Select **Web Server**.
    b. Select **Common HTTP Features** and only the following role services (if required, de-select other role services):

       Default Document

       HTTP Errors

       Static Content

       HTTP Redirection
    c. Select **Health and Diagnostics** and the following role service:

       HTTP Logging
    d. Select **Performance** and the following role service:

       Static Content Compression
    e. Select **Security** and the following role services:

       Request Filtering

       Windows Authentication
    f. Expand **Application Development** and the following role services:

       .NET Extensibility 4.8

       ASP.NET 4.8

       ISAPI Extensions

       ISAPI Filters
    g. Select **Management Tools** and the following role service:

       IIS Management Console
11. View the **Confirmation Page**.
12. Click **Install**.

    The new features are installed.
13. Click **Close**.

Microsoft .NET Core

> **Note:** Production Accounting Version 1.13 introduces new functionality built on .NET Core.

The ASP.NET Core Module (ANCM) for IIS must be installed on the Application Server. The ASP.NET Core 8.0 Module (ANCM) is installed with .NET Core Runtime from the .ASP.NET Core 8.0 Runtime Windows Hosting Bundle. Required files and installation information are available from: https://learn.microsoft.com/en-us/aspnet/core/host-and-deploy/aspnet-core-module?view=aspnetcore-8.0.

Microsoft URL Rewrite

Production Accounting uses URL rewrite rules in the `Web.config` file. Install the Microsoft URL Rewrite on the Application Server. For downloads and information, see https://www.iis.net/downloads/microsoft/url-rewrite.

Microsoft Message Queuing (MSMQ)

Production Accounting uses MSMQ for sending and receiving messages. MSMQ must be enabled on the Application Server.

To enable MSMQ:

1. Open the Windows **Server Manager** on the Application Server.
2. Select **Dashboard** in the left-hand panel.
3. Select **Add roles and features** in the right-hand panel.

   The **Add Roles and Features Wizard** screen displays.
4. On the **Installation Type** page, select **Role-based or feature-based installation**.
5. On the **Server Selection** page:
   a. Select **Select a server from the server pool**.
   b. Select the local machine name in the **Server Pool** list.
6. On the **Features** page, select the following features under **Message Queuing » Message Queuing Services**:

   Message Queuing Server

   Directory Service Integration
7. View the **Confirmation Page**.
8. Click **Install**.

   A restart may be required.

Microsoft Distributed Transaction Coordinator (MSDTC)

MSDTC must be enabled on the Application Server and the Database Server to coordinate Production Accounting transactions between the two machines.

To enable MSDTC:

1. Open the Windows **Control Panel**.
2. Select **Administrative Tools**.
3. Double-click **Component Services**.
4. Expand the **Console Root » Component Services » Computers » My Computer » Distributed Transaction Coordinator** node.
5. Right-click **Local DTC** and select **Properties** from the menu.
6. Select the **Security** tab.
7. Select the following options:

   Network DTC Access

   Allow Remote Clients

   Allow Inbound

   Allow Outbound

   Mutual Authentication Required
8. Click **OK**.

   A message that the MSDTC Service must be stopped and restarted displays.
9. Click **Yes**.

   A message confirms that the MSDTC Service was restarted.
10. Click **OK**.
11. Close the **Component Services** screen.
12. In **Administrative Tools**, double-click **Windows Defender Firewall with Advanced Security**.
13. In the left panel, select **Inbound Rules**.
14. Right-click **Distributed Transaction Coordinator (RPC)** and select **Enable Rule** from the menu.
15. Right-click **Distributed Transaction Coordinator (RPC-EPMAP)** and select **Enable Rule** from the menu.
16. Right-click **Distributed Transaction Coordinator (TCP-In)** and select **Enable Rule** from the menu.
17. In the left panel, select **Outbound Rules**.

18. Right-click **Distributed Transaction Coordinator (TCP-Out)** and select **Enable Rule** from the menu.
19. Close the **Windows Defender Firewall with Advanced Security** screen.

Self-signed Certificate Creation

> **Note:** This activity is not required if a certificate is provided by a certificate authority, or if not using SSL. If this activity is required, complete this activity on both the Application Server and the Database Server.

Activity Steps

1. Open Windows **PowerShell** with administrator permissions.
2. Run the following command, substituting appropriate values for the:
   - Friendly name
   - Fully qualified host name
   - Host name
   - Number of months before expiry

   ```
   New-SelfSignedCertificate -FriendlyName "<friendly name>" -DnsName "<fully qualified host name>", "<hostname>"  -NotAfter (Get-Date).AddMonths(<Number of months before expiry>) -CertStoreLocation cert:\LocalMachine\My
   ```

   For example:

   ```
   New-SelfSignedCertificate -FriendlyName "DataminePASoftwareCert" -DnsName "myservername.domain.com", "myservername"  -NotAfter (Get-Date).AddMonths(36) -CertStoreLocation cert:\LocalMachine\My
   ```

3. Run the following command.

   ```
   mmc
   ```

   The **Microsoft Management Console** opens.
4. From the **File** menu, select **Add/Remove Snap-in**.

   The **Add or Remove Snap-ins** dialog box opens.
5. In the **Available snap-ins** list, select **Certificates**.
6. Click **Add**.
7. In the **Certificates snap-in** dialog box:
   a. Select **Computer account**.
   b. Click **Next**.

8. In the **Select Computer** dialog box:
    a. Select **Local computer**.
    b. Click **Finish**.
9. Click **OK**.

    The **Add or Remove Snap-ins** dialog box closes and the **Certificates** node displays under the **Console Root**.
10. Select the **Certificates » Personal » Certificates** node.
11. Right-click the certificate in the middle panel and select **All Tasks » Export** from the menu.

    The **Certificate Export Wizard** opens.
12. Click **Next**.
13. On the **Export Private Key** page:
    a. Select **Yes, export the private key**.
    b. Click **Next**.
14. On the **Export File Format** page:
    a. Keep the default settings.
    b. Click **Next**.
15. On the **Security** page:
    a. Select **Password**.
    b. Enter a password and confirm the password.
    c. Click **Next**.
16. On the **File to Export** page:
    a. Specify a file name and location.

        The file type is *Personal Information Exchange (*.pfx)*.
    b. Click **Next**.
17. Click **Finish**.

    A status message displays.
18. Click **OK**.

    The **Certificate Export Wizard** closes.
19. Right-click the certificate in the middle panel and select **Copy** from the menu.
20. Select the **Trusted Root Certification Authorities » Certificates** node.
21. Click the **Paste** button on the toolbar.

    The certificate displays in the middle panel.

22. Close the **Microsoft Management Console**.

> **Note:** If prompted to *Save console settings to Console1*, click **No**. This refers to saving the settings as a new console view, which is not required.

23. Close **Powershell**.

Microsoft SQL Server

Microsoft SQL Server must be installed on the Database Server. Installation information is available from the Microsoft Technet site:

- SQL Server 2014 and above: https://docs.microsoft.com/en-us/sql/database-engine/install-windows/installation-for-sql-server

The recommended installation of Microsoft SQL Server includes the following features:

- **Database Engine Services**
- **Reporting Services - Native**—**Note:** This is a separate installation from SQL Server 2019.

Datamine recommends using Secure Sockets Layer (SSL) with Production Accounting.

To force SSL encryption:

> **Note:** The SSL certificate (self-signed or from another certificate authority) must be installed in the **Trusted Root Certification Authorities** store of the Database Server. Certain permissions may need to be configured on the certificate's private key. The following activity includes the steps for configuring private key permissions, if required.

> **Note:** The following activity assumes the certificate has been added to the **Certificates » Personal » Certificates** node in the **Microsoft Management Console** on the Database Server. See "Self-signed Certificate Creation" on page 28 above, if required.

1. Open Windows **PowerShell** with administrator permissions.
2. Run the following command.

   ```
   mmc
   ```

   The **Microsoft Management Console** opens.
3. From the **File** menu, select **Add/Remove Snap-in**.

   The **Add or Remove Snap-ins** dialog box opens.
4. In the **Available snap-ins** list, select **Certificates**.
5. Click **Add**.

6. In the **Certificates snap-in** dialog box:
    a. Select **Computer account**.
    b. Click **Next**.
7. In the **Select Computer** dialog box:
    a. Select **Local computer**.
    b. Click **Finish**.
8. Click **OK**.

    The **Add or Remove Snap-ins** dialog box closes and the **Certificates** node displays under the **Console Root**.
9. Select the **Certificates » Personal » Certificates** node.
10. Right-click the required certificate (either self-signed or from another certificate authority) in the middle panel and select **All Tasks » Manage Private Keys** from the menu.

    The **Permissions for private keys** dialog box displays.

    > **Note:** The user account used to run the SQL Server Service needs **Read** permissions for the private key.

11. Perform the following steps to locate the details of the user account that runs the SQL Server Service.
    a. Open the Windows **Control Panel**.
    b. Select **Administrative Tools**.
    c. Double-click **Computer Management**.
    d. Expand the **Services and Applications** node and select **Services**.
    e. In the **Services** list, right-click **SQL Server (MSSQLSERVER)** and select **Properties** from the menu.

        The **SQL Server (MSSQLSERVER) Properties** screen displays.
    f. Select the **Log On** tab.
    g. Select and copy the user account name displayed in **This Account**.
    h. Close the **SQL Server (MSSQLSERVER) Properties** screen.
    i. Close **Computer Management**.
12. In the **Permissions for private keys** dialog box under **Group or user names**, click **Add**.

    The **Select Users or Groups** dialog box displays.
13. Click **Locations**.

    The **Locations** dialog box opens.

14. Select the location of the user account used to run the SQL Server Service; for example, local machine.
15. Click **OK**.

    The **Locations** dialog box closes.
16. Paste the user account name in the **Enter the object names to select** field.
17. Click **OK**.

> **Note:** If the **Multiple Names Found** dialog box displays, select the required user name from the list and click **OK**.

18. Select the **Read—Allow** permission. All other permissions should be cleared.
19. Click **OK**.

    The **Permissions for private keys** dialog box closes.
20. Close the **Microsoft Management Console**.

> **Note:** If prompted to *Save console settings to Console1*, click **No**. This refers to saving the settings as a new console view, which is not required.

21. Close **Powershell**.
22. Open the **SQL Server Configuration Manager**.
23. Expand the **SQL Server Network Configuration** node.
24. Right-click the **Protocols for MSSQLSERVER** node and select **Properties** from the menu.
25. Select the **Certificate** tab.
26. From the **Certificate** drop-down, select the required certificate.
27. Select the **Flags** tab.
28. Set **Force Encryption** to *Yes*.
29. Click **OK**.
30. Restart the SQL Server service as required.

> **Note:** Once the self-signed certificate or a certificate from another certificate authority has been configured on the Database Server, this certificate must be imported to the **Trusted Root Certification Authorities** store on the Application Server. See **Import and trust the certificate on the Application Server** below.

To set up SQL Server Reporting Services to use HTTPS:

1. Open the **Report Server Configuration Manager**.
2. Click **Web Service URL**.

3. Select the **HTTPS Certificate**.

> **Note:** Use a self-signed certificate or a certificate from another certificate authority as required. Ensure that the certificate is installed in the **Trusted Root Certification Authorities** store of the Database Server.

4. Click **Apply**.

To import and trust the certificate on the Application Server:

> **Note:** This activity assumes that the certificate (either self-signed or from another certificate authority) has been saved as a `.pfx` file in a file location on the Database Server. If a password was set for the certificate's private key, the password is required for this activity. See "Self-signed Certificate Creation" on page 28 above if required.

1. On the Database Server, perform the following steps:
   a. Open the file location where the certificate is saved as a `.pfx` file.
   b. Right-click the certificate and select **Copy** from the menu.
2. On the Application Server, select a file location in which to save the certificate.
3. Right-click and select **Paste** from the menu.
4. On the Application Server, open Windows **PowerShell** with administrator permissions.
5. Run the following command.

```
mmc
```

   The **Microsoft Management Console** opens.
6. From the **File** menu, select **Add/Remove Snap-in**.
   The **Add or Remove Snap-ins** dialog box opens.
7. In the **Available snap-ins** list, select **Certificates**.
8. Click **Add**.
9. In the **Certificates snap-in** dialog box:
   a. Select **Computer account**.
   b. Click **Next**.
10. In the **Select Computer** dialog box:
    a. Select **Local computer**.
    b. Click **Finish**.

11. Click **OK**.

    The **Add or Remove Snap-ins** dialog box closes and the **Certificates** node displays under the **Console Root**.
12. Select the **Certificates » Trusted Root Certification Authorities» Certificates** node.
13. From the **Action** menu, select **All Tasks » Import**.

    The **Certificate Import Wizard** opens.
14. Click **Next**.
15. On the **File to Import** page:
    a. Click **Browse**.

       The **Open** dialog box opens.
    b. Select the file location in which you saved the certificate.
    c. Select *Personal Information Exchange (*.pfx; *.p12)* as the file type.
    d. Select the certificate and click **Open**.

       The **Open** dialog box closes.
    e. Click **Next**.
16. On the **Private key protection** page (if displayed):
    a. Enter the password for the certificate's private key.
    b. Keep the default **Import Options** settings.
    c. Click **Next**.
17. On the **Certificate Store** page:
    a. Select *Place all certificates in the following store*.
    b. Click **Browse**.

       The **Select Certificate Store** dialog box opens.
    c. Select **Trusted Root Certification Authorities** and click **OK**.

       The **Select Certificate Store** dialog box closes.
    d. Click **Next**.
18. Click **Finish**.

    A status message displays.
19. Click **OK**.

    The **Certificate Import Wizard** closes. The certificate displays in the middle panel.

20. Close the **Microsoft Management Console**.

> **Note:** If prompted to *Save console settings to Console1*, click **No**. This refers to saving the settings as a new console view, which is not required.

21. Close **Powershell**.

Production Accounting Installation

Integration with other Intelligent Mining Solutions applications

If Production Accounting is to be used with IMS Integration Hub (version 2.5 or later), install IMS Integration Hub before installing Production Accounting.

For more information, see the separate IMS Integration Hub Installation Guide.

Production Accounting Installation on the Application Server

The installation of Production Accounting is a manual process of copying files from the Production Accounting file package to various folders on the Application Server.

Production Accounting Configuration on the Application Server

A web server (IIS) must be configured for Production Accounting.

Optionally, JKMetAccount can be installed and configured.

The `Web.config` and `Bootstrap.config` files should be edited as required.

The `app.config.json` and `appsettings.json` files for PA Core should be edited as required.

Message Queuing must be configured.

> **Note:** Most installations include the setup of various reports. These reports are customised, and the required files are not distributed with the standard Production Accounting file package. Contact your Datamine consultant for assistance with all customisations.

Production Accounting Databases

Multiple databases must be created for Production Accounting. Some are created via a batch file from the Application Server. Others are created directly on the Database Server.

Production Accounting Services

Production Accounting uses four Windows services, which should be installed in the following order:

1. Notification Service
2. Audit Service
3. Logging Service
4. Time Service

> **Note:** `C:\Datamine\PA\Logs` is the default location for service log files. If this default location is not used, it must be changed in service configuration files. Activating the log files is recommended during the testing phases of project setup, or to diagnose errors. However, after successful testing, comment out the log file settings again in order to avoid creating large log files.

Production Accounting File Structure

The following file structure is required on the Application Server.

> **Note:** Folders do not need to be created manually within **wwwroot** of the Internet Information Services (IIS).

Prepare the Production Accounting file package for use:

1. Unzip the Production Accounting file package.

Create the file structure for Production Accounting functionality:

1. Create the following folders on the Application Server:

   `C:\Datamine\PA`

   `C:\Datamine\PA\Archive`

   `C:\Datamine\PA\Config`

   `C:\Datamine\PA\Deploy`

   `C:\Datamine\PA\Logs`

   `C:\Program Files\Datamine\PA`

2. Copy the `Configuration`, `PA Core`, `Portal`, `Setup` and `Services` folders of the Production Accounting file package to the `C:\Program Files\Datamine\PA` folder.

   > **Note:** The files in the `Setup` folder are only required for installation. The `Setup` folder can be deleted after installation of Production Accounting is complete.

Give the domain account or NETWORK SERVICE account permission to create folders and modify files:

1. In Windows Explorer, right-click the `C:\Program Files\Datamine\PA` folder and select **Properties** from the menu.
2. Select the **Security** tab.
3. Select the domain account or **NETWORK SERVICE** account in the **Group or user names** list.

   > **Note:** For more information, see **Add Network Service to the Group or user names list** in "System Configuration before Installing Production Accounting" on page 12.

4. Select the following permission.
   Full Control: Allow
5. Click **OK**.

Default Port Numbers

Default port numbers are used in Production Accounting configuration files. If required (for example, because the default is used by another website or application), default port numbers can be replaced with unique port numbers.

> **Important:** If changing any port numbers ensure that port numbers that are used in multiple configuration files continue to match. For example, if changing port 443, it must be changed in all applicable configuration files.

PA Framework

- TCP port for SLL/HTTPS: **443**
- TCP port for HTTP: **80**

PA Core

- TCP port for SSL/HTTPS: **444**
- TCP port for HTTP: **81**

> **Note:** Production Accounting may use additional ports for other configuration settings. Those additional ports are not documented here and generally should not be changed.

Required IIS Configuration

The following configuration is required for the Production Accounting web server. Support for JavaScript Object Notation (JSON) files is required for the Production Accounting Online Help.

Access the Internet Information Services (IIS) Manager screen:

1. Open the Windows **Server Manager**.
2. Select **IIS** in the left-hand panel.
3. Right-click the IIS server in the **SERVERS** list and select **Internet Information Services (IIS) Manager** from the menu.

   The **Internet Information Services (IIS) Manager** screen displays.

Configure authentication:

1. Select the node for the IIS server in the **Connections** list.
2. Select the **Features View** in the middle panel of the **Internet Information Services (IIS) Manager** screen.
3. Double-click the **Feature Delegation** icon.

   The **Feature Delegation** settings display in the middle panel.
4. Update the **Status** for the following settings:

   Authentication - Anonymous = Read/Write

   Authentication - Windows = Read/Write

Import a certificate if Secure Sockets Layer (SSL) is required:

> **Note:** This activity is only required if using SSL. Import either the self-signed certificate or the certificate provided by a certificate authority.

1. Select the node for the IIS server in the **Connections** list.
2. Double-click the **Server Certificates** icon.

   The **Server Certificates** display in the middle panel.
3. Select **Import** in the **Actions** menu in the right-hand panel.
4. Locate and select the certificate.
5. Enter the certificate **Password**.
6. Set **Select Certificate Store** to *Web Hosting*.

7. Click **OK**.

> **Note:** The *Web Hosting* certificate must be installed in the `Trusted Root Certification Authorities` folder on the computers used to access the Production Accounting application web client. See **Export and Store the Certificate** in "Internet Browser Configuration" on page 101.

Configure the default application pool:

1. Expand the node for the IIS server in the **Connections** list.
2. Select the **Application Pools** node.
3. Right-click the **DefaultAppPool** in the **Application Pools** list and select **Advanced Settings** from the menu.

   The **Advanced Settings** dialog box opens.
4. Edit the following settings in the **General** group:

   .Net CLR Version = v4.0

   Start Mode = AlwaysRunning
5. Edit the following settings in the **Process Model** group:

   Identity = Network Service or domain account

   Idle Time-out (minutes) = 0
6. Edit the following settings in the **Recycling** group:

   Disable Overlapped Recycle = True

   Generate Recycle Event Log Entry = True for all sub-items

   Regular Time Interval (minutes) = 0
7. Click **OK**.

   The **Advanced Settings** dialog box closes.

Configure the default web site:

> **Note:** The default web site hosts the PA Framework functionality (built on .NET Framework).

1. Expand the **Sites** node in the **Connections** list.
2. Right-click the **Default Web Site** node and select **Add Application** from the menu.

   The **Add Application** dialog box opens.
3. Enter *PA* as the **Alias**.
4. Ensure the **Application pool** is set to *DefaultAppPool*.

5. Select the physical path:
    a. Click the ellipsis (**...**) button next to **Physical path**.

       The **Browse For Folder** dialog box opens.
    b. Browse for and select the `C:\Program Files\Datamine\PA\Portal` folder.
    c. Click **OK**.

       The **Browse For Folder** dialog box closes.
6. Click **OK**.

   The **Add Application** dialog box closes and the **PA** node is selected under **Sites » Default Web Site** in the **Connections** list.
7. Edit the binding if using SSL:
    a. Right-click the **Sites » Default Web Site** node in the **Connections** list and select **Edit Bindings**.

       The **Site Bindings** dialog box displays.
    b. Click **Add**.

       The **Add Site Binding** dialog box displays.
    c. Set **Type** to *https*.
    d. Next to the **SSL certificate** drop-down, click **Select**.

       The **Select Certificate** dialog box displays a table of available certificates.
    e. Select the required certificate and click **OK**.

       > **Note:** The certificate can be the self-signed certificate or a certificate provided by a certificate authority. If multiple self-signed certificates have the same **Friendly Name**, choose the certificate for which the **Certificate Store** is *WebHosting*.

       The **Select Certificate** dialog box closes.
    f. Click **OK**.

       The **Add Site Binding** dialog box closes.
    g. Click **Close**.

       The **Site Bindings** dialog box closes.
8. Enable HTTP Strict Transport Security (HSTS) if using SSL:
    a. Select the **Sites » Default Web Site** node in the **Connections** list.
    b. Select **HSTS** in the **Manage Website » Configure** menu in the right-hand panel.

The **Edit Website HSTS** dialog box displays.

c. Check **Enable**, **IncludeSubDomains**, **Preload** and **Redirect Http to Https**.

d. Set **Max-Age** to *31536000*.

e. Click **OK**.

The **Edit Website HSTS** dialog box closes.

9. Configure redirection:

a. Select the **Sites » Default Web Site** node in the **Connections** list.

b. Double-click the **HTTP Redirect** icon.

The **HTTP Redirect** settings display in the middle panel.

c. Check **Redirect requests to this destination**.

d. Enter the address of the Production Accounting webserver, with *https* if SSL is configured. Example: *https://<server-name>/PA*.

e. Check **Redirect all requests to exact destination (instead of relative destination)**.

f. Uncheck **Only redirect requests to content in this directory (not subdirectories)**.

g. Set **Status code** to *Permanent (301)*.

h. Select **Apply** in the **Actions** menu in the right-hand panel.

10. Confirm the default document:

a. Select the **Sites » Default Web Site » PA** node in the **Connections** list.

b. Double-click the **Default Document** icon.

The **Default Document** settings display in the middle panel.

c. Ensure that **default.aspx** is at the top of the documents list.

Configure the PA Core web site:

> **Note:** The PA Core web site hosts the additional functionality introduced in Production Accounting 1.13 (built on .NET Core). Some additional configuration is required for the PA Core web site, but the end user experience of the Production Accounting web client is unchanged. The functionality from both sites displays in the same web client.

1. Verify that the ASP.NET Core Module (ANCM) for IIS is installed:
   a. Select the node for the IIS server in the **Connections** list.
   b. Select the **Features View** in the middle panel of the **Internet Information Services (IIS) Manager** screen.
   c. Double-click the **Modules** icon.

      The **Modules** list displays in the middle panel.
   d. Make sure that the **AspNetCoreModuleV2** is in the list.

      > **Note:** If the required module is not in the list, download and install it before you continue. See **Microsoft .NET Core** in "System Configuration before Installing Production Accounting" on page 12.
2. Expand the node for the IIS server in the **Connections** list.
3. Right-click the **Sites** node and select **Add Website** from the menu.

   The **Add Website** dialog box displays.
4. Enter *PACore* as the **Site name**.

   > **Note:** The **Application pool** auto-populates with the **Site name**.
5. Select the physical path:
   a. Click the ellipsis (**...**) button next to **Physical path**.

      The **Browse For Folder** dialog box opens.
   b. Browse for and select the `C:\Program Files\Datamine\PA\PA Core` folder.
   c. Click **OK**.

      The **Browse For Folder** dialog box closes.
6. Configure the binding as required.
   a. If not using SSL:
      1. Set **Type** to *http*.

         > **Note:** The **Port** may auto-populate the PA default website port number (default: *80* or a unique value).
      2. Enter the PA Core default **Port** *81* or a unique port number if required. See "Default Port Numbers" on page 41.

b. If using SSL:

1. Set **Type** to *https*.

> **Note:** The **Port** may auto-populate the PA default website port number (default: *443* or a unique value).

2. Enter the PA Core default **Port** *444* or a unique port number if required. See "Default Port Numbers" on page 41.

7. Select a certificate if using SSL:

a. Next to the **SSL certificate** drop-down, click **Select**.

The **Select Certificate** dialog box displays a table of available certificates.

b. Select the required certificate and click **OK**.

> **Note:** Use the same certificate as for the default web site. If multiple self-signed certificates have the same **Friendly Name**, choose the certificate for which the **Certificate Store** is *WebHosting*.

The **Select Certificate** dialog box closes.

8. Click **OK**.

The **Add Website** dialog box closes and **PACore** displays under **Sites** in the **Connections** list.

9. Enable HTTP Strict Transport Security (HSTS) if using SSL:

a. Select the **Sites » PACore** node in the **Connections** list.

b. Select **HSTS** in the **Manage Website » Configure** menu in the right-hand panel.

The **Edit Website HSTS** dialog box displays.

c. Check **Enable**, **IncludeSubDomains**, **Preload** and **Redirect Http to Https**.

d. Set **Max-Age** to *31536000*.

e. Click **OK**.

The **Edit Website HSTS** dialog box closes.

Configure the PA Core application pool:

> **Note:** The same identity (either Network Service or domain account) must be set for the **DefaultApp Pool** and **PACore** application pools.

1. Expand the node for the IIS server in the **Connections** list.
2. Select the **Application Pools** node.

3. Right-click **PACore** in the **Application Pools** list and select **Advanced Settings** from the menu.

   The **Advanced Settings** dialog box opens.
4. Edit the following settings in the **General** group:

   .Net CLR Version = v4.0

   Start Mode = AlwaysRunning
5. Edit the following settings in the **Process Model** group:

   Identity = Network Service or domain account (must be the same identity as the DefaultAppPool)

   Idle Time-out (minutes) = 0
6. Edit the following settings in the **Recycling** group:

   Disable Overlapped Recycle = True

   Generate Recycle Event Log Entry = True for all sub-items

   Regular Time Interval (minutes) = 0
7. Click **OK**.

   The **Advanced Settings** dialog box closes.
8. Close the **Internet Information Services (IIS) Manager** screen.

Optional IIS Configuration for Non-Production Environments

The following configuration is required in development environments only if using a consulting tool to send Simple Object Access Protocol (SOAP) messages.

> **Important:** This configuration should not be done in production environments because it poses a security risk.

Access the Internet Information Services (IIS) Manager screen:

1. Open the Windows **Server Manager**.
2. Select **IIS** in the left-hand panel.
3. Right-click the IIS server in the **SERVERS** list and select **Internet Information Services (IIS) Manager** from the menu.

   The **Internet Information Services (IIS) Manager** screen displays.

Configure authentication for the LogSheetService:

1. Expand the node for the IIS server in the **Connections** list.
2. Expand the **Sites » Default Web Site** node.
3. Select the **PA** node.
4. Select the **Content View** in the middle panel of the **Internet Information Services (IIS) Manager** screen.
5. Select the `LogSheetService.asmx` file.
6. Select **Switch to Features View** in the **Actions** menu in the right-hand panel.
7. Double-click the **Authentication** icon.

   The **Authentication** settings display in the middle panel.
8. Update the **Status** for the following settings:

   Anonymous Authentication = Enabled

   ASP .NET Impersonation = Disabled

   Forms Authentication = Disabled

   Windows Authentication = Disabled
9. Close the **Internet Information Services (IIS) Manager** screen.

Database Creation

Production Accounting uses three databases. By default, these databases are called:

- **Datamine_PA_Data**
- **Datamine_PA_Portal**
- **Datamine_PA_Services**

The **Datamine_PA_Data** and **Datamine_PA_Portal** databases are created via a script run from the Application Server. This script also creates the required database tables.

The **Datamine_PA_Services** database must be created manually via SQL Server Management Studio. The required tables for the Datamine_PA_Services database are created with each of the Production Accounting services.

If using Production Accounting with JKMetAccount, an additional database is needed. By default, this database is called **Datamine_PA_JKMA**.

> **Notes:**
> Other names can be used for these databases; however, all activities in this Installation Guide refer to these databases by these names. If using different names, consider if additional syntax is needed when editing configuration files. For example, square brackets may be needed if the name includes non-alphanumeric characters: **catalog="[Datamine_PA_Services 1.9]"**.
> When specifying server details, you can enter the name of the SQL Server instance on the Database Server using either the hostname or IP address. Datamine recommends using the server's hostname because the IP address may change. However, if the IP address is static or there are issues using the server's hostname, then use the IP address.

Configure the setup for the Datamine_PA_Data and Datamine_PA_Portal databases:

1. On the Application Server, open Windows **Notepad** or an alternative text editor with administrator permissions.
2. Open the `C:\Program Files\Datamine\PA\Setup\globalConfig.xml` file.
3. Update the following values in the first **connection** section:

> **Note:** Update the values between the XML tags: <tag label=" ">**value**</tag>.
> In the example below, the default value **localhost** must be updated with the required value.

```
<host label="db.portal.host">localhost</host>
```

db.portal.host—Default: *localhost*. Update to the *Name of the SQL Server instance on the Database Server using either the hostname or IP address*

db.portal.catalogue—Default: *Datamine_PA_Portal*. Use the default value.

db.portal.login—Default: *dPipeWeb*. Update to the *Login name of the database user to be used in deploying Production Accounting configuration.* It is important that this value is changed from the default to enhance security.

db.portal.password—Default: blank. Update to the *Password of the database user above*.

4. Update the following values in the second **connection** section:

   db.data.host—Default: *localhost*. Update to the *Name of the SQL Server instance on the Database Server using either the hostname or IP address*.

   db.data.catalogue—Default: *Datamine_PA_Data*. Use the default value.

   db.data.login—Default: *dPipeWeb*. Update to the *Login name of the database user, as above*.

   db.data.password—Default: blank. Update to the *Password of the database user, as above*.

5. Save and close the `globalConfig.xml` file.

Create the Datamine_PA_Data and Datamine_PA_Portal databases:

1. On the Application Server, navigate to `C:\Program Files\Datamine\PA\Setup`.
2. Run the `setup.bat` file with administrator permissions.

   The batch file connects to the SQL Server and creates the Datamine_PA_Data and Datamine_PA_Portal databases with the current user's permissions and creates the required database tables and default data. This script also creates the **db.portal.login** database user.

Create the Datamine_PA_Services database:

1. On the Database Server, open **SQL Server Management Studio**.
2. Connect to the SQL Server.
3. Create a new database with the database name **Datamine_PA_Services**.

4. Run the following script against the Datamine_PA_Services database:

```
CREATE SCHEMA [abb] AUTHORIZATION [dbo]
```

The required database tables are created as a part of the installation process for each of the Production Accounting services.

> **Note:** For more information about creating databases, see https://docs.microsoft.com/en-us/sql/relational-databases/databases/create-a-database

Create the Datamine_PA_JKMA database if required:

1. On the Database Server, open **SQL Server Management Studio**.
2. Connect to the SQL Server.
3. Create a new database with the database name **Datamine_PA_JKMA**.
4. Create the tables for the Datamine_PA_JKMA database:
   a. Navigate to the `Setup\JKMA` folder of the Production Accounting file package.
   b. Run the `JKMA_DB_Install.sql` script against the Datamine_PA_JKMA database.
5. Add the initial user:
   a. Extract the `AddJKMAUser.zip` file.
   b. Open Windows **Command Prompt**.
   c. Run the following command to create the user. Update the connection string values as required for the Datamine_PA_JKMA database:

      Data Source—Default: *localhost*. Update to the *Name of the SQL Server instance on the Database Server using either the hostname or IP address*.

      Initial Catalog—Default: *Datamine_PA_JKMA*. Update to the *Database Name*.

      Integrated Security—Default: *True*. Replace with **User ID** and **Password** if using SQL authentication instead of Windows Integrated Security.

```
AddJKMAUser.exe "Data Source=localhost;Initial Catalog=Datamine_PA_JKMA;
Integrated Security=True; Connect Timeout=30; MultipleActiveResultSets=true;
TrustServerCertificate=True"
```

6. Create the required transfer tables in the Datamine_PA_Data database:
    a. Navigate to the `Setup` folder of the Production Accounting file package.
    b. Run the `JKMATransferTables.sql` script against the Datamine_PA_Data database.

    > **Important:** Do not run `JKMATransferTables.sql` against the Datamine_PA_JKMA database.

Assign the domain account or NETWORK SERVICE as a database owner:

1. On the Database Server, open **SQL Server Management Studio**.
2. Connect to the SQL Server.
3. Expand the **Security » Logins** node in the Object Explorer.
4. If the domain account or NT AUTHORITY\NETWORK SERVICE already exists as a login:
    a. Right-click the domain account or NT AUTHORITY\NETWORK SERVICE and select **Properties** from the menu.

    The **Login Properties** dialog box opens.
    b. Select the **User Mapping** page.
    c. Select the three Production Accounting databases and the JKMetAccount database.
    d. Select the **db_owner** database role.
    e. Click **OK**.

    The **Login Properties** dialog box closes.
5. If the domain account or NT AUTHORITY\NETWORK SERVICE does not already exist as a login:
    a. Right-click the **Logins** node and select **New Login** from the menu.

    The **Login - New** dialog box opens.
    b. On the **General** page, click **Search**.
    c. Search for and select domain account or NETWORK SERVICE on the local machine.
    d. Select **Windows authentication**.
    e. Select the **User Mapping** page.
    f. For each of the three Production Accounting databases and the JKMetAccount database:
        1. Select **Map** in the **Users mapped to this login** table.
        2. Select the **db_owner** database role membership.

g. Click **OK**.

The **Login - New** dialog box closes.

JKMetAccount Installation

JKMetAccount is a tool for balancing masses and organising metallurgical accounting data.

If using Production Accounting with JKMetAccount, complete the following activities on the Application Server.

If an installation of JKMetAccount exists, it can be upgraded. If upgrading JKMetAccount, the JKMetAccount Service is retained with its current properties. However, from Production Accounting 1.14.0 the JKMetAccount balance engine is now included in the core Production Accounting application and no longer runs as a separate service. The software installation steps below are required for configuration purposes but the existing JKMetAccount Service can be disabled or removed after upgrading (see "Upgrade Production Accounting" on page 114).

In a default installation, the JKMetAccount application is installed in the following folder: `C:\Program Files (x86)\Datamine\JKMetAccount\`

Upgrade JKMetAccount:

> **Note:** The InstallShield Wizard version number is 2.2.33. If executables for version 2.2.34 were installed during a previous upgrade (for example, to Production Accounting 1.13.2), you do not need to upgrade the JKMetAccount version.

1. Stop the JKMetAccount Service.
2. Back up the current registry settings. In Windows **Registry Editor**:
   a. Access the following location: **[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\JKTech\MetAccount]**.
   b. Export the **MetAccount** node.
3. Use Windows **Control Panel** to uninstall the previous version of JKMetAccount.
4. Install JKMetAccount 2.2.33. See steps below.
5. Run the backup registry file to restore settings.
6. Confirm the path to the JKP database:
   a. Open **JKProjectAdministrator** with administrator permissions.
   b. Ensure the path to the JKP database is correct (for example, `C:\Program Files (x86)\Datamine\JKMetAccount\Database\JKMetAccount-JkpDB.mdb`).

Install JKMetAccount 2.2.33:

1. Navigate to the `Setup\JKMA` folder of the Production Accounting file package.
2. Run the `JKMetAccount-Client-V2.2.33.exe` installation file with administrator permissions.

   The InstallShield Wizard to install JKMetAccount opens.
3. Click **Next**.
4. Enter the **User Name** and **Organization**.
5. Click **Next**.
6. To change the location of the installation folder:
   a. Click **Change**.
   b. Navigate to and select the installation folder.
   c. Click **OK**.
7. Click **Next**.
8. Select the **Stand Alone** setup type.
9. Click **Next**.

   JKMetAccount is installed with the selected options.
10. Click **Finish**.

    The InstallShield Wizard to install JKMetAccount closes.

Copy the updated executable files to the installation folder:

1. Navigate to the `Setup\JKMA` folder of the Production Accounting file package.
2. Extract the files from the `JKMA_EXES_2.2.34` folder.
3. Copy the extracted executable files into the installation folder to overwrite the existing executable files.

Administer the JKMetAccount project:

1. Navigate to `C:\Program Files (x86)\Datamine\JKMetAccount\`.
2. Run `JKProjectAdministrator.exe` with administrator permissions.
3. Enter a name for the **Project**.
4. Under the **Configuration Database** heading:
   a. Select **Microsoft SQL Server**.
   b. Click the ellipsis (**...**) next to the **Data Source** field.

      The **Data Link Properties** screen opens.
   c. On the **Provider** tab, select **Microsoft OLE DB Provider for SQL Server**.

d. Select the **Connection** tab.
e. Enter the name of the Database Server.
f. Select **Use Windows NT Integrated security**.
g. Select the Datamine_PA_JKMA database.
h. Click **OK**.

   The **Data Link Properties** screen closes.

5. Repeat Step 4 to select the Datamine_PA_JKMA database under the **Main Database** heading.
6. Repeat Step 4 to select the Datamine_PA_Data database under the **ODBC Import Database** heading.
7. Click **Check Connectivity**.

   A message displays the status of the connectivity.
8. Click **OK**.
9. Close the **JKProjectAdministrator** application.

Enable full access to the Log folder for the domain account or NETWORK SERVICE:

1. Navigate to `C:\Program Files (x86)\Datamine\JKMetAccount\`.
2. Right-click the `Log` folder and select **Properties** from the menu.

   The **Log Properties** screen displays.
3. Select the **Security** tab.
4. Click **Edit**.

   The **Permissions for Log** screen displays.
5. Add the user:
   a. Click **Add**.
   b. Search for and select the domain account or **NETWORK SERVICE**.
   c. Click **OK**.
6. Select **Allow Full Control** in the **Permissions** list.
7. Click **OK**.

   The **Permissions for Log** screen closes.
8. Click **OK**.

   The **Log Properties** screen closes.

Edit the Web.config File

After creating the required databases, the `Web.config` file in the `Portal` folder on the Application Server must be edited.

Activity Steps

1. Open Windows **Notepad** or an alternative text editor with administrator permissions.
2. Open the `C:\Program Files\Datamine\PA\Portal\Web.config` file.
3. In the **appSettings** section:
    a. If using Production Accounting Analytics, update values in the following keys **after installing Centric** (see "Production Accounting Analytics Installation" on page 93):
        - **CentricURL**—Change *localhost* to the Application Server name.
        - **CentricAPIToken**—Enter the token generated during Centric installation. See "Production Accounting Analytics Installation" on page 93.
        - **CentricETLDebounceSeconds**—Edit the interval in seconds at which Production Accounting calls Centric for analytics data updates if required. Default: *30*.

```
<add key ="CentricURL" value="https://localhost/PAAnalytics"/>
<add key ="CentricAPIToken" value= ""/>
<add key ="CentricETLDebounceSeconds" value= "30"/>
```

    b. Edit the **LogsheetServiceLogMaxDays** value if required to set the maximum number of days to retain rolling log files generated by the Logsheet Service. A new log file is created each day, and the oldest files are automatically deleted once the specified limit is reached. Default: *30*.

```
<add key="LogsheetServiceLogMaxDays" value="30" />
```

> **Note:** The Logsheet Service handles data uploads to Production Accounting via the IMS Integration Hub. This service has its own logging functionality, separate from the "Production Accounting Logging Service" on page 78.

    c. Edit the name of the SQL Server instance on the Database Server using either the hostname or IP address in the **Portal.ConnectionString** and **Config.ConnectionString** keys if required.

```
<add key="Portal.ConnectionString" value="server=localhost;database=Datamine_
PA_Portal;Integrated Security=true" />
<add key="Config.ConnectionString" value="server=localhost;database=Datamine_
PA_Data;Integrated Security=true" />
```

d. If using Production Accounting with JKMetAccount, update the name of the SQL Server instance on the Database Server using either the hostname or IP address in the **JKMA.ConnectionString** key:

```
<add key="JKMA.ConnectionString" value="server=localhost;database=Datamine_
PA_JKMA;Integrated Security=true" />
```

e. By default, Production Accounting connects to Active Directory within the current domain using the security context of the application pool identity under which it runs. If a custom Active Directory connection is required, enter the applicable values in the following keys:

- **adRoot**—Enter the Active Directory root path; for example, in the format *LDAP://DC=example,DC=com* or *LDAP://example.com* as required.
- **adUsername** and **adPassword**—Leave blank to use the application pool identity for the specified Active Directory root or enter a username and password.

```
<add key="adRoot" value="" />
<add key="adUsername" value="" />
<add key="adPassword" value="" />
```

f. Edit the **adAuthTypes** key value if required to specify the authentication type(s) to connect to Active Directory. Multiple types can be entered but must be separated by a semi-colon. Example combinations are:

- *Secure;Signing;Sealing* (Default)
- *Secure;SecureSocketsLayer*
- *Secure;Signing*"
- *Secure* (Minimum recommended)

For the full list of authentication types, see https://learn.microsoft.com/en-us/dotnet/api/system.directoryservices.authenticationtypes?view=windowsdesktop-9.0.

```
<add key="adAuthTypes" value="Secure;Signing;Sealing" />
```

> **Note:** *SecureSocketsLayer* is not compatible with *Signing* or *Sealing* because they use different port numbers.

g. Update the **PACoreBaseURL** key value. Change *localhost* to the Application Server name; and if required, change the default port number *444* to a unique port number (if configured for the PA Core web site). See "Default Port Numbers" on page 41.

```
<add key="PACoreBaseURL" value="https://localhost:444/" />
```

4. In the **system.webServer** section, change *localhost* to the Application Server name if required; and *https* to *http* if not using Secure Sockets Layer (SSL).

```
<httpRedirect
enabled="false" destination="https://localhost/PA" httpResponseStatus="Permanent"
/>
```

5. In the **system.webServer » httpProtocol » customHeaders** section:
   a. For the *https://localhost/* value, change *localhost* to the Reports Server (generally the Database Server) name if required.
   b. For the *https://localhost:444/* value, change *localhost* to the Application Server name; and if required, change the default port number *444* to a unique port number (if configured for the PA Core web site). See "Default Port Numbers" on page 41.

```
<add name="Content-Security-Policy" value="default-src 'self'
https://localhost/ https://localhost:444/;
        style-src 'self' 'unsafe-inline';
        script-src 'self' 'unsafe-eval' 'unsafe-inline';
        frame-ancestors 'self' "/>
```

6. In the **system.web** section, change **requireSSL** to *false* if not using SSL.

```
<httpCookies httpOnlyCookies="true" requireSSL="true" />
```

7. In the **system.transactions** section, edit the **timeout** value only if advised to do so by an Datamine representative.

```
<defaultSettings timeout="00:02:00"/>
```

8. In the **system.serviceModel** section for the CalcNet Recalculation Service, change **bindingConfiguration** to *SecureBasicHTTP* and **binding** to *basicHttpBinding* if not using SSL.

```
<service name="CalcNet Recalculation Service"
behaviorConfiguration="Heavily Throttled">
  <endpoint address="calcnet.recalc.svc"
  bindingConfiguration="RecalcBasicHTTPS"
  binding="basicHttpsBinding"
  contract="ABB.IMS.PA.CalcNet.Recalculator.IRecalcService"
  bindingNamespace="http://www.abb.com/ims/pa/calcnet/recalc"/>
</service>
```

9. If using the Network Service account instead of a domain account, in the **system.serviceModel » bindings » netMsmqBinding** section, uncomment the *None* security mode and comment out the *Transport* security mode for the **MSMQ**, **MSMQ_NMDataEvent** and **MSMQ_Log** bindings. However, Datamine recommends using a domain account.

```
<security mode="None"/>
<!--<security mode="Transport">
  <message algorithmSuite="TripleDesSha256Rsa15" />
  <transport msmqAuthenticationMode="WindowsDomain" msmqEncryptionAlgorithm="Aes"
msmqSecureHashAlgorithm="Sha512" msmqProtectionLevel="EncryptAndSign" />
</security>
-->
```

10. If using Production Accounting with IMS Integration Hub:
    a. Add the following service in the **services** section:

```
<service name="Mincom.IMS.DAL.TransactionService.TransactionMappingService"
behaviorConfiguration="Throttled">
  <endpoint
address="net.msmq://localhost/private/datamine.ims.transactionqueue"
  binding="netMsmqBinding"
  bindingConfiguration="msmqPoisonHandling"
  contract="IntegrationHub.WCF.Transactions.IMSDataProductionService" />
</service>
```

    b. Add the **PersistentSubscriptionManager** endpoint in the **client** section:

```
<endpoint address="net.msmq://localhost/private/datamine.ims.ihub_
registersubscribers"
behaviorConfiguration="LargeDataTransferBehavior"
binding="netMsmqBinding"
bindingConfiguration="SecuredMSMQ"
contract="IntegrationHub.WCF.Transactions.IMSTransactionRegistrationService"
name="PersistentSubscriptionManager" />
```

    c. Add the **IMSTransactionService** endpoint in the **client** section:

```
<endpoint address="net.msmq://localhost/private/datamine.ims.ihub"
binding="netMsmqBinding"
bindingConfiguration="SecuredMSMQ"
contract="IntegrationHub.WCF.Transactions.IMSDataProductionService"
name="IMSTransactionService" />
```

    d. Add the following endpoint in the **client** section:

```
<endpoint address="net.pipe://localhost/Retriever/"
behaviorConfiguration="LargeDataTransferBehavior"
binding="netNamedPipeBinding"
bindingConfiguration="pipe"
contract="Karjeni.DAL.Web.TransactionImporter.TransactionRetriever" />
```

    e. Add the following binding in the **netMsmqBinding** section:

```
<binding name="msmqPoisonHandling"
durable="true"
exactlyOnce="true"
receiveErrorHandling="Move"
maxReceivedMessageSize="8388608"
maxRetryCycles="6"
```

```
retryCycleDelay="00:05:00"
receiveRetryCount="2">
  <readerQuotas maxStringContentLength="8388608" />
  <security mode="Transport">
  <message algorithmSuite="TripleDesSha256Rsa15" />
  <transport msmqAuthenticationMode="WindowsDomain"
  msmqEncryptionAlgorithm="Aes"
  msmqSecureHashAlgorithm="Sha512"
  msmqProtectionLevel="EncryptAndSign" />
</security></binding>
```

Note: In this binding:

- receiveErrorHandling="Move" - Use the move-to-poison-subqueue mechanism for handling poison messages.
- maxRetryCycles="6" - The number of retry batches after initial delivery batch failure. The total number of delivery batches is (1 + maxRetryCycles).
- retryCycleDelay="00:05:00" - The time between retry batches.
- receiveRetryCount="2" - The number of redelivery attempts in a batch after the initial delivery attempt. The total number of delivery attempts is (1 + receiveRetryCount).
- The total delay to move a message from the head of the queue to the poison subqueue is guaranteed to be at least maxRetryCycles * retryCycleDelay.

f. Add the following binding in the **netNamedPipeBinding** section:

```
<binding name="pipe"
transactionFlow="true"
maxReceivedMessageSize="1147483647"
closeTimeout="00:05:00"
openTimeout="00:05:00"
receiveTimeout="00:05:00"
sendTimeout="00:05:00" />
```

g. Add the following endpointBehavior in the **behaviors** section:

```
<endpointBehaviors>
  <behavior name="LargeDataTransferBehavior">
    <dataContractSerializer maxItemsInObjectGraph="8388608" />
  </behavior>
</endpointBehaviors>
```

h. Add the following behavior in the **serviceBehaviors** section:

```
<behavior name="Throttled">
  <serviceThrottling
maxConcurrentCalls="1" maxConcurrentSessions="2" maxConcurrentInstances="1"/>
</behavior>
```

11. To disable web service (SOAP) logging, comment out the following code (so that it can be restored for troubleshooting if required):

```
<webServices>
  <soapExtensionTypes>
    <add
type
="Karjeni.DAL.WebService.TraceExtension,DataAbstractionLayer.WebService.Factory" />
  </soapExtensionTypes>
</webServices>
```

12. Save and close the `Web.config` file.

Edit the Bootstrap.config File

The `Bootstrap.config` file in the `Portal` folder on the Application Server may need to be edited.

Activity Steps

1. Open Windows **Notepad** or an alternative text editor with administrator permissions.
2. Open the `C:\Program Files\Datamine\PA\Portal\Bootstrap.config` file.
3. Cascade Manager runs by default with a single thread. Edit the **Thread Pool Size** argument in the Cascade Manager **Application** section if required:

```
<Application
ManagerType="Karjeni.CalcNet.CalculationEngine.DataManagement.CascadeManager,
Karjeni.CalcNet" Description="Cascade Manager" AutoStart="True">
  <StartupMethod name="initialise">
    <arg>Karjeni.CalcNet.DB.QueuePersistence4,
Karjeni.CalcNet.SQLServerAdapter</arg>
    <arg>%Config.ConnectionString%</arg>
    <!--Command Timeout for adding/removing items off the calc queue-->
    <arg>00:00:20</arg>
    <!--Thread Pool Size-->
    <arg>1</arg>
    <!--Thread Priority-->
    <arg>BelowNormal</arg>
    <!--Retries before cascade tasks are suspended-->
    <arg>6</arg>
    <!--Suspensions before cascade tasks are moved to poison-->
    <arg>6</arg>
    <!--Back off time before cascade retry, format 00:00:00-->
    <arg></arg>
    <!--True/False to allow or disallow task merging-->
    <arg>False</arg>
  </StartupMethod>
  <TearDownMethod name="blat" />
</Application>
```

Important: The Cascade Manager is a calculation engine manager, which coordinates the execution order of the calculations in Production Accounting. The **Thread Pool Size** argument is the maximum number of threads. Multiple threads can be used for high calculation load situations. However, too many threads will degrade performance as they can block each other. Performance testing is recommended on the intended configuration before this number is increased.

4. If logsheets will be recalculated on a schedule, change the **AutoStart** value to *True* in the Logsheet Recalculator Scheduler **Application** section:

```
<Application ManagerType="ABB.IMS.PA.CalcNet.Recalculator.Recalculator,
CalcNet.Recalculator" Description="Logsheet Recalculator
Scheduler" AutoStart="True">
```

5. To override the default retry count for Batch Tracking timeouts in CalcNet, change the **Timeout retry count** argument in the Commodity Flow System **Application** section:

```
<Application ManagerType="Karjeni.MaterialFlow.FlowResourceManager,
MaterialFlow" Description="Commodity Flow System" AutoStart="True">
  <StartupMethod name="initialise">
    <arg>Karjeni.MaterialFlow.Persistence.Abstraction.AbstractionAdapter,
MaterialFlow</arg>
    <!--Timeout retry count-->
    <arg>6</arg>
  </StartupMethod>
  <TearDownMethod name="tearDown" />
</Application
```

6. If using Production Accounting with IMS Integration Hub, uncomment the following application:

```
<Application
ManagerType="Mincom.IMS.DAL.TransactionService.TransactionMappingService,
TransactionService" Description="TransactionService" AutoStart="True">
  <StartupMethod name="initialise">
    <arg>Mincom.IMS.DAL.TransactionService.Persistence.Linq.SQLServerAdapter,
TransactionService</arg>
    <arg>%Config.ConnectionString%</arg>
  </StartupMethod>
  <TearDownMethod name="dispose" />
</Application>
```

7. If using Production Accounting with JKMetAccount, uncomment the following application:

```
<Application ManagerType="Karjeni.JKMALoader.JKMAManager,
Karjeni.JKMALoader" Description="JKMA Data Transfer Manager" AutoStart="True">
    <StartupMethod name="getInstance" >
        <arg>Karjeni.JKMALoader.DB.JKMASQLAdapter, Karjeni.JKMALoader</arg>
        <arg>%Config.ConnectionString%</arg>
        <arg>%JKMA.ConnectionString%</arg>
        <!--True/False to activate built-in Balance Engine-->
        <arg>True</arg>
```

```
    </StartupMethod>
    <TearDownMethod name="tearDown" />
</Application>
```

Important: Because XML does not support nested comments, the `Bootstrap.config` file has a workaround of additional spaces between the hyphens in the line *<!- -True/False to activate built-in Balance Engine- ->*. Delete these spaces.

8. If using Production Accounting Analytics, configure the Extract, Transform, Load (ETL) process settings for Centric integration in the Analytics Adaptor **Application** section:
    a. Set the **Run ETL extraction on PA startup** argument as required to control whether Production Accounting automatically runs the ETL extracts at startup. Default: *True*.
    b. Set the **Max ETLs to process in parallel** argument to the maximum number of ETL updates that may run at the same time. Any additional ETLs will be queued until a thread is available. Value must be between *1* and *100*. Default value: *5*.
    c. Update the **LogTime dimension ETL name; Extraction time** only if your LogTime dimension has a different name or should run at a different time. The format is the *LogTime dimension ETL name* followed by a semicolon and the time in 24-hour format.

    Note: If **Run ETL extraction on PA startup** is set to *True*, then the LogTime ETL runs at start up.

```
<Application
ManagerType="Centric.CentricAnalyticsAdaptor.CentricAnalyticsManager,
Centric.CentricAnalyticsAdaptor" Description="Analytics
Adaptor" AutoStart="True">
    <StartupMethod name="initialise">
        <!-- Run ETL extraction on PA startup -->
        <arg>True</arg>
        <!-- Max ETLs to process in parallel -->
        <arg>6</arg>
        <!-- LogTime dimension ETL name; Extraction time -->
        <arg>D_PA_LogTime;00:00</arg>
    </StartupMethod>
    <TearDownMethod name="tearDown" />
</Application>
```

9. Save and close the `Bootstrap.config` file.

Edit the PA Core App.config.json and Appsettings.json Files

Some settings in the app.config.json and appsettings.json files for PA Core must be edited.

Edit the app.config.json:

1. Open Windows **Notepad** or an alternative text editor with administrator permissions.
2. Open the `C:\Program Files\Datamine\PA\PA Core\wwwroot\app.config.json` file.
3. In the **Settings** section, edit the **baseServerUrl** and **appBaseUrl**:
   a. Change *https* to *http* if not using SSL.
   b. Change *localhost* to the Application Server name if required.
   c. Change the port number to the default port number *444* or the unique port number if configured for the PA Core web site. See "Default Port Numbers" on page 41.

```
{
   "baseServerUrl": "https://hostname:portnumber/",
   "appBaseUrl": "https://hostname:portnumber/",
```

4. Save and close the `app.config.json` file.

Edit the appsettings.json file:

1. Open Windows **Notepad** or an alternative text editor with administrator permissions.
2. Open the `C:\Program Files\Datamine\PA\PA Core\appsettings.json` file.
3. In the **Settings** section, edit the following:
   a. **PACoreFrontEndBaseUrl**
      1. Change *https* to *http* if not using SSL.
      2. Change *localhost* to the Application Server name if required.
      3. If required, change the default port number *444* to the unique port number if configured for the PA Core web site. See "Default Port Numbers" on page 41.

```
"PACoreFrontEndBaseUrl": "https://localhost:444",
```

b. **PAFrameworkBaseURL**:

1. Change *https* to *http* if not using SSL.
2. Change *localhost* to the Application Server name if required.

```
"PAFrameworkBaseURL": "https://localhost:443/PA/",
```

4. Save and close the `appsettings.json` file.

Production Accounting Notification Service

The Notification Service is a publish-subscribe messaging service, with the definition of the subscribers defined by database.

Edit the imsnotificationsvc.exe.config file:

1. On the Application Server, open Windows **Notepad** or an alternative text editor with administrator permissions.
2. Open the `C:\Program Files\Datamine\PA\Services\Notification Service\imsnotificationsvc.exe.config` file.
3. In the **components** section, update the following parts of the connection string if required:
   - Name of the SQL Server instance on the Database Server using either the hostname or IP address
   - Database name
   - Integrated Security

```
<parameter name="connectionString" value="server=localhost;database=Datamine_PA_
Services;Integrated Security=SSPI" />
```

4. If using the Network Service account instead of a domain account, in the **system.serviceModel » bindings » netMsmqBinding** section, uncomment the *None* security mode and comment out the *Transport* security mode for the **MSMQ_DataEvent** and **MSMQ_Log** bindings. However, Datamine recommends using a domain account.

```
<security mode="None"/>
<!--<security mode="Transport">
  <message algorithmSuite="TripleDesSha256Rsa15" />
  <transport msmqAuthenticationMode="WindowsDomain" msmqEncryptionAlgorithm="Aes"
msmqSecureHashAlgorithm="Sha512" msmqProtectionLevel="EncryptAndSign" />
</security>
-->
```

5. In the **system.diagnostics** section, uncomment the following code if required:

```
<source name="System.ServiceModel"
switchValue="Warning,Error,Critical"
propagateActivity="true">
  <listeners>
```

```
    <add name="traceListener"
    type="System.Diagnostics.XmlWriterTraceListener"
    initializeData= "C:\Datamine\PA\Logs\datamine.ims.notification.service.svclog"
/>
  </listeners>
</source>
```

Note: The `datamine.ims.notification.service.svclog` file is created automatically when it is first needed.

6. Save and close the `imsnotificationsvc.exe.config` file.

Create the database tables and register the Notification Service:

Note: If using a domain account instead of the Network Service account, replace **NT Authority\Network Service** with the domain account in the commands in this activity. Datamine recommends using a domain account.

1. On the Application Server, open Windows **Command Prompt** with administrator permissions.
2. Run the following command to navigate to the Notification Service folder:

```
cd C:\Program Files\Datamine\PA\Services\Notification Service
```

3. Run the following command to create the database tables for the Notification Service:

```
imsnotificationsvc.exe -install_db
```

4. Run one of the following commands as required to register the Notification Service with:
   a. The Network Service account and add a dependency on the Message Queuing service.

```
imsnotificationsvc.exe -install --user="NT Authority\Network Service" --
depends="MSMQ"
```

   b. The domain account and add a dependency on the Message Queuing service.

```
imsnotificationsvc.exe -install --user="domain\username" --
password="password" --depends="MSMQ"
```

5. Run the following command to delay the start of the Notification Service:

```
sc config "Datamine IMS Notification Service" start= delayed-auto
```

6. Run the following command to add a description to the Notification Service:

```
sc description "Datamine IMS Notification Service" "Production Accounting
Notification Service"
```

7. Run the following command to reserve the specified URL for the domain account or Network Service account.

```
netsh http add urlacl url=http://+:15200/Notification/SubscriptionService/ user="NT
Authority\Network Service"
```

8. Run the following command to reserve the specified URL for the domain account or Network Service account.

```
netsh http add urlacl url=http://+:15100/Notification/NotificationListenerService/
user="NT Authority\Network Service"
```

9. Run the following command to register the Notification Service with the Application log in Windows Event Viewer for logging messages:

```
imsnotificationsvc.exe -e
```

10. Press **Ctrl + C** to stop the Notification Service.
11. Open the Windows **Services** application.
12. Verify that the Datamine IMS Notification Service has been installed with:
    - A startup type of automatic (delayed start)
    - The domain account or Network Service as the logon user

Production Accounting Audit Service

The Audit Service provides persistence to the database of data audit messages from a subscription to the Notification Service. The Audit Service is self-subscribed to the Notification Service.

Edit the imsauditsvc.exe.config file:

1. Open Windows **Notepad** or an alternative text editor with administrator permissions.
2. Open the `C:\Program Files\Datamine\PA\Services\Audit Service\imsauditsvc.exe.config` file.

   > **Note:** Steps 3–4 below configure the Audit Service to purge old or unnecessary audit records for business process restarts and perform database maintenance. This process is resource-intensive. Do **not** run it at the same time as the Logging Service log clean up. Coordinate with local IT support to determine a suitable low-usage window.

3. In the **processRestartCleanup** section, update the following values to configure when the Audit Service cleans up its records:
   - **initialStartDayOfWeek**—Day of week used as the schedule's starting day (where *1 = Sunday*; *7 = Saturday*). Default: *2*.
   - **daysBetweenRuns**—Number of days between each clean-up run. Set to *0* to disable scheduled runs (a start-up run is unaffected). Default: *7*.
   - **timeOfDay**—Time of day the process runs, in 24-hour format *hh:mm*. Default: *03:00*.
   - **runOnStart**—Whether to run a clean-up at service start-up before reverting to the configured schedule. If a start-up run clashes with the scheduled run, only one occurs; the other is blocked. Default: *false*.
   - **maxDurationPerRunMinutes**—Maximum number of minutes spent deleting records per run (does not include index maintenance or database shrinking). Each delete batch can take several minutes; the run duration is checked between batches. Default: *Not specified (example: 30)*.
   - **deleteOlderThan**—Time span indicating how far back from the current date to delete records. Format: *[days].[hours]:[minutes]:[seconds]*. Default: *180.00:00:00*.

```
<processRestartCleanup
    initialStartDayOfWeek="2"
    daysBetweenRuns="7"
    timeOfDay="03:00"
    runOnStart="false"
    badKeyHashToPurge ="71695070"
    maxDurationPerRunMinutes="30"
    deleteOlderThan="180.00:00:00">
```

4. In the **processRestartCleanup » execution** section, update the following values to control how each clean-up run executes:
    - **batchSize**—Number of records deleted per batch. Deletion proceeds in batches of this size while records remain and until the maximum run time is reached. Recommended: Use a large value to minimise the number of calls, because each batch can take several minutes to complete. Default: *100000*.
    - **commandTimeoutSeconds**—Maximum time (in seconds) allowed for each delete batch to complete. Recommended: At least *1200* (20 minutes). Default: *1200*.
    - **schemaName**—Schema name of the **LogEntries** table in the Services database. Default: *abb*. Update to *datamine* if required.
    - **windowDays**—Number of days processed per window. Should be less than *25* days. Default: *21*.
    - **shrinkAfterRun**—If *true*, performs a database shrink (after any re-indexing) if rows were deleted. Default: *false*.
    - **shrinkCommandTimeoutSeconds**—Maximum time (in seconds) allowed for the shrink operation. Default: *3600* (1 hour).
    - **updateStatisticsAfterRun**—If *true*, updates table statistics if rows were deleted to assist future queries. Default: *true*.
    - **updateStatisticsCommandTimeoutSeconds**—Maximum time (in seconds) allowed for the statistics update. Default: *3600* (1 hour).

```
<execution
    batchSize="100000"
    commandTimeoutSeconds="1200"
    schemaName="abb"
    windowDays="21"
    shrinkAfterRun="false"
    shrinkCommandTimeoutSeconds="3600"
    updateStatisticsAfterRun="true"
    updateStatisticsCommandTimeoutSeconds="3600" />
```

5. In the **hibernate-configuration** section, update the following parts of the connection string if required:
   - Name of the SQL Server instance on the Database Server using either the hostname or IP address
   - Database name
   - Integrated Security

```
<property name="connection.connection_string">Server=localhost;initial
catalog=Datamine_PA_Services;Integrated Security=true</property>
```

6. In the **hibernate-mapping** section, edit the catalog name twice:

```
<class name="EventDetailEntity" table="EventDetail" schema="abb" catalog="Datamine_
PA_Services">
<class name="EventEntity" table="EventLog" schema="abb" catalog="Datamine_PA_
Services">
```

7. If using the Network Service account instead of a domain account, in the **system.serviceModel » bindings » netMsmqBinding** section, uncomment the *None* security mode and comment out the *Transport* security mode for the **MSMQ_NMDataEvent**, **MSMQ_PortalDataEvent**, **MSMQ_AuditDataEvent**, **MSMQ_Log**, **MSMQ_Recovery_DL** and **MSMQ_Recovery** bindings. However, Datamine recommends using a domain account.

```
<security mode="None"/>
<!--<security mode="Transport">
  <message algorithmSuite="TripleDesSha256Rsa15" />
  <transport msmqAuthenticationMode="WindowsDomain" msmqEncryptionAlgorithm="Aes"
msmqSecureHashAlgorithm="Sha512" msmqProtectionLevel="EncryptAndSign" />
</security>
-->
```

8. In the **system.diagnostics** section, uncomment the following code if required:

```
<source name="System.ServiceModel"
switchValue="Warning,Error,Critical"
propagateActivity="true">
  <listeners>
    <add name="traceListener"
    type="System.Diagnostics.XmlWriterTraceListener"
    initializeData= "C:\Datamine\PA\Logs\datamine.ims.audit.service.svclog" />
  </listeners>
</source>
```

> **Note:** The `datamine.ims.audit.service.svclog` file is created automatically when it is first needed.

9. Save and close the `imsauditsvc.exe.config` file.

Create the database tables and register the Audit Service:

> **Note:** If using a domain account instead of the Network Service account, replace **NT Authority\Network Service** with the domain account in the commands in this activity. Datamine recommends using a domain account.

1. Open Windows **Command Prompt** with administrator permissions.
2. Run the following command to navigate to the Audit Service folder:

```
cd C:\Program Files\Datamine\PA\Services\Audit Service
```

3. Run the following command to create the database tables for the Audit Service:

```
imsauditsvc.exe -install_db
```

4. Run one of the following commands as required to register the Audit Service with:
   a. The Network Service account and add a dependency on the Notification Service.

```
imsauditsvc.exe -install --user="NT Authority\Network Service" --
depends="Datamine IMS Notification Service"
```

   b. The domain account and add a dependency on the Notification Service.

```
imsauditsvc.exe -install --user="domain\username" --password="password" --
depends="Datamine IMS Notification Service"
```

5. Run the following command to delay the start of the Audit Service:

```
sc config "Datamine IMS Audit Service" start= delayed-auto
```

6. Run the following command to add a description to the Audit Service:

```
sc description "Datamine IMS Audit Service" "Production Accounting Audit Service"
```

7. Run the following command to register the Audit Service with the Application log in Windows Event Viewer for logging messages:

```
imsauditsvc.exe -e
```

8. Press **Ctrl + C** to stop the Audit Service.
9. Open the Windows **Services** application.
10. Verify that the Datamine IMS Audit Service has been installed with:
    - A startup type of automatic (delayed start)
    - The domain account or Network Service as the logon user
    - Datamine IMS Notification Service as a dependency

Production Accounting Logging Service

The Logging Service provides configurable persistence of messages to a database, file or the Windows Event Log.

Edit the imslogsvc.exe.config file:

1. Open Windows **Notepad** or an alternative text editor with administrator permissions.
2. Open the `C:\Program Files\Datamine\PA\Services\Logging Service\imslogsvc.exe.config` file.

   > **Note:** Steps 3–4 below configure the Logging Service to purge old logs and perform database maintenance. This process is resource-intensive. Do **not** run it at the same time as the Audit Service log clean up. Coordinate with local IT support to determine a suitable low-usage window.

3. In the **logCleanup** section, update the following values to configure when the Logging Service cleans up its logs:
   - **initialStartDayOfWeek**—Day of week used as the schedule's starting day (where *1 = Sunday*; *7 = Saturday*). Default: *1*.
   - **daysBetweenRuns**—Number of days between each clean-up run. Set to *0* to disable scheduled runs (a start-up run is unaffected). Default: *7*.
   - **timeOfDay**—Time of day the process runs, in 24-hour format *hh:mm*. Default: *02:00*.
   - **runOnStart**—Whether to run a clean-up at service start-up before reverting to the configured schedule. If a start-up run clashes with the scheduled run, only one occurs; the other is blocked. Default: *false*.
   - **maxDurationPerRunMinutes**—Maximum number of minutes spent deleting records per run (does not include re-indexing or database shrinking). Default: 20.

   ```
   <logCleanup
           initialStartDayOfWeek="1"
           daysBetweenRuns="7"
           timeOfDay="02:00"
           runOnStart="false"
           maxDurationPerRunMinutes="20">
   ```

4. In the **logCleanup » execution** section, update the following values to control how each clean-up run executes:

- **batchSize**—Number of records deleted per batch. Deletion proceeds in batches of this size while there are records to remove and the maximum run time has not been reached. Default: *5000*.
- **commandTimeoutSeconds**—Maximum time (in seconds) allowed for each delete batch to run. Default: *120*.
- **schemaName**—Schema name of the **LogEntries** table in the Services database. Default: *abb*. Update to *datamine* if required.
- **shrinkAfterRun**—If *true*, performs a database shrink (after any re-indexing) if rows were deleted. Default: *false*.
- **shrinkCommandTimeoutSeconds**—Maximum time (in seconds) allowed for the shrink operation. Default: *3600* (1 hour).
- **reindexAfterRun**—If *true*, re-indexes the table if rows were deleted. Default: *false*.
- **reindexCommandTimeoutSeconds**—Maximum time (in seconds) allowed for the re-indexing operation. Default: *3600* (1 hour).

```
<execution
batchSize="5000" commandTimeoutSeconds="120" schemaName="abb" shrinkAfterRun
="false" shrinkCommandTimeoutSeconds="3600" reindexAfterRun="true"
reindexCommandTimeoutSeconds="3600"/>
```

5. In the **hibernate-configuration** section, update the following parts of the connection string if required:
   - Name of the SQL Server instance on the Database Server using either the hostname or IP address
   - Database name
   - Integrated Security

```
<property name="connection.connection_string">Server=localhost;initial
catalog=Datamine_PA_Services;Integrated Security=SSPI</property>
```

6. In the **hibernate-mapping** section, edit the **catalog** name:

```
<class name="LogItemEntity" table="LogEntries" schema="abb" catalog="Datamine_PA_
Services">
```

7. If using the Network Service account instead of a domain account, in the **system.serviceModel » bindings » netMsmqBinding** section, uncomment the *None* security mode and comment out the *Transport* security mode for the **MSMQ_Log** binding. However, Datamine recommends using a domain account.

```
<security mode="None"/>
<!--<security mode="Transport">
  <message algorithmSuite="TripleDesSha256Rsa15" />
  <transport msmqAuthenticationMode="WindowsDomain" msmqEncryptionAlgorithm="Aes"
msmqSecureHashAlgorithm="Sha512" msmqProtectionLevel="EncryptAndSign" />
</security>
-->
```

8. In the **system.diagnostics** section, uncomment the following code if required:

```
<source name="System.ServiceModel"
switchValue="Warning,Error,Critical"
propagateActivity="true">
  <listeners>
    <add name="traceListener"
    type="System.Diagnostics.XmlWriterTraceListener"
    initializeData= "C:\Datamine\PA\Logs\datamine.ims.logging.service.svclog" />
  </listeners>
</source>
```

> **Note:** The `datamine.ims.logging.service.svclog` file is created automatically when it is first needed.

9. Save and close the `imslogsvc.exe.config` file.

Create the database tables and register the Logging Service:

> **Note:** If using a domain account instead of the Network Service account, replace **NT Authority\Network Service** with the domain account in the commands in this activity. Datamine recommends using a domain account.

1. Open Windows **Command Prompt** with administrator permissions.
2. Run the following command to navigate to the Logging Service folder:

```
cd C:\Program Files\Datamine\PA\Services\Logging Service
```

3. Run the following command to create the database tables for the Logging Service:

```
imslogsvc.exe -install_db
```

4. Run one of the following commands as required to register the Logging Service with:

a. The Network Service account and add a dependency on the Message Queuing service.

```
imslogsvc.exe -install --user="NT Authority\Network Service" --depends="MSMQ"
```

b. The domain account and add a dependency on the Message Queuing service.

```
imslogsvc.exe -install --user="domain\username" --password="password" --
depends="MSMQ"
```

5. Run the following command to delay the start of the service:

```
sc config "Datamine IMS Logging Service" start= delayed-auto
```

6. Run the following command to add a description to the service:

```
sc description "Datamine IMS Logging Service" "Production Accounting Logging
Service"
```

7. Run the following command to enable the Production Accounting Portal to write messages to the Application log in Windows Event Viewer:

```
imslogsvc.exe -spaev
```

8. Run the following command to register the Logging Service with the Application log in Windows Event Viewer for logging messages:

```
imslogsvc.exe -e
```

9. Press **Ctrl + C** to stop the Logging Service.
10. Open the Windows **Services** application.
11. Verify that the Datamine IMS Logging Service has been installed with:
    - A startup type of delayed automatic (delayed start)
    - The domain account or Network Service as the logon user
    - The Message Queuing service as a dependency

Production Accounting Time Service

The Time Service contains a configurable set of time period definitions for the Portal, which may be retrieved via a Windows Communication Foundation (WCF) request. Time period details include name, type, start, end and time zone.

Edit the imstimesvc.exe.config file:

1. Open Windows **Notepad** or an alternative text editor with administrator permissions.
2. Open the `C:\Program Files\Datamine\PA\Services\Time Service\imstimesvc.exe.config` file.
3. In the **components** section, update the following parts of the connection string if required:
   - Name of the SQL Server instance on the Database Server using either the hostname or IP address
   - Database name
   - Integrated Security

```
<parameter name="connectionString" value="server=localhost;database=Datamine_PA_
Services;Integrated Security=SSPI" />
```

4. In the **system.diagnostics** section, uncomment the following code if required:

```
<source name="System.ServiceModel"
switchValue="Warning,Error,Critical"
propagateActivity="true">
  <listeners>
    <add name="traceListener"
    type="System.Diagnostics.XmlWriterTraceListener"
    initializeData= "C:\Datamine\PA\Logs\datamine.ims.time.service.svclog" />
  </listeners>
</source>
```

> **Note:** The `datamine.ims.time.service.svclog` file is created automatically when it is first needed.

5. Save and close the `imstimesvc.exe.config` file.

Create the database tables and register the Time Service:

> **Note:** If using a domain account instead of the Network Service account, replace **NT Authority\Network Service** with the domain account in the commands in this activity.

1. Open Windows **Command Prompt** with administrator permissions.
2. Run the following command to navigate to the Time Service folder:

```
cd C:\Program Files\Datamine\PA\Services\Time Service
```

3. Run the following command to create the database tables for the Time Service:

```
imstimesvc.exe -install_db
```

4. Run one of the following commands as required to register the Time Service with:
   a. The Network Service account.

```
imstimesvc.exe -install --user="NT Authority\Network Service"
```

   b. The domain account.

```
imstimesvc.exe -install --user="domain\username" --password="password"
```

5. Run the following command to delay the start of the Time Service:

```
sc config "Datamine IMS Time Service" start= delayed-auto
```

6. Run the following command to add a description to the Time Service:

```
sc description "Datamine IMS Time Service" "Production Accounting Time Service"
```

7. Run the following command to reserve the specified URL for the domain account or Network Service account.

```
netsh http add urlacl url=http://+:10002/time/ user="NT Authority\Network Service"
```

8. Run the following command to register the Time Service with the Application log in Windows Event Viewer for logging messages:

```
imstimesvc.exe -e
```

9. Press **Ctrl + C** to stop the Time Service.
10. Open the Windows **Services** application.

11. Verify that the Datamine IMS Time Service has been installed with:
    - A startup type of automatic (delayed start)
    - The domain account or Network Service as the logon user

Message Queue Permissions

The following message queues are created when the applicable services are started for the first time.

- datamine.ims.notification.service.events
- datamine.ims.notification.service.eventsdl
- datamine.ims.audit.service.events
- datamine.ims.audit.service.eventsdl
- datamine.ims.log.service
- datamine.ims.log.servicedl

Enable full control of message queues for the domain account or NETWORK SERVICE:

1. Open the Windows **Control Panel** on the Application Server.
2. Select **Administrative Tools**.
3. Double-click **Computer Management**.
4. Expand the **Services and Applications » Message Queuing** node.
5. Expand the **Private Queues** node.
6. Right-click the **datamine.ims.notification.service.events** node and select **Properties** from the menu.

   The **datamine.ims.notification.service.events Properties** screen displays.
7. Select the **Security** tab.
8. Add the user:
   a. Click **Add**.
   b. Search for and select the domain account or **NETWORK SERVICE**.
   c. Click **OK**.
9. Select **Allow Full Control** in the **Permissions** list.
10. Change the owner of the message queue:
    a. Click **Advanced**.
    b. Click **Change** next to **Owner**.
    c. Search for and select the domain account or **NETWORK SERVICE**.
    d. Click **OK**.
11. Click **OK**.

    The **datamine.ims.notification.service.events Properties** screen closes.

12. Repeat steps 6–12 for the other Production Accounting message queues in the list above.

IMS Integration Hub Message Queue Configuration

The **datamine.ims.transactionqueue** message queue is created when Production Accounting is started for the first time.

The following additional message queue configuration on the Application Server is only required if using Production Accounting with IMS Integration Hub.

> **Note:** The following message queue names must match the message queue names in `DistributionManager.Service.exe.config` and `DistributionManager.Server.exe.config` in the IMS Integration Hub installation.

Create the datamine.ims.ihub_registersubscribers message queue:

1. Open the Windows **Control Panel** on the Application Server.
2. Select **Administrative Tools**.
3. Double-click **Computer Management**.
4. Expand the **Services and Applications » Message Queuing** node.
5. Right-click the **Private Queues** node and select **New » Private Queue** from the menu.

   The **New Private Queue** dialog box displays.
6. Enter **datamine.ims.ihub_registersubscribers** as the **Queue name**.
7. Select **Transactional**.
8. Click **OK**.

   The **New Private Queue** dialog box closes.
9. Expand the **Private Queues** node.
10. Right-click the **datamine.ims.ihub_registersubscribers** node and select **Properties** from the menu.

    The **datamine.ims.ihub_registersubscribers Properties** screen displays.
11. On the **General** tab, check **Authenticated**.
12. Select the **Security** tab.
13. Add the user:
    a. Click **Add**.
    b. Search for and select the domain account or **NETWORK SERVICE**.
    c. Click **OK**.
14. Select **Allow Full Control** in the **Permissions** list.

15. Click **OK**.

    The **datamine.ims.ihub_registersubscribers Properties** screen closes.

Create the datamine.ims.ihub queue:

1. Repeat Steps 5 - 15 to create the **datamine.ims.ihub** message queue.

Configuration Editor Installation

The Configuration Editor provides an interface to:

- Define a configuration for Production Accounting
- Load that configuration into the portal databases

Using the Configuration Editor avoids the need to load configuration with SQL commands.

Apart from setting up the file structure on the Production Accounting Application Server, no further installation is required for the Configuration Editor.

Start up Production Accounting

When installation is complete and the services have been created and configured, Production Accounting can be started.

Activity Steps

1. On the Application Server, start the Production Accounting services in the following order:
    a. Notification Service
    b. Audit Service
    c. Logging Service
    d. Time Service
    e. JKMA Service
2. On the Application Server, open Microsoft Edge and enter **http://server-name or fully-qualified-server-name** or **https://server-name or fully-qualified-server-name**, depending on whether SSL is enabled..

    The **Login** screen displays.

    > **Note:** If *Can't reach this page* or *This site is not secure* displays, trust the certificate. See "Internet Browser Configuration" on page 101.
3. Log in using *admin* and no password.
4. Navigate to **Admin » Systems**.
5. Ensure all systems are green.

Permissions Editor Installation

The Permission Editor provides an interface to:

- Define user and group security permissions for Production Accounting
- Load that configuration directly into the running portal

Apart from setting up the file structure on the Production Accounting Application Server, no further installation is required for the Permissions Editor.

However, to be able to use the Permissions Editor, each required Windows user must be added as a Production Accounting user with permissions to the Authorisation Loading Service.

To add a Windows user as a Production Accounting user:

1. On the Application Server, create a local Windows user.

   > **Note:** This user has the sole purpose of managing Production Accounting permissions, and does not need to be added to any user groups such as the Administrators user group.

2. In Production Accounting, select **Admin » Users/Groups** from the menu.
3. Select **New User**.
4. Enter the local Windows user name in the **Username** field.
5. Complete the following fields.

   Family Name

   Given Name

   Email

   Password

   Confirm Password

   > **Note:** Real values do not have to be given for these fields. This user will not need to log in to Production Accounting with this username. However, the user must be registered with Production Accounting in order to use the Permissions Editor.

6. Click **Save**.

To add Authorisation Loading Service permissions:

1. In Production Accounting, select **Admin » Permissions** from the menu.
2. Select the local Windows user in the **Users and Groups** tree.
3. Select the **Authorisation Loading Service** node in the **SecurityRoot** tree.

4. Select the local Windows user as the **User permitted to access this resource**.
5. Click **Save Permission**, even if **User permitted to access this resource** was already selected.
6. Activate the Security Permissions service for a period of time:
    a. Enter a number of hours in **Activate Service**.
    b. Click **Activate**.

> **Note:** The registered Windows user can use the Permissions Editor while logged into the Application Server for the specified period of time. If the Permissions Editor needs to be used again later by this user, repeat step 6.

To run the Portal Permissions Editor:

The Portal Permissions Editor is an external tool to manage Production Accounting permissions. The tool allows permissions to be exported, saved and re-imported.

1. On the Application Server, navigate to the `C:\Program Files\Datamine\PA\Configuration\Permissions Editor` folder.
2. Hold down Shift while right-clicking the `Security.Permissions.Editor.exe` file and select **Run as different user** from the menu.
3. Enter the details of the local Windows user.

Production Accounting Analytics Installation

Production Accounting's analytics capabilities are powered by integration with Datamine's Centric application.

To enable Production Accounting Analytics, Centric must be installed and configured on the Application Server.

> **Note:** To enable analytics for an existing Production Accounting configuration, upgrade Production Accounting to the latest version first. See "Upgrade Production Accounting" on page 114.

Analytics Installation Prerequisites

A local IT administrator must complete the following prerequisite tasks before you install Production Accounting Analytics.

Provision the required databases and users:

The following blank databases must be created in SQL:

- *Datamine_PA_Analytics*
- *Datamine_PA_Analytics_Warehouse*

For both databases, the following user accounts and roles are required:

- The domain or Network Service account used to run Production Accounting Analytics must have the **dbowner** role.
- A dedicated SQL user with the **dbowner** role must also be provisioned. This user account is needed to install Centric.

Set up Production Accounting Analytics

Install Centric on the Application Server:

1. Open the `PA Analytics` folder in the Production Accounting file package.
2. Run the `Centric2.21.exe` installer with administrator permissions.
3. Follow the detailed installation steps described in the separate Centric Installation Guide.

4. When prompted to enter the **SQL instance and database information**:
    a. Enter the **Server Name** of the SQL Server instance on the Database Server.
    b. Select **Specify Username and Password (SQL Authentication)**.
    c. Enter the **Login** and **Password** for the dedicated SQL user provisioned for the Centric installation. See "Analytics Installation Prerequisites" on the previous page for more information.
    d. Click **Test Connection**.
5. When prompted to select a **New or existing database**:
    a. Select **Use an existing database**.
    b. From the **Database Name** list, select *Datamine_PA_Analytics*. See "Analytics Installation Prerequisites" on the previous page for more information.
6. When prompted to **Select Installation Address**, enter or select the following values:
    a. **Site**—*Default Web Site*.
    b. **Virtual Directory**—*PAAnalytics*
    c. **Mobile Virtual Directory**—*Mobile* (default).
    d. **Culture**—Select the required user interface culture. This controls the language and display of culture-dependent data such as dates and numbers.
7. When prompted to select the **Destination Folder** to install Centric, use the default location: `C:\inetpub\wwwroot\PAAnalytics`.

    > **Important:** If you change the destination folder to a protected location such as `Program Files`, the installation will fail.

8. Follow the prompts to finish the installation.

    > **Important:** For new installations, a web browser opens and displays prompts to enter license key and user details. **Do not** complete these fields now. You must update some authentication settings first.

9. Close the web browser.

Enable access to the CentricReporting folder:

1. In Windows Explorer, go to `C:\Windows\Temp\`.
2. Create a new folder and enter the name as *CentricReporting*.

3. Right-click the `C:\Windows\Temp\CentricReporting` folder and select **Properties** from the menu.

   The **CentricReporting Properties** screen displays.
4. Select the **Security** tab.
5. Click **Edit**.

   The **Permissions for CentricReporting** screen displays.
6. Add the application pool identity or user under which Production Accounting Analytics runs:
   a. Click **Add**.
   b. Search for and select the user (for example, the domain account or **NETWORK SERVICE**).
   c. Click **OK**.
7. Select **Allow Full Control** in the **Permissions** list.
8. For other Production Accounting user groups, repeat step 6 to add if required, and select **Read & execute** in the **Permissions** list.
9. Click **Apply**.
10. If a Windows Security message about changing permission settings displays, click **Yes**.
11. Click **OK**.

    The **Permissions for CentricReporting** screen closes.
12. Click **Advanced**.

    The **Advanced Security Settings for CentricReporting** screen displays.
13. Select **Replace all child object permission entries with inheritable permission entries from this object**.
14. Click **Apply**.
15. If Windows Security messages display about inheritable permissions and/or changing permission settings, click **Yes** to continue.
16. Click **OK**.

    The **Advanced Security Settings for CentricReporting** screen closes.
17. Click **OK**.

    The **CentricReporting Properties** screen closes.

Configure the application pool and authentication settings:

1. Open the Windows **Internet Information Services (IIS) Manager** application.
2. Configure an application pool:
    a. Expand the node for the IIS server in the **Connections** list and select **Application Pools**.

       The **Application Pools** display in the middle panel.
    b. Select **Add Application Pool** in the **Actions** menu in the right-hand panel.

       The **Add Application Pool** dialog box displays.
    c. Enter the **Name** as *PAAnalytics* and use the default selections for other fields.
    d. Click **OK**.

       The **Add Application Pool** dialog box closes.
    e. Right-click the **PAAnalytics** application pool and select **Advanced Settings...** from the menu.

       The **Advanced Settings** dialog box displays.
    f. In the **Process Model** group, set the **Identity** to the same account used for the **DefaultAppPool**.
    g. Click **OK**.

       The **Advanced Settings** dialog box closes.
3. Change authentication settings:
    a. Select the **Sites » Default Web Site » PAAnalytics** node in the **Connections** list.
    b. Double-click the **Authentication** icon.

       The **Authentication** settings display in the middle panel.
    c. Set **ASP.NET Impersonation** to *Disabled*.
4. If you are installing Analytics **as part of an upgrade to an existing Production Accounting configuration only**, disable redirection:
    a. In the **Connections** list, select **Default Web Site**.
    b. Double-click the **HTTP Redirect** icon.

       The **HTTP Redirect** settings display in the middle panel.
    c. Uncheck **Redirect requests to this destination**.
    d. Select **Apply** in the **Actions** menu in the right-hand panel.
5. Close the **Internet Information Services (IIS) Manager**.

6. Reset the internet services:
    a. Open Windows **Command Prompt** with administrator permissions.
    b. Run the following command.

```
iisreset
```

Create the Centric administrator user and initialize databases:

1. Open the Microsoft Edge web browser.
2. Enter the URL to access Production Accounting Analytics:
    a. If using SSL, enter *https://<applicationservername>/PAAnalytics/*, where *<applicationservername>* is replaced with the correct Application Server name.
    b. If not using SSL, update the Centric `web.config` file before you access the site:
        1. Open Windows **Notepad** or an alternative text editor with administrator permissions.
        2. Open the `C:\inetpub\wwwroot\PAAnalytics\web.config` file.
        3. In the **appSettings** section, update the **SameSiteNone** key value to *false*.

```
<add key="SameSiteNone" value="false" />
```

        4. Save and close the `web.config` file.
        5. Enter the applicable URL; for example, *http://localhost/PAAnalytics* or *http://<applicationservername>/PAAnalytics/*, where *<applicationservername>* is replaced with the correct Application Server name.

           A Centric welcome screen displays.
3. Enter the required license key and administrator user information.

> **Note:** Refer to the Centric Installation Guide for password requirements and recommendations for configuring the admin user. Securely record the administrator user credentials for later use.

4. Click **Initialize Database**.

   The blank Centric database is populated with the required tables and default configuration. A Centric log in page displays.
5. Enter the administrator **User Name** and **Password** you created at step 3 and click **Log In**.

The Centric application loads and displays the administrator user's home page.

Generate the API token:

1. Click the settings (cog) icon in the top right of the Centric screen.

   The **User Settings** dialog displays.
2. Next to **API Token**, click **Generate**.

   The token is created and displays in a text field.
3. Click the copy icon below the field.
4. Click **Save**.
5. If applicable, paste the token directly into the required key in the Production Accounting `Web.config` file. See "Edit the Web.config File" on page 58. Or, you can return to the **User Settings** dialog later and copy the token when you need it.

Update configuration settings

Update the settings for Production Accounting Analytics in the `Web.config` file. See "Edit the Web.config File" on page 58.

Configure the analytics time zone:

1. In the Centric menu, click **More Tools**.
2. Under the **General** category, select **Settings**.

   > **Note:** Start typing "settings" into the **Filter** field to find it quickly.

   The **App Settings** display in the middle panel.
3. Select **Analytics**.
4. Set the **Analytics Time Zone** to the same as the Production Accounting Database Server.
5. Click **Save**.

Configure the custom display:

This activity customises the Centric user interface display for integration with Production Accounting.

1. In the Centric menu, click **More Tools**.
2. Under the **General** category, select **Settings**.

   > **Note:** Start typing "settings" into the **Filter** field to find it quickly.

   The **App Settings** display in the middle panel.

3. Select **Layout**.
4. Configure the **Layout** settings:
    - **Enabled**—*Yes*
    - **Key**—*PAView*
5. Configure the **Header Bar** settings:
    - **Enabled**—*No*
    - **Title**—Set to *Yes* and enter the **Title** as *Production Accounting Analytics*. Then change back to *No*.
6. Configure the **Menu** settings:
    - **Enabled**—*No*
    - **Desktops**—*No*
    - **Recent Items**—*No*
    - **Favorites**—*No*
7. Configure the **Breadcrumb Bar** settings:
    - **Enabled**—*No*
    - **Home**—*No*
    - **Hide Bar**—*Yes*
8. Click **Save**.

Map Centric groups to Active Directory groups:

This activity creates a mapping between Centric groups and Active Directory groups.

1. In the Centric menu, click **More Tools**.
2. Under the **General** category, select **Settings**.

    > **Note:** Start typing "settings" into the **Filter** field to find it quickly.

    The **App Settings** display in the middle panel.
3. Select **Authentication**.
4. Configure the **Account Provisioning** settings:
    - **Enabled**—*Yes*
    - **Account Name Type**—*Full Name*
    - **Full Name Claim**—*http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name*

5. Configure the **Permission Provisioning** settings:
    - **Enabled**—*Yes*
    - **Groups Claim**—*http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid*
6. In the **Administrator Claim** field, enter the names of the Active Directory administration group(s). Separate group names with a comma.
7. In the **Tool Managed Group Name** category, enter the following:
    - **Analytics**—Active Directory group names for user groups who can view analytics dashboards. Separate group names with a comma.
    - **Reports**—Active Directory group names for user groups who can view reports. Separate group names with a comma.
8. Click **Save**.

Save the Data Services Add-in to the local network:

Copy the `DataServiceAddin.exe` file from the installation package to a shared network location that users can access.

With the add-in installed on their machine, users can connect to Production Accounting Analytics Data Services and retrieve data into Excel for analysis.

> **Note:** Configuration of analytics dashboards and reports in Centric is outside the scope of this guide. Datamine consultants can contact the Production Accounting R&D team for additional configuration support.

Internet Browser Configuration

Production Accounting has been tested with Microsoft Edge.

Self-Signed Certificate Trust in Edge

Adding Production Accounting as a trusted local intranet site is required if *Your connection isn't private* or *NET::ERR_CERT_AUTHORITY_INVALID* displays when accessing Production Accounting. This activity may also be required for Production Accounting to display secure reports created with SQL Server Reporting Services (SSRS).

By default, browsers will not accept a self-signed certificate. Importing the certificate is required if *Your connection isn't private* or *NET::ERR_CERT_AUTHORITY_INVALID* displays when accessing Production Accounting.

These activities may not be required if using a different certificate authority.

Add Production Accounting as an Intranet Site:

1. Open the Windows **Internet Options** screen.
2. Select the **Security** tab.
3. Select **Local Intranet**.
4. Click **Sites**.

   The **Local intranet** dialog box displays.
5. Enter **http://server-name or fully-qualified-server-name** or **https://server-name or fully-qualified-server-name**, depending on whether SSL is enabled.
6. Click **Add**.
7. Click **Close**.

   The **Local intranet** dialog box closes.
8. Click **OK**.

   The **Internet Options** screen closes.

Export and Store the Certificate:

1. Open the **Microsoft Edge** browser.
2. Enter the Production Accounting web address.
3. In the Edge browser address bar, click **Not secure**.

   A menu displays with certificate and security options.
4. Click the *Your connection to this site isn't secure* message.

   The message expands with more detail.

5. Export the certificate:
    a. Click the **Certificate** icon in the top-right corner.
    The **Certificate** screen displays its details.
    b. Select the **Details** tab.
    c. Click **Copy to File**.
    The **Certificate Export Wizard** displays.
    d. Click **Next**.
    e. Select the *DER encoded binary X.509 (.CER)* format.
    f. Click **Next**.
    g. Enter a temporary path and **File name**.
    h. Click **Next**.
    i. Click **Finish**.
    A status message displays.
    j. Click **OK**.
    k. On the **Certificate** screen, click **OK**.
    The **Certificate** screen closes.
6. Store the certificate:
    a. On the Edge browser ellipsis (...) menu, select **Settings**.
    b. Select **Privacy, search, and services**.
    c. Under **Security**, select **Manage certificates**.
    The **Certificates** screen displays.
    d. Select the **Trusted Root Certification Authorities** tab.
    e. Click **Import**.
    The **Certificate Import Wizard** displays.
    f. Click **Next**.
    g. Click **Browse** to browse for and select the temporary certificate file that you exported.
    h. Click **Next**.
    i. On the **Certificate Store** screen:
        1. Select **Place all certificates in the following store**.
        2. Set **Certificate store** to *Trusted Root Certification Authorities*.
        3. Click **Next**.

j. Click **Finish**.

   A security warning displays.

k. Click **Yes**.

   A status message displays.

l. Click **OK**.

m. Click **Close**.

   The **Certificates** screen closes.

7. Restart the Edge browser for the certificate to take effect.

Pop-ups

Pop-ups must be enabled. The first time Production Accounting uses a pop-up, Microsoft Edge displays a confirmation message about pop-ups. Accept the confirmation message.

Email Notification Configuration

Production Accounting includes email notification functionality to support efficient data authorisation and quarantine workflows. If configured, the system can send automated emails to nominated recipients to notify them of pending tasks; for example, data authorisation processes to approve or quarantined data to review.

Production Accounting 1.13 introduces enhanced email notification functionality that is specific to data quarantine. In future releases, this feature will be extended to other email notifications. Datamine consultants will continue to set up other types of email notifications in a separate configuration process, which is not included in this Installation Guide.

> **Note:** The information and activities in this section are to enable the PA Core email functionality (currently for quarantine notifications only). Some activities assume that the site uses Microsoft Azure.

Email Notification Prerequisites

The following prerequisite tasks must be done by a local IT administrator before the email notification functionality can be configured.

User Account and Email Provision

A dedicated user account and email are required for the purpose of sending emails from the Production Accounting application. This email account appears as the sender in the automated email notifications sent to Production Accounting users.

The email account should be a generic system account, not the email address of an individual user or administrator. If a domain or service account is used to run Production Accounting, the email associated with that domain or service account could be used. Otherwise, an alternate account and email must be provisioned.

> **Note:** Datamine recommends using *no-reply* in the email address or display name to indicate that the email is from an unmonitored address to which users should not reply.

The local IT administrator must provide the Datamine consultant with the account credentials to enable configuration and testing of the email notification functionality. If multi factor authentication or other verification steps are required, the local IT administrator may need to help the Datamine consultant authenticate the account during the configuration steps.

Open Authorisation (OAuth) and Microsoft Azure Configuration

For sites using OAuth with Microsoft Azure, email notification configuration requires that an application (or 'app') registration is created to register Production Accounting with Microsoft's identity platform, Entra.

For detailed information and instructions for app registration in Microsoft Entra, see https://learn.microsoft.com/en-us/entra/identity-platform/quickstart-register-app.

Microsoft Entra App Registration Settings and Permissions

The table below describes required and recommended settings for the Microsoft Entra app registration. Fields not described below are not required for the Production Accounting email notification functionality.

Microsoft Entra Property	Required or Recommended Settings
Name	The recommended application display name is *Production Accounting*. Use the organisation's naming conventions for production and non-production environments as required. **Note:** The app registration's automatically generated Application (client) ID, not its display name, uniquely identifies the app within the identity platform.
Supported account types	The required selection depends on the organisation's Microsoft Entra tenant structure. For most scenarios, *Accounts in this organizational directory only* is recommended. **Note:** Datamine recommends that the app registration and the identity and email account used as the sender for the Production Accounting email notifications are in the same tenant (directory).
Homepage URL	If required, enter the URL for the Production Accounting application homepage. Format the URL as per the examples below, depending on whether SSL is enabled. • http://*server-name or fully-qualified-server-name*/PA • https://*server-name or fully-qualified-server-name*/PA **Note:** The homepage URL is different from the redirect URL below.
Platform configuration	Only **Web** is required.
Redirect URL	Required for the **Web** platform only. A redirect URL is the location where the Microsoft identity platform redirects a user's client and sends security tokens after authentication. Format the redirect URL as per the example below, where *hostname* is replaced with the Application Server name and *portnumber* is replaced with the default or unique port number used to configure the PA Core website (see "Required IIS Configuration" on page 42). *https://hostname:portnumber/auth-callback* **Note:** Do not enter the redirect URL on the first screen in the app registration process. Enter it for the Web platform only, on the **Configure platforms** screen.

Microsoft Entra Property	Required or Recommended Settings
Credentials	Create a **Client Secret** to provide to Datamine. **Certificates** and **Federated Credentials** are not required.
Application owner	If an application owner is required, Datamine recommends using the organisation's IT admin account.
API role and scope	Not required.
API permissions	The following permissions are required: • *Mail.Send* • *Mail.Send.Shared* • *User.Read* • *offline_access* **Note:** The Production Accounting email notification functionality uses the Microsoft Graph Rest API. • For an overview, see https://learn.microsoft.com/en-us/graph/permissions-overview?tabs=http#permission-types. • For more about Graph API sendMail, see https://learn.microsoft.com/en-us/graph/api/user-sendmail?view=graph-rest-1.0&tabs=http#permissions. • For the complete Graph API permissions reference, see https://learn.microsoft.com/en-us/graph/permissions-reference.
Permission settings	For each permission listed above, configure the following: • **Type**— *Delegated* • **Admin consent required**—*No* (Recommended) **Note:** Permissions can be configured to require admin consent or user consent. Both consent options support the configuration of Production Accounting email notifications. The organisation's security and permissions policies should determine which option to use. The email notification configuration and authentication steps vary slightly based on the option selected. • For detailed information about application permissions, see https://learn.microsoft.com/en-

Microsoft Entra Property	Required or Recommended Settings
	us/entra/identity/enterprise-apps/manage-application-permissions. • For an overview of Microsoft Entra ID user and admin consent, see https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/user-admin-consent-overview.
Token configuration	Select *ID tokens*.

Required App Registration Details for Datamine Consultants

After completing the app registration, the local IT administrator must provide the following details, which are required to enable email notifications in Production Accounting:

- **Tenant ID**—The unique identifier for the organisation's Microsoft identity platform tenant.
- **Client ID**—Also called the **Application ID**. The unique identifier for the app in the Microsoft identity platform.
- **Client Secret**—Also called an **Application Password**. The client secret is a string value the app can use in place of a certificate to identity itself.

SMTP Server Configuration

For sites using Simple Mail Transfer Protocol (SMTP), the methods described below can be used to configure and test Production Accounting's email notification functionality. The local IT administrator must provide the following details, which are required to enable email notifications in Production Accounting.

SMTP

Because authentication with username and password is less secure, Datamine does not generally recommend this method.

Required details for configuration:

- **Email Host**—The SMTP server hostname. Usually starts with *smtp*; for example, *smtp.emailprovidername.com*.

- **Sender Address**—The email address from which the automated system notifications will be sent; for example, *productionaccounting@emailprovidername.com*. See "User Account and Email Provision" on page 104.
- **Enable TLS**—Optional. Can be selected if the SMTP server uses the Transport Layer Security (TLS) security protocol.
- **Port Number**—The port number that the SMTP email server uses for communication; for example, *25* or *587*.
- **Username**—Optional. The email address from which the automated system notifications will be sent; for example, *productionaccounting@emailprovidername.com*. See "User Account and Email Provision" on page 104.
- **Password**—Optional. The password for the sender email account.

> **Note:** The local IT administrator should refer to the email service provider's support documentation for how to obtain the SMTP hostname and port number.

SMTP with App Code

Using SMTP with an app code is recommended for secure authentication.

Required details for configuration:

- **Email Host**—The SMTP server hostname. Usually starts with *smtp*; for example, *smtp.emailprovidername.com*.
- **Sender Address**—The email address from which the automated system notifications will be sent; for example, *productionaccounting@emailprovidername.com*. See "User Account and Email Provision" on page 104.
- **App Code**—A unique code or password generated by the email service provider to authorise the Production Accounting application to send emails using the specified host and sender address.

> **Note:** The local IT administrator should refer to the email service provider's support documentation for how to obtain the SMTP hostname and app code.

Postmark (Datamine testing only)

The Postmark API is provided only for Datamine consultants to test an SMTP configuration from their local machine on the Datamine network. The Postmark API allows consultants to use their Datamine Microsoft Outlook account as the sender and recipient email address for testing purposes.

Required details for configuration:

- **Email Host**—*smtp.postmarkapp.com*
- **Sender Address**—The email address from which the automated system notifications will be sent; for example, *productionaccounting@emailprovidername.com*. See "User Account and Email Provision" on page 104.
- **API Key**—Datamine consultants should request the API Key from the Datamine IT team.

Enable Email Notifications

The user(s) who will set up email notifications; for example, the Default Administrator user or Datamine consultant, must have edit permissions or be in a group with edit permissions for email notification configuration.

For new installations as of Production Accounting 1.13.1, the Admins group (and any user in the Admins group, including the Default Administrator user) has edit permissions for email notification configuration by default. When upgrading from a previous version, permissions must be manually assigned. If required, complete the activity steps below to assign the permissions to a group or user.

Assign email notification configuration permissions:

1. Open the Production Accounting default web site in Microsoft Edge and log in as required.
2. Navigate to **Admin » Permissions**.
3. Expand the **Users and Groups** node.
4. Expand the **Users** or **Groups** node if required.
5. Select the required **User** or **Group**.

   The selected **User** or **Group** displays in bold font.
6. Expand the **SecurityRoot** node and select **Email Notification Configuration**.

   The settings for the selected user or group and the permission category display.
7. From the **Email Notification Configuration** drop-down list, select *Edit*.
8. Click **Save Permission**.

Configure the menu item and page host:

1. Navigate to **Admin » Portal Layout**.
2. Click **Create New Tab**.

3. Enter page settings:
    - **Page Name**—Enter *Email Configuration*.
    - **Move Under**—Select *Admin*.
4. In the module settings table, click **New Module**.
5. Enter module settings:
    - **Name**—*Email Configuration*.
    - **Module**—Select *Page Host*.
6. Click **Save**.
7. Navigate to **Admin » Email Configuration**.

    The message *No URL has been set for this page host. Please set a URL.* displays.
8. Click the settings icon.
9. Enter the **URL to display** in the format *https://hostname:444/emailConfiguration*, where:
    - The *hostname* is replaced with the Application Server name.
    - The default port number *444* is replaced with the correct unique port number if configured for the PA Core website.
10. Click **Submit** and refresh the screen if required.

    The **Email Configuration** module displays.

Configure email notifications:

1. Navigate to **Admin » Email Configuration**.
2. Click **Add**.

    The **Email Configuration Form** displays.
3. Select the **Email Configuration Method** from:
    - *OAuth*
    - *SMTP*
    - *SMTP With AppCode*
    - *Postmark*—For Datamine consultant use only to test SMTP configuration.

4. Configure the following settings:
    a. For **OAuth**, enter the **Tenant ID**, **Client ID** and **Client Secret**.
    b. For **SMTP**:
        1. Enter the **Email Host** and **Sender Address** and **Port Number**.
        2. If required, select **Enable TLS**.
        3. If required, enter the **Username** and **Password**.
    c. For **SMTP With AppCode**, enter the **Email Host**, **Sender Address** and **App Code**.
    d. For **Postmark**, enter the **Email Host**, **Sender Address** and **API Key**.

    > **Note:** Values for these settings must be provided by the local IT administrator.

5. Click **Submit**.

    The **Email Configuration Form** closes. The email configuration settings display.

6. Click **Test Email**.

    The **Send Email** dialog box displays.

7. Enter a **Test Email Recipient** email address. This recipient receives a test email from the Production Accounting system when you complete these activity steps. The recipient email is used for testing only and is not stored in the configuration settings. For example, you may send the test email to yourself or another user who can verify that the test email was received.

8. Click **Send**.

    For SMTP, SMTP With AppCode or Postmark configurations, go to step 14.

    For OAuth configurations, a new browser tab opens and displays sign in prompts. The credentials you enter on this screen must be for the account from which the automated system notifications will be sent (not the recipient email entered at the previous step). A dedicated email address must be provisioned for this purpose. See "User Account and Email Provision" on page 104.

9. Sign in with the credentials provided by the local IT administrator and complete multi factor authentication or verification steps if required.

    A **Permissions requested** or **Approval required** screen may display app permissions that are required for Production Accounting to send emails from the account. The message displayed depends on the consent option configured in the Microsoft Entra app registration. See "Microsoft Entra App Registration Settings and Permissions" on page 105.

10. Click **Accept** or **Request Approval**.

    > **Note:** If approval is required, wait for a local IT administrator to action the approval request before you continue.

    If configuration and authentication were successful, a confirmation message displays.

    > **Note:** If the configuration and authentication fails, an error message displays. To troubleshoot, check the log file in `C:\Program Files\Datamine\PA\Logs`.

11. Close the browser tab with the confirmation message.
12. Select the browser tab with the **Email Configuration** screen.
13. If the **Configured Email Address** displays **---**, refresh the screen so that the correct email displays.
14. As a separate activity in an external email application, confirm that test email recipient received an email with the subject *Test Email from PA*.

> **Note:** This activity is required as part of the Production Accounting installation to enable the system to send automated emails. Additional activities are required to set up the various email notifications, including configuring message templates and adding recipients. See the separate Production Accounting Configuration Guide.

Upgrade Production Accounting

> **Important:** Before upgrading Production Accounting, back up the:
> - **Datamine_PA_Data**, **Datamine_PA_Portal**, **Datamine_PA_Services** and **Datamine_PA_JKMA** databases.
> - `C:\Datamine\PA` folder.
> - `C:\Program Files\Datamine\PA` folder.
>
> Backup configuration files are essential for reference purposes.

Upgrading from 2.0.0 or earlier

Run `Data Upgrade 2.0.0 to 2.0.1.sql` and `Portal Upgrade 2.0.0 to 2.0.1.sql` to upgrade the Production Accounting and Portal databases (and other scripts as required).

Upgrading from 1.14.0 or earlier

Run upgrade scripts

Run `Data Upgrade 1.14.0 to 2.0.0.sql` to upgrade the Production Accounting database (and other scripts as required).

Update service configuration files

The Audit Service and Logging Service can now run clean-up and database maintenance processes to help keep databases manageable.

1. For the Audit Service, update settings in the new **processRestartCleanup** section of the `imsauditsvc.exe.config` file as required. See "Production Accounting Audit Service" on page 73.
2. For the Logging Service, update settings in the new **logCleanup** section of the `imslogsvc.exe.config` file as required. See "Production Accounting Logging Service" on page 78.

Upgrading from 1.13.2 or earlier

Run `Data Upgrade 1.13.2 to 1.14.0.sql` to upgrade the Production Accounting database (and other scripts as required). If your configuration includes integration with JKMetAccount, complete the activities below.

> **Note:** Database upgrade scripts for Production Accounting 1.14.0 may take some time to run, especially for large databases. Datamine recommends that you plan and test your upgrade process accordingly.

JKMetAccount

Production Accounting 1.14.0 includes structural changes for the JKMetAccount balance engine. The balance engine is now included in the core Production Accounting application, and no longer runs as a separate service. To upgrade a Production Accounting configuration that includes JKMetAccount, complete the activities below.

Update IMS Integration Hub adaptor for JKMetAccount integration

The IMS Integration Hub adaptor(s) for JKMetAccount integration must be updated. Please contact your Datamine representative for help with adaptor updates.

Run the JKMetAccount database upgrade script

Run `JKMA Upgrade 1.13.2 to 1.14.0.sql` in the installation package to update the JKMetAccount databases.

Activate the balance engine in the Bootstrap.config file

The default `Bootstrap.config` file includes updates to the JKMA Data Transfer Manager **Application** section. Edits are required in this file to activate the new JKMetAccount balance engine. See "Edit the Bootstrap.config File" on page 65.

Disable or delete the JKMetAccount Service

1. To disable the service:
    a. Open the Windows **Services** application.
    b. Stop the JKMetAccount Service.
    c. Right-click the JKMetAccount Service and select **Properties** from the menu.
    d. Set the **Startup type** to *Disabled*.
    e. Click **OK**.

2. To delete the service:
    a. Open Windows **PowerShell** with administrator permissions.
    b. Run the following command to stop the JKMetAccount Service, substituting the correct value for the service name if required.

```
Get-Service -Name "JKMAService" | Stop-Service -Force
```

    c. Run the following command to delete the JKMetAccount Service, substituting the correct value for the service name if required.

```
sc.exe delete "JKMAService"
```

    d. Close **Powershell**.

Upgrading from 1.13.1 or earlier

Production Accounting 1.13.2 introduces initial updates to support daylight saving. A **Data Upgrade Tool** is included in the installation file package to upgrade business process and quarantine data for compatibility with daylight saving functionality.

> **Note:** This upgrade procedure assumes that all business process data in the Production Accounting database has correct time zone and hour data. Any business process data with incorrect time zone and hour data must be repaired before completing the activity steps below. Please contact the Production Accounting R&D team for customised scripts and tools if required.

If your Production Accounting configuration is run in region with daylight saving, please discuss with a Datamine representative whether the new functionality is suitable for your configuration. If advised by a Datamine representative to do so, complete the activity steps below to enable daylight saving support.

Enable daylight saving support

1. Ensure that automatic adjustment for daylight saving is enabled on the Application Server and Database Server. See **Daylight Saving Settings** in "System Configuration before Installing Production Accounting" on page 12.
2. Use the **Production Accounting Configuration Editor** to update the Production Accounting Time Service configuration to **Use Daylight Savings** for each time interval.

3. Navigate to the `Setup\UpgradeScripts` folder of the Production Accounting file package.
4. Run the database upgrade scripts.
5. Navigate to the `Setup\UpgradeTools` folder and locate the `Data Upgrade Tool 1.13.1 to 1.13.2.exe` file.
6. Rename the executable file to append an underscore and the update type (*Process* or *Quarantine*); for example:
    - `Data Upgrade Tool 1.13.1 to 1.13.2_Process.exe`
    - `Data Upgrade Tool 1.13.1 to 1.13.2_Quarantine.exe`

    > **Note:** The Data Upgrade Tool must be run for both data types. Complete steps 6-10 for either *Process* or *Quarantine* and then repeat for the other data type.
7. Open the matching configuration file in Windows **Notepad** or an alternative text editor. The configuration file name is the same as the executable file name but is appended with `.config` for example, `Data Upgrade Tool 1.13.1 to 1.13.2_Process.exe.config`.
8. In the **appSettings** section, update the connection string **Initial Catalog** value to the required database name. The connection string is configured for Integrated Security but can be changed if required.

    ```
    <add key="ConnectionString" value="Data Source=localhost;Initial Catalog=Datamine_
    PA_Data;Integrated Security=SSPI"/>
    ```
9. Save and close the configuration file.
10. Run the executable file.
11. Repeat steps 6-10 to upgrade the other data type.

Upgrading from 1.12.4 or earlier

Production Accounting 1.13 introduces new functionality built on .NET Core. This requires the installation of .NET Core modules and the configuration of a new web site to run alongside the existing default web site (built on .NET Framework).

Create database tables for PA Core

Run the database upgrade scripts to create the new database tables required for PA Core.

Install .NET Core on the Application Server

A new. NET Core module is required for the Application Server. See **Microsoft .NET Core** in "System Configuration before Installing Production Accounting" on page 12.

Configure the PA Core web site and email notification functionality

See "Required IIS Configuration" on page 42 for steps to set up the new PA Core web site to run in conjunction with the existing PA default website.

See "Email Notification Configuration" on page 104 for steps to enable the new email notification functionality.

Update the Web.config file

See "Edit the Web.config File" on page 58 for the required updates to the **appSettings** and **system.webServer » httpProtocol » customHeaders** sections.

Upgrading from 1.12.3 or earlier

Reregister the Logging Service

Perform the following steps to reregister the Logging Service with the Application log in Windows Event Viewer for logging messages:

1. Open Windows **Command Prompt** with administrator permissions.
2. Run the following command to navigate to the Logging Service folder:

```
cd C:\Program Files\Datamine\PA\Services\Logging Service
```

3. Run the following command to enable the Production Accounting Portal to write messages to the Application log in Windows Event Viewer:

```
imslogsvc.exe -spaev
```

4. Run the following command:

```
imslogsvc.exe -e
```

5. Press **Ctrl + C** to stop the Logging Service.

Bootstrap.config file

The default `Bootstrap.config` file includes two new arguments in the Cascade Manager **Application** section. See "Edit the Bootstrap.config File" on page 65.

```
<!--Back off time before cascade retry, format 00:00:00-->
<arg></arg>
<!--True/False to allow or disallow task merging-->
<arg>False</arg>
```

Upgrading from 1.12.0 or earlier

After copying files as required and running the required database upgrade scripts, redeploy the current configuration using the current Configuration Editor before starting Production Accounting.

Upgrading from 1.9.1 or earlier

Complete the following tasks to upgrade to Production Accounting 1.12.

New files

> **Important:** The recommended file structure for Production Accounting has changed since Production Accounting 1.9.1. The new recommendation described in this Installation Guide is simpler to set up and more secure than previous recommendations.

Copy files from the following folders of the Production Accounting file package to locations as described for the Production Accounting file structure.

- `Portal` folder
- `Services` folder
- `Configuration` folder

Some files (for example, upgrade scripts) may be needed from the `Setup` folder, but this folder does not need to be copied to the Application Server for upgrades.

Configuration files

Re-configure each of the following files:

- `GlobalConfig.xml`
- `Web.config`
- `Bootstrap.config`
- `imsnotificationsvc.exe.config`
- `imsauditsvc.exe.config`
- `imslogsvc.exe.config`
- `imstimesvc.exe.config`

> **Important:** Most of these files have changed since Production Accounting 1.9.1. Do not use old configuration files. Use backed up files for reference purposes only.

Database schema change

The database schema has been changed to "**abb**". Run `Schema change to abb.sql` against the **Datamine_PA_Services** database.

This schema change also affects the following configuration files:

- `imsauditsvc.exe.config` (configuration file of the Audit Service)
- `imslogsvc.exe.config` (configuration file of the Logging Service)

Database update

The time format control list setting in the Data Process Manager has been converted to use IOC. The format is now determined from the name of the component rather than the class names. Run the `Portal Upgrade 1.10.0 to 1.11.0.sql` script to convert from assembly qualified class names to the component name.

Restart Production Accounting

Production Accounting completes the upgrade process when it is restarted for the first time.

Upgrading from 1.8 or earlier

In addition to the items listed above, contact your Datamine representative for assistance determining which database upgrade scripts should be run and in which order.

Disaster Mitigation and Recovery

Full and frequent backups of Production Accounting installation folders and the Production Accounting databases are essential to minimise data loss in the case of disaster.

In addition to regular server snapshots, Datamine recommends the following minimum backup routine.

Time/Frequency	Backup
Immediately after installation and configuration of Production Accounting	• Installation folders, including customised configuration files. • All Production Accounting databases • The JKMA database, if used
After every update to the Production Accounting installation	• Installation folders, including customised configuration files. • All Production Accounting databases • The JKMA database, if used
Before any Production Accounting configuration changes	• All Production Accounting databases
Daily	• All Production Accounting databases • The JKMA database, if used

Important Considerations

Test Environment

Datamine recommends that customers test their disaster recovery process in a test environment, before a disaster occurs.

Database Backups when Services are Running

Ideally, the Production Accounting Services should be stopped before backing up the Production Accounting databases. Stopping services ensures that all transactions are either committed or rolled back.

Datamine recognises that stopping and restarting services on a daily basis may not be practical. Database backups are still possible with the Production Accounting services running; however, should be taken at a time when the least number of users are logged in, or the least number of transactions are being processed. Follow Microsoft best practices for transactional database backups without interrupting the system operations.

Restoration from Backup

In case of failure on:

- The Application Server—Restore the latest server snapshot.
- The Database Server—Restore the latest server snapshot, or use standard SQL Server procedures to restore the latest database backups.

Support in Case of Disaster

Please contact your Datamine representative as soon as possible. Subject to your support policy with Datamine, your Datamine representative can assist you with restoration or repair of data and Production Accounting configuration, and with provision of new installation packages or update scripts if required.

Production Accounting Maintenance

This section described maintenance and troubleshooting activities on the Production Accounting Application Server.

Recover Messages from Dead-Letter and Poison Queues

This activity uses a special running mode of the Production Accounting Audit Service to recover messages in 'dead-letter' and 'poison' queues. This activity can be run concurrently with the regular Audit Service. That is, the Audit Service does not need to be stopped to make these configuration changes and run the recovery.

Expired or purged messages are moved to the dead-letter queues. Messages that fail processing repeatedly are moved to a poison queue. Running this recovery service can return Production Accounting log messages and data event messages to their regular queues for processing. Messages should be in the system transactional dead-letter queue only rarely.

> **Important:** This recovery service can only recover Production Accounting log messages (from the Logging Service) and data event messages (from the Audit Service, the Notification Service and the Production Accounting Portal). All other messages in the queues for the enabled endpoints will be dropped (that is, lost). Dropped messages are not logged.

You need to ensure that you have **Full Control** access to the affected private queues. Administrators already have access to the system queues.

In order to use this recovery service you must take note of where you are reading from (the **system.serviceModel » service**) and where you want the recovered messages to be sent (the **system.serviceModel » client**). Only uncomment the required endpoints in the configuration file. There are endpoints for reading from the custom dead-letter queues, poison queues and the system transaction dead-letter queue. Log and data event messages can be recovered simultaneously when reading from the system dead-letter queue.

Perform these steps on the Production Accounting Application Server.

Step 1: Determine if there are Production Accounting messages in dead-letter or poison queues:

1. Open Windows **Computer Management**.
2. Expand **Services and Applications » Message Queuing**.
3. Select **Private Queues**.
4. Check the **Number of Messages** in the following queues (if they exist):
    - **datamine.ims.log.servicedl**—Custom dead-letter queue for the Logging Service
    - **datamine.ims.audit.service.eventsdl**—Custom dead-letter queue for the Audit Service

- **datamine.ims.notification.service.eventsdl**—Custom dead-letter queue for the Notification Service
- **datamine.ims.portal.eventsdl**—Custom dead-letter queue for the Production Accounting Portal
- **datamine.ims.log.service**—Regular queue for the Logging Service
- **datamine.ims.audit.service.events**—Regular queue for the Audit Service

5. If a regular queue has a **Number of Messages** greater than zero, expand that queue in the tree.

   If there is a node called **Poison**, there are messages in the poison queue for that service.
6. Expand **System Queues**.
7. Select **Transactional dead-letter messages**.
8. Review each message:
   a. Right-click a message and select **Properties** from the menu.
   b. Select the **Queues** tab.

      If the recipient or destination is related to Production Accounting, the message may be recoverable. Note the recipient name, because that indicates the queue to which to return the message. If there are multiple messages in this system queue, you may need to determine which messages have the highest importance. It may not be possible to recover all messages in this queue simultaneously. Any messages not recovered (including any not related to Production Accounting) will be dropped after running the recovery service for this queue.

Step 2: Enable access to the private queues (if you are recovering messages from those queues for the first time):

1. Open Windows **Computer Management**.
2. Expand **Services and Applications » Message Queuing**.
3. Select **Private Queues**.
4. Right-click an affected queue and select **Properties** from the menu.

   The **Properties** dialog box displays.
5. Select the **Security** tab.
6. Ensure you are the owner so that you can make changes to the queue:
   a. Click **Advanced**.

      The **Advanced Security Settings** dialog box displays.

b. If you are not the **Owner**, click the **Change** hyperlink.

   The **Select User, Computer, Account Service or Group** dialog box displays.

c. Enter yourself as the owner.

d. Click **OK** twice.

7. In the **Properties** dialog box, add yourself as a user for the queue.
8. Select **Allow** for **Full Control** for your user.
9. Repeat steps 4-8 for other affected queues as required.

Step 3: Enable the required endpoints for the recovery service:

1. Open Windows **Notepad** or an alternative text editor with administrator permissions.
2. Open the `C:\Program Files\Datamine\PA\Services\Audit Service\imsauditsvc.exe.config` file.
3. Ensure all recovery service endpoints under the **PoisonMessageRecoveryService** are commented out.

> **Important:** Only uncomment endpoints for a single source queue before running the recovery service. (Except for the system transaction dead-letter queue, where you can have an endpoint for each contract type.) You can then uncomment a different set of endpoints and re-run the recovery service if required.

4. Ensure all client endpoints between *<!--Start Recovery Clients-->* and *<!--End Recovery Clients-->* are commented out.
5. If there are dead-letter messages in **datamine.ims.log.servicedl**:

   a. Uncomment the following endpoint in the recovery service section.

```
<endpoint address="net.msmq://localhost/private/datamine.ims.log.servicedl"
contract="Mincom.IMS.Logging.Contracts.ILoggingService"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_Recovery" />
```

   b. Ensure the following endpoint remains uncommented in the client section.

```
<endpoint contract="Mincom.IMS.Logging.Contracts.ILoggingService"
address="net.msmq://localhost/private/datamine.ims.log.service"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_Log"/>
```

6. If there are dead-letter messages in **datamine.ims.audit.service.eventsdl**:
    a. Uncomment the following endpoint in the recovery service section.

```
<endpoint
address="net.msmq://localhost/private/datamine.ims.audit.service.eventsdl"
contract="Mincom.IMS.Audit.IAuditEventListener"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_Recovery"/>
```

    b. Uncomment the following endpoint in the client section.

```
<endpoint name="Audit Recovery"
address="net.msmq://localhost/private/datamine.ims.audit.service.events"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_AuditDataEvent"
contract="Mincom.IMS.Audit.IAuditEventListener"/>
```

7. If there are dead-letter messages in **datamine.ims.notification.service.eventsdl**:
    a. Uncomment the following endpoint in the recovery service section.

```
<endpoint
address
="net.msmq://localhost/private/datamine.ims.notification.service.eventsdl"
contract="Mincom.IMS.Audit.IAuditEventListener"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_Recovery" />
```

    b. Uncomment the following endpoint in the client section.

```
<endpoint name="Notification Manager Recovery"
address
="net.msmq://localhost/private/datamine.ims.notification.service.events"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_NMDataEvent"
contract="Mincom.IMS.Audit.IAuditEventListener"/>
```

8. If there are dead-letter messages in **datamine.ims.portal.eventsdl**:
    a. Uncomment the following endpoint in the recovery service section.

```
<endpoint address="net.msmq://localhost/private/datamine.ims.portal.eventsdl"
contract="Mincom.IMS.Audit.IAuditEventListener"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_Recovery"/>
```

    b. Uncomment the following endpoint in the client section.

```
<endpoint name="Portal Event Recovery"
address="net.msmq://localhost/private/datamine.ims.portal.events"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_PortalDataEvent"
contract="Mincom.IMS.Audit.IAuditEventListener"/>
```

9. If there are poison messages in **datamine.ims.log.service**:
    a. Uncomment the following endpoint in the recovery service section.

```
<endpoint
address="net.msmq://localhost/private/datamine.ims.log.service;poison"
contract="Mincom.IMS.Logging.Contracts.ILoggingService"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_Recovery_DL"/>
```

    b. Ensure the following endpoint remains uncommented in the client section.

```
<endpoint contract="Mincom.IMS.Logging.Contracts.ILoggingService"
address="net.msmq://localhost/private/datamine.ims.log.service"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_Log"/>
```

10. If there are poison messages in **datamine.ims.audit.service.events**:
    a. Uncomment the following endpoint in the recovery service section.

```
<endpoint
address
="net.msmq://localhost/private/datamine.ims.audit.service.events;poison"
contract="Mincom.IMS.Audit.IAuditEventListener"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_Recovery_DL"/>
```

    b. Uncomment the following endpoint in the client section.

```
<endpoint name="Audit Recovery"
address="net.msmq://localhost/private/datamine.ims.audit.service.events"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_AuditDataEvent"
contract="Mincom.IMS.Audit.IAuditEventListener"/>
```

11. If there are dead-letter messages in the system **Transactional dead-letter messages**:
    a. Uncomment the following two endpoints in the recovery service section.

```
<endpoint address="net.msmq://localhost/SYSTEM$;DEADXACT"
contract="Mincom.IMS.Audit.IAuditEventListener"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_Recovery_DL"/>
<endpoint address="net.msmq://localhost/SYSTEM$;DEADXACT"
contract="Mincom.IMS.Logging.Contracts.ILoggingService"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_Recovery_DL"/>
```

    b. Uncomment ONLY ONE of the following endpoints in the client section.

```
<endpoint name="Audit Recovery"
address="net.msmq://localhost/private/datamine.ims.audit.service.events"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_AuditDataEvent"
contract="Mincom.IMS.Audit.IAuditEventListener"/>
<endpoint name="Portal Event Recovery"
address="net.msmq://localhost/private/datamine.ims.portal.events"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_PortalDataEvent"
contract="Mincom.IMS.Audit.IAuditEventListener"/>
<endpoint name="Notification Manager Recovery"
address
="net.msmq://localhost/private/datamine.ims.notification.service.events"
```

```
binding="netMsmqBinding"
bindingConfiguration="MSMQ_NMDataEvent"
contract="Mincom.IMS.Audit.IAuditEventListener"/>
```

c. Ensure the following endpoint remains uncommented in the client section.

```
<endpoint contract="Mincom.IMS.Logging.Contracts.ILoggingService"
address="net.msmq://localhost/private/datamine.ims.log.service"
binding="netMsmqBinding"
bindingConfiguration="MSMQ_Log"/>
```

12. Save and close the `imsauditsvc.exe.config` file.

Step 4: Run the recovery service:

1. Open Windows **Command Prompt** with administrator permissions.
2. Change directory to the file location of the Audit Service.

```
cd "C:\Program Files\Datamine\PA\Services\Audit Service\"
```

3. To run the recovery service and log the recovery to text files in the same file location as the Audit Service, run the following command. The **Command Prompt** window also displays a log of the processed messages.

```
imsauditsvc.exe -recover
```

4. To run the recovery service without logging to text files, run the following command. The **Command Prompt** window displays a log of the processed messages.

```
imsauditsvc.exe -recover false
```

5. To stop the recovery service, press **Enter** or **Ctrl + C**.

DATAMINE

PRODUCTION ACCOUNTING

Datamine enables efficient and sustainable mining through the application of world-leading technology and services.

Read the Docs

docs.dataminesoftware.com

Get in Touch

www.dataminesoftware.com/contact

www.dataminesoftware.com/support