Sage Employee Self Service

Installation and Setup Guide

Contents

Contents

Introduction

Read all chapters in this guide before you install Sage Employee Self Service. This document includes instructions for installing and setting up Sage Employee Self Service for the first time and upgrading Sage Employee Self Service from prior versions.

> **Note:** Before installing, consult with your business partner or Sage to ensure that this program is compatible with customizations, integrated third-party applications, and other configuration options. If you install this program independently, you assume responsibility for any impact on your system.

Support and resources

Sage strives to provide you with the best help and support in the industry. If you have a question, we're here to help!

- **Online Help:** Click or press **F1** within in the product to open the online help for the window you are viewing. From within the help, you can click the **Contents** tab (on the left side of the window) to explore a variety of topics, click the **Index** tab to look for topics related to a particular keyword, or use the search box (in the upper right corner of the window) by typing a particular word or phrase and clicking to search for topics containing that text.

- **Product Documents:** Access this and other documents from the Sage HRMS Product Documents website.

- **Community Hub:** Visit the online community at https://communityhub.sage.com/us/sage_hrms/ for blogs, tips, and guidance for your Sage programs.

- **Sage Knowledgebase:** Search the Sage Knowledgebase, which provides 24/7 access to support articles as well as the latest software downloads and updates.

- **Customer Support:** For other support resources, visit the Sage Support Resource Centre page, select your country, and then select your product.

- **Sage University:** Learn pro tips for year-end processing in online or classroom courses. Visit http://SageU.com and log on or create an account to register for training.
- **Tax forms:** Because all printed forms have variations, Sage HRMS Payroll only supports forms printed by Sage Checks and Forms. Call Sage Checks and Forms at 800-617-3224 or order online at www.SageChecks.com.

System requirements

See Sage Knowledgebase article 225924250083549 for the hardware and software recommendations for Sage HRMS and Sage Employee Self Service.

Before you start

Make sure you have the following items before you install or upgrade:

- The *Sage Employee Self Service Installation and Setup Guide* (this document).

- The appropriate Sage Employee Self Service installation package from the Sage Knowledgebase. Follow the steps below to download the product install.

1. Visit the Sage Knowledgebase at https://support.na.sage.com.
2. Log in if required.
3. Search for the Sage Knowledgebase article 230614202903173.
4. In the article, locate and select the appropriate download link:
   a. For the premium web version of Sage Employee Self Service, look under the **Sage HRMS Premium Web Version with ESS Quarterly Update** section.
   b. For the non-premium (existing) version of Sage Employee Self Service, look under the **Sage HRMS ESS Quarterly Update Non-Premium (Existing)** section.
5. Click the **direct download** link to download the product update.

In addition to reading this document, review the Sage HRMS and Sage Employee Self Service release notes if you are upgrading from a prior version.

> **Note:** You can find the latest documentation on the Sage HRMS Product Documents website. This website is also linked from the Help menu in Sage HRMS.

Chapter 1: Pre-installation setup

This chapter helps you prepare your system before installing Sage Employee Self Service (Sage ESS). It includes the following topics:

- Microsoft Windows Server and SQL Server compatibility and configuration
- Firewall and network configuration
- Security configuration and best practices

About Microsoft Windows Server compatibility

Microsoft database management resources

Information concerning Microsoft SQL Server security, stability, and scalability is available on the Microsoft SQL Server website: http://www.microsoft.com/sql/techinfo/default.mspx

Client requirements for web access to Sage Employee Self Service

Your system must meet the minimum requirements for the latest versions of Microsoft® Edge, Chrome and Firefox.

Setting up employee analytics with Microsoft Windows Server

You can use the Employee Analytics feature in Sage ESS to share workforce data with other employees in your company. Using View Builder, a highly versatile and customizable analytical tool, you can implement Employee Analytics in your company. View Builder is used for creating a view (similar to a template) that both generates data and displays the output in a web browser.

Follow these steps if you install Sage Employee Self Service on a server running Windows Server and you plan to use View Builder.

> **Note:** At the end of these steps, you must restart the server. Before you begin, prepare for this.

1. On the server, select **Start > Administrative Tools > Server Manager**.

2. In the **Server Manager** window, click the **Roles** node in the left pane.

3. Click **Add Roles Services**.

4. In the **Add Role Services** window, select **Application Development** and then click **Install**.

5. Scroll down the list of Role services and select **Security** and also select **IIS Management Compatibility**.

6. Click **Next**, and then click **Install** to install the selected components.

7. After the install is complete, click the **Features** node, and then click **Add Features**.

8. In the **Add Features Wizard**, select **SMTP Server**. If necessary, click **Install** to also install the Web Server (IIS) service.

9. Click **Next**, and then click **Install** to install the selected features.

10. Restart the server.

> **Note:** Microsoft has deprecated the built-in SMTP Server in Windows Server 2025. If you are installing Sage Employee Self Service on a windows server version prior to 2025, you can continue to use the built-in SMTP Server. When installing Sage Employee Self Service on a Windows Server 2025, you must use a third-party SMTP service.

Configuring firewall and security services

Sage HRMS clients and the Sage Employee Self Service server require the firewall considerations listed in this section.

> **Tip:** For guidance to configure your Windows Firewall to allow SQL Server access, go to the Microsoft knowledgebase or technical documentation website. See the Microsoft article titled Configure the Windows Firewall to Allow SQL Server Access for useful information.

Incoming connections

The following ports must be open for incoming connections to the Sage ESS server:

- **www-http: 80/TCP**. This is needed only when non-secure (http) access to the server is allowed.
- **https: 443/TCP**. This is needed only if you want https access to the server and it is configured.

Outgoing connections

The following ports must be open for Sage HRMS clients to connect to Sage Employee Self Service:

- **www-http: 80/TCP**. This is needed only when non-secure (http) access to the server is allowed.
- **https: 443/TCP**. This is needed only if you want https access to the server and it is configured.

When Sage Employee Self Service is configured to connect to a non-local SQL Server, incoming and outgoing traffic for the following port is required:

- **mssql ms-sql: 1433/TCP**

To resolve IP addresses via DNS (depending on your server configuration), the following ports need to be open:

- domain:53/TCP
- domain:53/UDP

To send email from the local SMTP service, the following port must be available if outgoing connections are configured to send or forward from the Sage Employee Self Service server:

- smtp:25/TCP

Network security configurations

The following figures show common configurations that are used when implementing Sage Employee Self Service. These are guidelines only and can be modified for your environment.

Basic network security – IIS behind Firewall
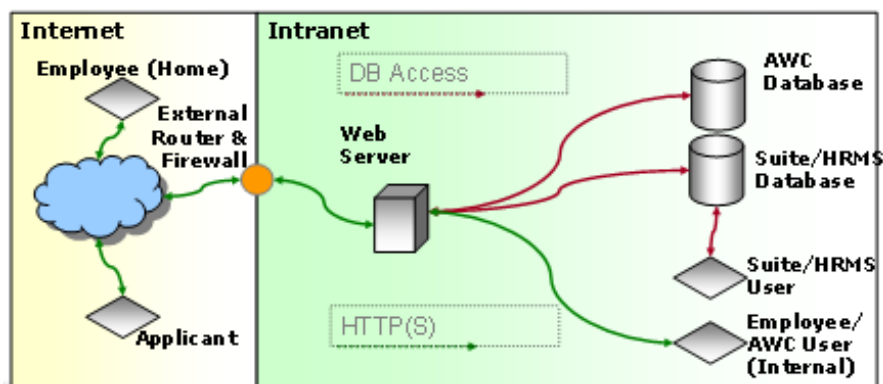
Advanced network security – IIS and two Demilitarized Zones (DMZs)
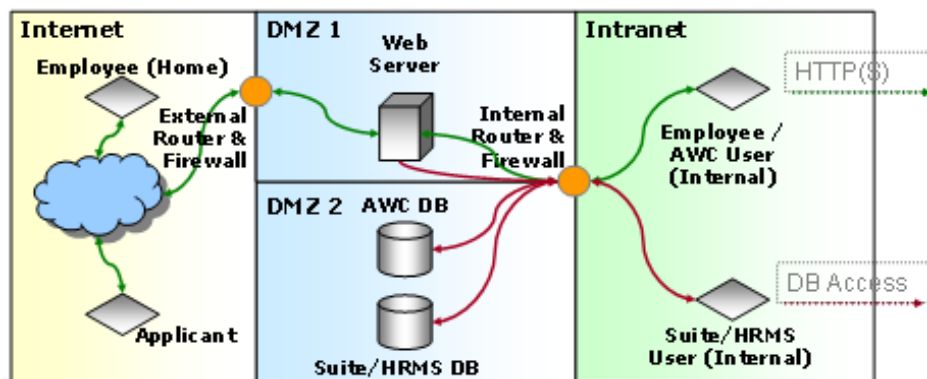
Enhanced network security – IIS in Demilitarized Zone (DMZ)
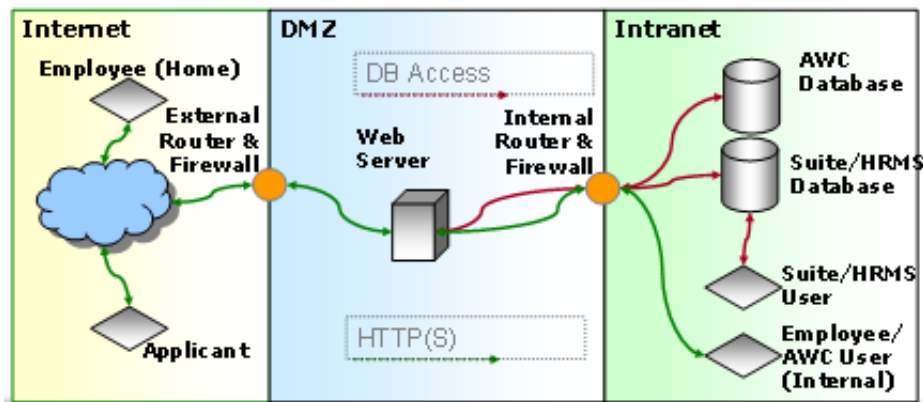
Sage ESS Data Execution Prevention (DEP) settings

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running on a system. If you are running Sage Employee Self Service on a supported Windows Server, you must verify the DEP settings are correct.

> **Tip:** See Microsoft Knowledgebase DEP article for more information on DEP.

To verify the DEP settings, have your company's IT department perform the following steps on the Sage Employee Self Service server. We recommend that they perform the steps with the assistance of a certified business partner or the Sage Professional Services Group.

> **Note:** At the end of these steps, you must reboot the server. Before you begin, prepare for this.

1. To verify the operating system is a supported Windows Server:
    a. Click **Start > Run**,
    b. Type `winver`, and then press **Enter**.
2. To verify that the processor supports hardware DEP:
    a. Go to **Control Panel > System > Advanced**.
    b. Click **Settings** (in the **Performance** section).
    c. Click the **Data Execution Prevention** tab.

      d. Verify that you do not see the following message at the bottom of the tab: "Your computer's processor does not support hardware-based DEP. However, . . ."

3. If you do not see the message but Sage ESS is generating error 80010105, switch some DEP settings:

      a. Go to **Control Panel > System > Advanced**.

      b. Click **Settings** (in the **Performance** section).

      c. Click the **Data Execution Prevention** tab.

      d. Select **Turn on DEP** for essential Windows programs and services only.

      e. Click **OK** to save and close all windows.

4. Reboot the server.

Security recommendations and best practices

The recommendations depend on how your company and employees will use Sage Employee Self Service.

Recommendations for public access workstations

Sage Employee Self Service allows employees to access their personal, payroll, and benefit information via the Internet or an intranet.

When you connect to a network and communicate with others, you are taking a risk. Internet security involves the protection of a computer's internet account and files from intrusion of an unknown user. Some people will strive to find new ways to circumvent IT security, so your company will need to be continually vigilant.

This section provides some recommendations for keeping your system and network secure. However, we highly recommend that you contact an Information Security expert to determine the best way for your company to keep your information secure.

Software application best practices

- Install and maintain up to date and properly configured anti-virus software. Be sure that real-time protection scans all files.

- Install active spy-ware defenses (such as Windows Defender).

- Install only the minimum number of applications needed.

- Update web plug-ins, Java scripts, and media players on a regular basis as these are areas of increasing vulnerability.

- Periodically check the website of the Operating System vendor (such as Microsoft) for critical security updates.

- Consider using multiple web browsers for different software applications. Currently, Sage ESS operates with Edge, the latest version of Google Chrome, and the latest version of Mozilla Firefox.

- Disable other unnecessary network services.

- Disable http server response headers.

> **Note:** You may also want to customize certain error messages to provide information specific to your company. For example, the **HTTP Error 404.0** message could be customized to "Contact your administrator at ###-###-#### if you see this error."

Data security best practices

- Keep backup copies of important documents on a secure server and not a shared workstation.

- Use certificates, especially if you modify a DNS server (or write a Java-based SSL proxy) to point your web or XML client to another website.

- Configure the Sage Employee Self Service web server for HTTPS/SSL using a valid site certificate and do not allow access from public workstations or computers on the Internet.

- Enable or disable functionality as required to secure your web browser.

  - Because some software features (such as ActiveX, Java, JavaScript, VBScript) that provide functionality to the web browser can also introduce vulnerabilities to the computer system, you must understand which browsers support those features and the subsequent risks they could introduce.

- If you are not sure how to define the security settings, consult an Information Security expert.

- Disable broadcast services.

- Disable the cache on the local system and always store confidential data securely (in transit and at rest).

- Clear temporary files regularly, set your web browsers to store 0-day history, and to clear the cache upon exit.

- Prevent web browsers from caching passwords and auto-filling data.

- Require users to change their password regularly and require a strong password.

- Never allow Windows to remember your passwords.

- Lock the BIOS to prevent USB, or Network booting and use a strong BIOS password.

- Perform a port scan or network statistics on the kiosk operating system to determine active TCP connections. Block everything except the ports you need.

- Institute strong group policies. This is a good way to prevent security issues.

- Stress the importance of logging off and closing all applications with your employees and users. Do not open attachments unless you know the sender and know that it was intentionally sent to you. Do not click links without considering the risks first.

- Consult your Information Security expert to determine the best approach to regularly maintain security of your system without inconveniencing your employees.

Next steps:

See for information about configuring your system before installing Sage Employee Self Service.

Chapter 2: System Configuration

This chapter provides instructions for configuring Internet Information Services (IIS) for Windows Server 2016 and higher (including .NET) as well as SMTP in preparation for installing Sage Employee Self Service.

> **Note:** Microsoft has deprecated the built-in SMTP Server in Windows Server 2025. If you are installing Sage Employee Self Service on a windows server version prior to 2025, you can continue to use the built-in SMTP Server. When installing Sage Employee Self Service on a Windows Server 2025, you must use a third-party SMTP service.

Before you start

- You must have the appropriate downloads or disks necessary for installing Microsoft Windows Server 2016 or higher (Standard, Express, or Enterprise Editions).

- You must have already created an administrative user account to work from on your Microsoft Windows Server.

- You must have added the server to your domain or workgroup (depending on your organization requirements).

> **Important!** The following sections describe how to configure the built-in SMTP Server to send emails from Sage Employee Self Service when ESS is installed on a Windows Server that supports the built-in SMTP Server.

Configuring the Mail Server

The next server role that needs to be added is the Mail Server (SMTP, POP3) role.

1. From the Start Menu, select **All Programs > Administrative Tools > Manage Your Server** and select **Add or remove a role**.

2. On the **Preliminary Steps** window, verify that you have completed the tasks, and then click **Next**.

3. On the **Server Role** window, select **Mail server (POP3, SMTP)**, and then click **Next**.

4. Proceed with configuring the mail server in accordance with your company's network environment.

> **Note:** Proper SMTP configuration requires knowledge about networking, protocols, authentication methods, firewalls, and configuration of the specific receiving mail servers. We recommend you consult with your IT department or your ISP for the correct settings for your company's specific messaging requirements.

Next steps:

If you plan to use SQL Server 2019 or higher for the Sage Employee Self Service database, install SQL Server.

Troubleshooting email delivery issues

If emails are not being delivered from Sage ESS, check the following items:

1. Check that there are no firewalls or other hardware and software installed that could be blocking the ports needed for mail delivery. Port 25 should be made available for delivery when using Sage ESS.

2. Go to the root of the **C drive** on the web server where Sage ESS is installed and locate the **Inetpub** directory.

3. Expand the folder and browse to find the **Queue** folder. If there are emails collecting there, they are not being delivered, and you must check relay permissions in Properties for the Default SMTP Virtual Server.

4. Right-click the **Default SMTP Virtual Server** in the IIS console.

5. Select **Properties**, select the **Access** tab, and then click the **Relay** button.

6. Ensure that there is a path directed to the Exchange Server so that mail can be delivered. To test this:

a. Copy one of the queued messages and paste it in the Pickup folder.

b. If it returns to the Queue folder, a Smart Host is not assigned in the Default SMTP Virtual Server properties. The Smart Host will be the name of the server that is used as the Exchange server and/or Mail server.

c. To locate this setting, right-click on the **Default SMTP Virtual Server** in the IIS console, and select **Properties**.

d. Select the **Delivery** tab and click on the **Advanced** tab.

e. Enter the name of the correct server in the **Smart Host** field.

> **Note:** When using Microsoft Exchange for email, a connector is needed to accept the email from the Default SMTP virtual server.

7. From the IIS console manager, right-click the **Default SMTP Virtual Server** and stop the process.

8. Restart the Default SMTP Virtual Server and the email messages should be delivered.

Modifying relay permissions in IIS

To modify the relay permissions in IIS for the Virtual SMTP server to allow the service to run properly with Sage ESS.

1. Select **Start > Run**, enter MMC, and click **OK**.

2. In the Microsoft Management Console (MMC), select **File > Internet Information Services**.

3. Expand IIS and select the computer on which Sage ESS is installed.

4. Expand the section, right-click **Default SMTP Virtual Server**, and select **Properties**.

5. Select the **Access** tab, and then click the **Relay** button.

6. In the **Relay Restriction** window, select the **All but the list below** button (by default, it is set not to allow the relay of email).

7. Right-click the **Default SMTP Virtual Server** and stop the service.

8. Restart the service.

9. Enter the SMTP server name on the System Maintenance utility and click **Save**.

Windows Server Configuration

For this configuration, set up the application and web services roles and then add the SMTP Server mail feature ("To add the SMTP Server mail feature:" (page 15)).

To set up the Application and Web Services roles:

1. Log in to Microsoft Windows Server using your Administrator credentials.

2. Select the **Server Manager** from your programs.

3. From the Server Manager Dashboard, select **Dashboard > Add roles and features** to access the Add Roles and Features Wizard.

4. On the Select destination server page, select the server on which you want to install the roles and features and click Next.

5. In the **Server Roles** window, expand **Web Server (IIS)** and then the **Web Server** node.

6. Expand **Application Development (Installed)** as shown in the following image.
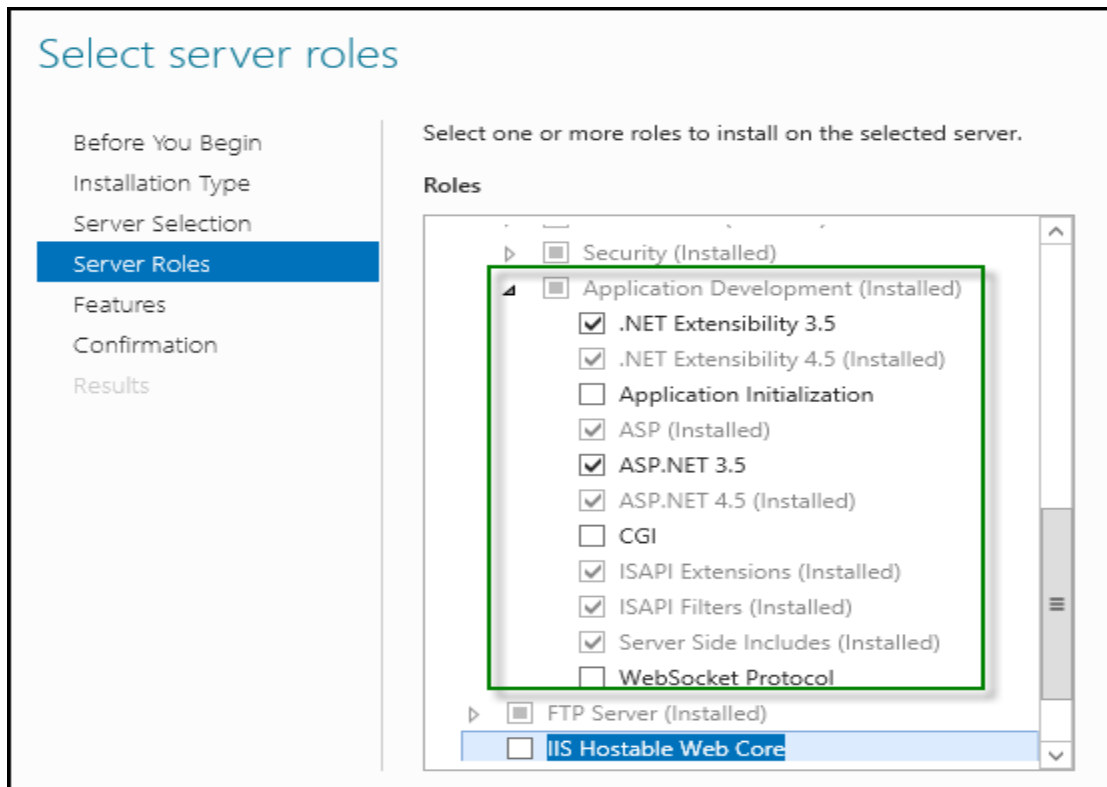
7. Select the roles below and click **Next**.

- **.NET Extensibility 3.5**.
- **.NET Extensibility 4.7**.
- **ASP**.
- **ASP .NET 3.5**.
- **ASP .NET 4.7**.
- **.NET Extensibility 4.7**.

8. In the **Select Server Roles** page, click **Next**.

9. In the **Features** window, select the Features below:

   - **.NET Framework 3.5 Features**.
   - **.NET Framework 4.7 Features**.

10. Click **Next**.

11. In the **Confirm Installation Selections** window, click **Install**.

12. After the installation is complete, click **Close**.

To add the SMTP Server mail feature:

1. Log in to Windows Server with the server roles that you set up in the previous section.

2. Select **Start > Administrator Tools > Server Manager**.

3. From the Server Manager tree in the **Server Manager** window, select **Features** to access the Add Roles and Features Wizard.

4. Select the **SMTP Server** check box.

5. Click the **Add Required Role Services** button.

6. Click **Next**.

7. In the **Web Server (IIS)** window, click **Next**.

   The **Add Roles and Features Wizard** window opens. (This window can be accessed by selecting **Web Server (IIS) > Server Roles**.)

> **Note:** The installer will accept the items that are checked by default in the **Add Roles and Features Wizard**.

8. Click **Next**.

9. In the **Confirm Installation Selections** window, click **Install**.

10. After the installation is complete, click **Close** to close the wizard.

11. Restart your server.

> **Note:** The premium version of Sage Employee Self Service requires that the .NET Framework Version be set to v4.0 for the **AbraAWCAppPool**.

Next steps:

See for information about installing or upgrading Sage Employee Self Service.

Chapter 3: Installing Sage Employee Self Service

This chapter provides instructions to install or upgrade Sage Employee Self Service (Sage ESS). However, there are things you must do before you install.

Before you start

- You must install the desktop version of Sage HRMS before you can install Sage Employee Self Service. Refer to the *Sage HRMS Installation Guide* on the Product Documents website for instructions.

- If you are loading Sage Employee Self Service from a network drive, we recommend that you copy the files to a local drive or that you initialize the network connection during startup.

- Do not install Sage Employee Self Service on a Windows Server that is an Active Directory or Domain Controller. Microsoft does not recommend this, and Sage does not support this configuration.

- Using your external backup procedures, perform a backup of your Sage HRMS system. Make sure everyone has exited Sage HRMS before beginning the backup and installation.

- You must have Administrator access (Local Administrator access is preferred) and access to Sage HRMS data to perform the Sage Employee Self Service installation.

- Your Sage HRMS database must be accessible through a local or UNC path (Windows share) from your Sage Employee Self Service server.

- System Administrator privileges are required if you are installing Sage Employee Self Service on Windows Server.

- When you enter text in fields on the installation windows (such as the company name or server name), the text must contain only alpha or numeric characters (alphabetic characters a-z, A-Z, and numeric characters 0-9). You cannot use special characters (such as #, -, @ or punctuation marks).

Sage Employee Self Service and Microsoft

SharePoint Services 2.0

Although Sage Employee Self Service can be used on the same server as Microsoft Windows SharePoint Services 2.0, Sage does not recommend this and cannot assist you with issues that may result from this type of installation.

If you use this type of installation, note that Sage Employee Self Service uses the default website. Thus, you must install SharePoint Services 2.0 *on a site other than the default website* to prevent conflicts. If SharePoint Services uses the default website, it prevents access to the installed version of Sage Employee Self Service. To troubleshoot Windows SharePoint Services 2.0 installation issues, visit: http://msdn.microsoft.com/en-us/library/cc288422(office.12).aspx.

Installing Sage Employee Self Service

If you are installing Sage Employee Self Service on a new server, follow these instructions and cautions. Due to the complexity of Sage Employee Self Service, we recommend that you consult a certified business partner or member of Sage Professional Services Group to perform the process.

To install Sage Employee Self Service:

1. Open the Sage Employee Self Service installation package. Right-click the **setup.exe** file, select **Run as Administrator**, and then click **Next**.

   > Note: The setup.exe is the generic term for the install exe file. The name of the install file is dependent upon the version of Sage ESS you have. Review the most recent version of the Sage HRMS and Sage Employee Self Service release notes for the correct version of the file.

2. In the **License Agreement** window, read the License Agreement, accept the terms of the license agreement, and click **Next**.

3. In the **Customer Information** window, enter your **Name**, **Organization**, **Serial Number**, and **Install Code**, and then click **Next**.

4. In the **Destination Folder** window, select the path and directory where you want Sage Employee Self Service and its components installed. This must be a local drive. The server can be the same as the Sage HRMS server, but this is not a requirement. Click **Next**.

5. In the **Sage HRMS SQL Server Setup** window, specify the server configuration for the Sage HRMS database. Enter the **Server Name**, **Username**, **Password**, and **Database**. Click **Next**.

6. In the **Sage Employee Self Service Web Alias** window, the **Name/Alias** is initially set to "selfservice," but you can change it. The **Name/Alias** is used to access Sage Employee Self Service from a web browser. Click **Next**.

7. In the **Email Configuration** window, select **Enable Emails (SMTP)** if you are installing Sage Employee Self Service on a Windows Server version prior to 2025 and want to use the built-in SMTP Server. Otherwise, you do not need to select the **Enable Emails (SMTP)** checkbox.

8. Click **Next**.

> **Note:** If you do not want Sage ESS to send emails automatically, you can disable this setting in the System Maintenance utility later. If you choose to maintain this setting, you must configure your SMTP server before you can enable email delivery.

9. In the **SQL Server Setup** window, specify your version of SQL Server (the default database embedded with Sage Employee Self Service). Enter the **Server Name**, **Username**, **Password**, and **Database**. You must provide a SQL Server logon that uses or emulates your SA (System Administrator) permissions. Click **Next**.

10. In the **Ready to Install the Program** window, click **Install** to proceed with the installation.

11. When the **InstallShield Wizard Completed** window appears, click **Finish**.

12. When the installation is complete, click **Yes** to restart your computer.

13. After your Sage Employee Self Service server restarts, from your Start menu, select **All Programs > Sage Employee Self Service > System Maintenance** to open the System Maintenance utility.

14. Review the information on the **Configuration and Settings** tab, and then click **Save**.

15. Click the **SQL Maintenance** tab, and then verify or enter the location and name of your Sage Employee Self Service database backup file.

16. Click **Backup** and confirm the action to start the process.

An indicator shows the process as it runs, and a message confirms when it is finished.

17. Select the **Duplicate Key Report** tab and click **Run Report**.

This verifies that you can access the Sage HRMS data location and that the user account to access Sage HRMS data is correct. If there are errors in the database, give the report to the person responsible for maintaining the data so they can fix the errors. For information on running the **Duplicate Key** report, see the "Duplicate Key Report tab" (page 46).

18. **Close** the System Maintenance utility.

19. If you installed Sage Employee Self Service on a Windows 64-bit server, set the Application Pool Identity to use an administrator account when running Sage Employee Self Service in order to avoid an "Access to the temp directory is denied…" error message.

    a. On the Sage Employee Self Service server, select **Start > Administrative Tools > IIS Manager**.

    b. In **Connections**, select **<servername>Application Pools**.

    c. In **Application Pools**, select **AbraAWCAppPool**.

    d. In **Actions**, select **Edit Application Pool > Advanced Settings…**.

    e. In **Advanced Settings**, select **Process Model > Identity**.

    f. In the **Application Pool Identity** window, select **Custom account** and set it to **<servername>\<user>**, where **<user>** is a user with an administrator account.

20. Launch Microsoft Edge on any client workstation connected to the server (but not the server itself), and then enter the following URL for **Address**:
`http://<YourServer>/<ConfiguredVirtualDirectoryName>`

For example: `http://localhost/selfservice`

If you already have a domain name for external access and intend to use https, enter:
`https://<Server.Domain.TopLevelDomain>/<ConfiguredVirtualDirectoryName>`

> **Notes:**
> - The **<ConfiguredVirtualDirectoryName>** is the **Name/Alias** you entered in step 6 above.
> - You must enter the URL exactly as the Sage HRMS client calls it, because this is what is stored in Sage HRMS to allow access to Sage Employee Self Service. The system stores the Sage Employee Self Service URL in the SYENTER system table as **E_AWCURL**.

21. In the Sage Employee Self Service logon page, **you must complete the following setup steps immediately after you install or upgrade Sage ESS**.

    a. Log on as the Master user and use the password provided in the installed System Maintenance utility

> **Tip:** In the System Maintenance utility on the **Configuration and Settings** tab, click **Generate Master Password** and copy the password provided to log into Sage ESS as the Master user.

    b. Select **System Administrator > Roles and Logon > Logon Setup**.

    c. At the bottom of the **Logon Setup** page, select five security questions to present to a user when they attempt to create a new logon.

> **Note:** When an employee creates a new logon, they must select one of the five security questions and provide a security answer. The question is then presented whenever the employee attempts to change or reset their password. If the answer does not match the answer they created, they are returned to the **Employee Logon** page with a message that the Logon information could not be verified.

    d. Click **Save** to save the security questions.

Installation is now complete. You are ready to start using Sage Employee Self Service.

> **Important!** After performing a new install or upgrade of Sage Employee Self Service, it is important to **Save** the **Configuration and Settings** tab in the System Maintenance utility.

1. Log on to the Sage ESS server and select Programs > Sage Employee Self Service >System Maintenance.

2. On the **Configuration and Settings** tab click **Save**.

   This step will ensure that the **AbraAWCAppPool** is running under the Integrated Managed Pipeline mode in IIS.

Next steps:

See "Setting up Sage Employee Self Service" (page 26) for information about setting up Sage Employee Self Service.

Upgrading Sage Employee Self Service

Before you start

- Take a screenshot of your **System Maintenance > Configuration and Settings** window prior to beginning this process. You may be prompted to enter the information on this window during the upgrade.

- Verify that Sage HRMS has been installed and is working correctly.

- Verify that you have Administrator access (Local Administrator access is preferred) and permissions to log on as a service, launch processes, and access the Sage HRMS data.

- If you are using Benefits Enrollment/Open Enrollment, make sure all enrollment periods are closed.

- Make sure that all users have exited and logged off from Sage HRMS and Sage Employee Self Service before beginning the backup and upgrade.

- When the upgrade is complete, you must restart your computer. Make the necessary preparations for this required restart.

To upgrade Sage Employee Self Service:

1. Using your external backup procedures, perform a backup of the Sage HRMS and Sage ESS databases to a media device that is external to your Sage HRMS and Sage ESS servers.

2. Log on to the Sage ESS server and select **Programs > Sage Employee Self Service > System Maintenance**.

3. In the Sage ESS System Maintenance utility on the **Configuration and Settings** tab, select the **Locked** check box in the **Sage Employee Self Service** section.

4. Click **Save**.

5. Go to the **SQL Maintenance** tab, verify the **Backup File Path** is correct, click **Backup**, and confirm the action to start the process.

6. Close all Windows applications that are running.

7. Open the Sage Employee Self Service installation package. Right-click the **setup.exe** file, select **Run as Administrator**, and then click **Next**.

8. Select **Sage Employee Self Service**, and then select **Install Sage Employee Self Service**.

9. The installation program detects that a previous version of Sage Employee Self Service was installed. Click **Next**.

10. In the **Sage HRMS Database Type** window, select the SQL Server database type and click **Next**.

11. In the **Sage HRMS SQL Server Setup** window, enter the **Server Name**, **Username**, **Password**, and **Database**. If you are using a SQL database, you must provide a SQL Server logon that has SA (System Administrator) permissions. Click **Next**.

12. In the **Ready to Install the Program** window, click **Install** to proceed with the installation.

13. When the **InstallShield Wizard Completed** window appears, click **Finish**.

14. When the upgrade is complete, click **Yes** to restart your computer.

15. After your Sage Employee Self Service server restarts, from your Start menu, select **All Programs > Sage Employee Self Service > System Maintenance** to open the System Maintenance utility.

16. Click the **SQL Maintenance** tab, and then verify or enter the location and name of your Sage Employee Self Service database backup file.

17. Click **Backup** and confirm the action to start the process.

   An indicator shows the process as it runs, and a message confirms when it is finished.

18. Select the **Configuration and Settings** tab, and then click **Save**.

19. Exit System Maintenance.

20. In the Sage Employee Self Service logon page, **you must complete the following setup steps immediately after you install or upgrade Sage ESS**.

   a. Log on as the Master user and use the password provided in the installed System Maintenance utility

   > **Tip:** In the System Maintenance utility on the **Configuration and Settings** tab, click **Generate Master Password** and copy the password provided to log into Sage ESS as the Master user.

   b. Select **System Administrator > Roles and Logon > Logon Setup**.

   c. At the bottom of the **Logon Setup** page, select five security questions to present to a user when they attempt to create a new logon.

   > **Note:** When an employee creates a new logon, they must select one of the five security questions and provide a security answer. The question is then presented whenever the employee attempts to change or reset their password. If the answer does not match the answer they created, they are returned to the **Employee Logon** page with a message that the Logon information could not be verified.

   d. Click **Save** to save the security questions.

21. When the backup is finished, go to the **Configuration and Settings** tab and clear the **Locked** check box.

The upgrade is now complete. You are ready to start using Sage Employee Self Service.

> **Important!** After performing a new install or upgrade of Sage Employee Self Service, it is important to **Save** the **Configuration and Settings** tab in the System Maintenance utility.
>
> 1. Log on to the Sage ESS server and select Programs > Sage Employee Self Service >System Maintenance.
>
> 2. On the **Configuration and Settings** tab click **Save**.
>
> This step will ensure that the **AbraAWCAppPool** is running under the Integrated Managed Pipeline mode in IIS.

Note: See "Setting up Sage Employee Self Service" (page 26) if you need to make any changes to Sage Employee Self Service setup.

Chapter 4: Setting up Sage Employee Self Service

This chapter provides instructions to set up Sage HRMS to work with Sage Employee Self Service. The extent of your setup depends on the modules you are using in Sage HRMS, the modules you installed for Sage Employee Self Service (such as Benefits Enrollment), and the way you will use these modules. Review each step in its entirety to determine if it applies to your usage requirements.

When you finish these steps, employees and administrators can create their logons and use Sage Employee Self Service as needed.

> **Tip:** When your company is ready to set up Sage Employee Self Service for benefits enrollment or life events, refer to the *Sage Employee Self Service Benefits Planning Guide* on the [Product Documents website](#).

Setting up Sage HRMS for Sage Employee Self Service

Use the following instructions to prepare Sage HRMS for integration with Sage ESS.

Assigning supervisors

In Sage HRMS, you can assign a Supervisor as well as a Manger to an employee. In Sage Employee Self Service, the supervisor is responsible for overseeing the day-to-day tasks performed by an individual employee. While they lack the level of authority of a manager, they have an oversight responsibility for the employees with whom they work. For example, a supervisor might be responsible for tracking and approving employee time off requests.

If you want to use the Supervisor role in Sage Employee Self Service, you must assign a Supervisor for each employee.

1. Log in to Sage HRMS.

2. Select **Employees > View/Edit Employee** and select an employee.

3. For that employee, select **Job and Pay**, select the **Current Job** tab, and then the **Organization** subtab.

4. For **Supervisor**, click the **Find** button, select the employee to assign as the employee's supervisor, and then click **OK**.

5. Repeat steps 2-4 for all employees who should have supervisors assigned.

6. Save your changes.

Updating email addresses

Sage Employee Self Service can send emails and post notifications to employees, managers, supervisors, administrators, recruiters, and hiring managers when an action was taken (such as request for approval, benefit update, time off request, or interview invitation). If you set up the system to send emails, verify that email addresses have been entered for your Sage HRMS employees.

> You can use the Update E-mail Addresses process to verify that all your employees have email addresses. For detailed instructions:
>
> 1. In Sage HRMS, select **Employees > Processes > Update E-mail Addresses**.
>
> 2. Click and follow the instructions in the "Update E-mail Addresses" topic.

Reviewing attendance plan setup

Sage Employee Self Service can be configured to allow employees to submit time off requests. When they are approved, they are transmitted to the employee's Sage HRMS attendance plans. In order for this Time Off Request function to work correctly, verify that each attendance plan was set up with unique absence reason codes. You cannot have more than one plan with the same absence reason codes.

Setting up single sign-on access for HRMS users

Sage HRMS includes a feature that enables an HRMS user with single sign-on access to log into an employee's account and view exactly what the employee sees without requiring access

to the employee's personal password.

To set up a user with single sign-on access from Sage HRMS:

1. From your Windows Programs menu, open Sage ESS **System Maintenance** (IIS application server).

2. Select the **Keys** tab.

3. If no existing keys exist, click the **Generate Keys** button.

> **Note:** You do not need to save or copy the key–Sage ESS will send it to the Sage HRMS system for you.

4. Log in to Sage HRMS with Master access.

5. From the HRMS navigation pane, select **Setup > System > User Security**.

6. Select the user who will have single sign-on access to employees' ESS accounts.

7. For **Allow Single Sign-on to ESS**, select **Yes**.

8. Finally, ask that user to log in to Sage ESS from Sage HRMS with their own login–in Sage HRMS, select **Connected Services > Employee Self Service > System Login**.

To use single sign-on:

1. As the user with single sign-on access, in Sage HRMS, select **Employees > View/Edit Employee**.

2. Select the employee whose Sage Employee Self Service account you want to view.

3. Click the **Self Service** link under the employee's name.

   This launches an Internet browser with the Sage Employee Self Service account for that specific employee.

Setting up Sage Employee Self Service

Each Sage Employee Self Service page available to the employee and manager can be tailored to meet the needs of each employer or for the entire enterprise. When you define page settings, you build the automated process that passes information and tasks from one person to another for action. Actions can include viewing a page, viewing a change, adding

information to a page, receiving a notification of a change or addition, and approving or rejecting a change or addition.

Before you define the settings, decide whether the settings should apply to:

- A specific employer
- The entire enterprise–all employers in your Sage Employee Self Service system

Defining page settings

Use the **Page Setup** tab on the **Employer Setup** page to define the following information for pages in Sage ESS:

- **Access**. Determines whether the page can be updated, whether updates need approval, and whether notifications need to be sent to specific administrators.
- **Approval**. If updates to the page need approval, the person assigned to the approval role must approve the updates before the data is saved to Sage HRMS.
- **Notify**. When employees update the page, the person assigned to the notify role is notified of the update. You can select one or two notify roles.

You can set this information for a specific employer or for the enterprise.

> For detailed instructions:
>
> 1. In Sage Employee Self Service, log on as the Master User.
>
> 2. On the **System Admin** menu, select **System Settings > Employer Setup**, select the employer, and click the **Page Setup** tab.
>
> 3. Click ❓ > **Help** and follow the instructions in the "Page Setup" topic.

Defining settings for display, Message Center, and email

Use the **Settings** tab on the **Employer Setup** page to:

- Specify how or whether certain items can be viewed, including the employer benefits contribution, salary grade and step rates (**Minimum/Maximum/Midpoint**), and bank account number.

- Specify email settings and set up reminders that are posted to the Message Center when an employee's performance review, birthday, or employment anniversary is upcoming.

You can set this information for a specific employer or for the enterprise.

> For detailed instructions:
>
> 1. In Sage Employee Self Service, log on as the Master User.
>
> 2. On the **System Admin** menu, select **System Settings > Employer Setup**, select the employer, and click the **Settings** tab.
>
> 3. Click ❓ > **Help** and follow the instructions in the "Employer Setup - Settings" topic.

Defining custom content

Use the **Custom Content** tab on the **Employer Setup** page to add custom content to pages. You can add text references, file links, a View URL (created using the View Builder), and web links. For example, you can add a hyperlink on a benefit page that takes the user to a Benefits Guide for your company's plans.

You can set this information for a specific employer or for the enterprise.

> For detailed instructions:

1. In Sage Employee Self Service, log on as the Master User.

2. On the **System Admin** menu, select **System Settings > Employer Setup**, select the employer, and click the **Custom Content** tab.

3. Click 🔵 **> Help** and follow the instructions in the "Employer Setup - Custom Content" topic.

Assigning roles

In Sage Employee Self Service, assign one or more roles to each employee to define their access rights, approval authority, and notification settings.

Although most employees only use the system for normal self-service functionality (with the Employee role), you may want to assign some individuals to the Administrator role or a View Builder role.

Administrator roles

Individuals who perform administration for an employer's human resources, training, or benefits departments need additional rights and authority to perform their duties in Sage Employee Self Service. When you assign individuals to administrator roles, you also specify the employers for which the administrator has authority to approve requests and receive notifications. Benefit administrators can also set up benefit functionality, open enrollment, and life events. For example, a benefit administrator can determine the parameters for an open enrollment period, such as the length of the open enrollment period and which benefit plans are available for employees.

View Builder roles

View Builder is a Sage Employee Self Service feature that enables certain employees to create a View (similar to a template) that generates data output. Employees who are regular Sage ESS users (such as Human Resources Generalists) that have this role can then share data with employees who may not use Sage ESS (such as upper-management). After creating a View, it can be distributed as a URL link in an email message or saved as a Microsoft Excel Web Query file (*.iqy).

Sage Employee Self Service includes two system-defined roles for View Builder users:

- **View Creator.** Assign this role to any employee you want to view the data for their assigned employers. In addition to the **View Builder** menu, the employee with this role will have access to the **System Settings > Employer Setup**, **Custom Content > Create Custom Menu**, **Custom Content > User-defined Fields**, **Custom Content > Create Web Links**, and **Custom Content > Create File Links** on the **System Administration** menus.

- **Executive Viewer.** Assign this role to any employee you want to view all data for their assigned company. To create a View for an employee assigned this role, select **Executive Viewer** for **Access Level** on the **Format View** page of the **View Builder** page.

You can also create a custom View Builder role if your company needs more levels of access to views for various sets of employees.

> For detailed instructions on assigning administrator and view builder roles:
>
> 1. In Sage Employee Self Service, log on as the Master User.
>
> 2. On the **System Admin** menu, select **Roles and Logon > Assign Admin Roles** or **Roles and Logon > View Builder Roles**.
>
> 3. Click ❓ > **Help** and follow the instructions in the "Assign Administrator Roles" topic or "View Builder Roles" topic.

Setting up logon parameters

In Sage Employee Self Service, set the rules by which an employee is permitted to log on or create a new logon.

These rules apply to all employees in all employers in your system and include:

- Information an employee must provide to set up a logon and access the system

- The status the employee must have to be permitted to log on

- Employee logon history

- Password properties (such as length and expiration)

- Situations when an employee can be locked out (such as three failed logon attempts)

- Security questions to ensure the employee provides the correct answer for a password change or reset

> For detailed instructions:

1. In Sage Employee Self Service, log on as the Master User.

2. On the **System Admin** menu, select **Roles and Logon > Logon Setup**.

3. Click ❓ **> Help** and follow the instructions in the "Logon Setup" topic.

Your selections must ensure that the information the employee enters is unique. You must select at least one initial logon field. However, to uniquely identify employees, you might need to select more than one field. For example, if a company has more than one Robert Smith, you would need to require more than just first and last name for the employee to create a logon. In this case, you could require first name, last name, and social security number or social insurance number.

> **Note:** If you require the Social Security Number (U.S.) or Social Insurance Number (Canada), it does not display when the employee enters it on the **Create New Logon** page or the **Change or Reset Password** page. Instead, it is masked like a password.

Defining system settings

Use the **System Setup** page (**System Settings > System Setup**) in Sage Employee Self Service to define the following settings for all employers:

- **Archive Messages.** Specifies whether approved requests are archived.

- **Display All Training Courses.** Specifies whether all courses or only the employee's required courses are available for employee enrollment.

- **Display Home Page.** Specifies whether the Home page displays when then user logs on.

- **SSN/SIN Display Settings.** Specifies how the social security number (or SIN) for dependents and beneficiaries displays in windows and on reports.

- **SSN/SIN Display on Personal Page.** Specifies how the social security number (or SIN) displays on an employee's **Personal Profile** page.

- **View Indirect Reports.** Specifies whether managers can see information for their indirect reports.

- **Search Phone List By.** Sets the organization level by which an employee can search through the employee phone list.

- **Display Pay History From.** This date determines how much pay history information (hours, gross pay, deductions, taxes, and net pay) is shown on the employee's Pay History page.

- **Display Employment History From.** This date determines how much history information is shown to employees on their compensation, job, and performance pages.

- **Retain Audit Trail From.** This date determines how many audit trail history records should be kept in the system.

- **Display Pay History Before Published Date.** Specifies whether your employees can view their pay history data before their pay day.

- **Technical Admin Email Address.** Specifies the email address where information about unexpected error messages are sent.

- **System Emails Sent From.** Enter the email address of your company that you want to display for **From** in system-generated email messages.

> **Note:** The system does not verify that this email address is valid. SMTP (Simple Mail Transfer Protocol) must be set up and configured in order to send emails.

- **Display Available Fields.** Select how you want fields to display in the **Available Fields** list on the **Select Fields** page of the View Builder. You can select **Alphabetically** or **Grouped**.

> **Note:** If you select **Grouped**, you can expand a group to make individual selections or select a group to automatically select all fields in the group. For example, job and pay-related fields such as Unit Pay Rate, Hours/Units, and Annual Pay display under the Job and Pay group.

- **View Server Application URL.** If the View Builder and the View Consumer access the system by different URLs, you can specify which URL will be used for the View Builder's Copy to Clipboard function. (Otherwise, the View Builder will use the same URL that is being used for Employee Self Service.) This View Server Application URL will also be used for the Generate IQY File check box.

> For detailed instructions:
>
> 1. In Sage Employee Self Service, log on as the Master User.
>
> 2. On the **System Admin** menu, select **System Settings > System Setup**.
>
> 3. Click ❓ **> Help** and follow the instructions in the "System Setup" topic.

Defining time off

Use the **Time Off Setup** page in Sage Employee Self Service to define how employee time off functions for each of your Sage HRMS employers. For example, you can choose whether the system sends a notification when an employee deletes a request or you can define a specific number of hours an employee is allowed to exceed their available balance. You must define Time Off settings for each employer in your system.

> For detailed instructions:
>
> 1. In Sage Employee Self Service, log on as the Master User.
>
> 2. On the **System Admin** menu, select **System Settings > Time Off Setup**, and then select an employer.
>
> 3. Click ❓ **> Help** and follow the instructions in the "Time Off Setup" topic.

Customizing Sage Employee Self Service (optional)

You can customize the appearance of the Sage Employee Self Service to meet the specific needs of your employers. View the online Help for the specified page for more information.

- **Adding a welcome message on the logon page**

   Use the **Customize Logon Page** to select custom features for the logon page, including adding a welcome message.

- **Adding a custom logon reset message**

   When an employee has trouble logging in (such as an unsuccessful attempt to reset the password or retrieve the username), you can have a custom message displayed. Enter the message for **Logon Reset Message** on the **Customize Logon Page**.

- **Adding a company logo and color scheme**

Use the **Customize Employer** page to select custom stylesheets and logos for each employer in Sage Employee Self Service. You can display the company logo prominently on all screens and change color schemes to be consistent with your company's branding.

Before you customize the styles and graphics for an employer, you must create and upload any stylesheets or graphics to be used.

- **Adding links to external intranet or internet sites**

Use the **Create Web Links** page to create a link to a web page to help employees as they use Sage Employee Self Service. For example, you could add a link so employees could access the company's intranet. (This view URL can be created using View Builder.)

- **Adding links to company documents**

Use the **Create File Links** page to create a link to a document to help employees as they use Sage Employee Self Service. For example, you provide links so employees could view and print the company's handbook, company directory, or organization chart.

- **Adding text to pages**

Use the **Create Text References** page to enter and format text on a page to give employees more information about how to use the page. For example, you can add more information about the benefits listed on the **Current Benefit** page.

- **Adding a new menu item**

Use the **Create Custom Menu** page to add new menu items to the existing Sage Employee Self Service menus. For example, if your company has a company handbook, you can give your employees quick access to it by adding a **Company Handbook** menu item to the **Employee** menu.

- **Displaying user-defined fields**

Use the **User-defined Fields** page to select up from one to eight user-defined fields from Sage HRMS and payroll to display on employees' **Personal Profile** pages.

Setting up your web server for Sage HRMS Mobile App

This section outlines the steps you must take to support the Sage HRMS Mobile application. You can skip this section if:

- You are not on the premium version of Sage HRMS and Employee Self Service
- You do not wish to provide access to your web server outside of your firewall

Configuring your web server

Preparing your web server to support the Sage HRMS Mobile app may require a few extra steps. In the following instructions, the server where your Sage Employee Self Service is installed is considered your **"web server."** We may also refer to this server as the Sage HRMS web server. This is the same server where IIS is running and where Sage Employee Self Service is installed. The Sage HRMS web server must support SSL and be accessible outside your firewall. Follow the guidelines below to ensure your employees can access and take advantage of the new Sage HRMS Mobile app.

- You must have a premium subscription of Sage HRMS and Sage Employee Self Service
- You must be on the Q4 2024 release or later version of these products
- Your Employee Self Service address must be publicly accessible outside of your firewall
- The Employee Self Service AbraAWCAppPool must be set to use the Integrated Pipeline Mode in IIS
- Your web server must be configured to use "HTTPS" by installing an SSL certificate from a trusted certificate authority
- Your IT Administrator needs to configure your web server to enable HTTPS by specifying the SSL certificate

Once the configuration steps above are completed, your web server is ready for employees to connect using the Sage HRMS Mobile app.

> **Important!** The following requirements must be met before the Sage HRMS Mobile app can be used by your employees:
>
> - You must be on the Q4, 2024 release of the premium version of Sage HRMS and Sage Employee Self Service.

- Employee Self Service must be configured to use "HTTPS" and be publicly accessible outside of your firewall.

  If you have any concerns about security, please contact your Sage business partner or IT professional.

Chapter 5: Sage Employee Self Service System Maintenance

After you install Sage Employee Self Service, use the System Maintenance utility to configure your system, diagnose and troubleshoot errors, and check for invalid Sage Employee Self Service logons.

Using System Maintenance

The System Maintenance utility resides in a secure location on the server where Sage Employee Self Service is installed. To open the utility, you must have access to the Sage Employee Self Service server.

From the Start menu on your Sage Employee Self Service server, select **All Programs > Sage Employee Self Service > System Maintenance**.

Use the System Maintenance utility to:

- Configure the program and default settings
- Email configuration
- Perform SQL maintenance
- Reset the Master password
- Review server errors
- Review the API Log
- Review benefit calculation errors
- Remove invalid logons
- Configure Web security
- Create keys to link to add-on products and initiate single sign-on in Sage HRMS
- Run the Duplicate Key report

- Review the Process Log for information including errors related to the Processes completed in the web version of Sage HRMS
- Configure Sage 100 Payroll Link by entering the Sage 100 Payroll Location (if applicable)
- Run a process to Sync Employee GUIDS in Sage 100 Payroll Link
- Configure Sage Employee Self Service to allow automatic single sign-on authentication to the iRecruit web application for specific user roles (in iRecruit)
- Enable the Import Pay History feature to import employee paycheck information into Sage HRMS

Configuration and Settings tab

Use this tab to review or modify system information, such as the SQL database connection, Sage HRMS data location, your install information (code, serial number, and product licensing). These are system-specific settings that must be configured in order for Sage Employee Self Service to function. The configuration values are set during the installation of Sage Employee Self Service, but you can modify them on this tab.

When you click **Save** to save your changes, the utility validates information on this tab and returns error messages if you entered any invalid information.

> **Important!** You cannot save any information in the System Maintenance utility or proceed with any other system maintenance functions until you resolve all validation errors.

SQL Server section

- **Server Name**. Name of the SQL server where the Sage Employee Self Service database is located.
- **Database Name**. Name of the Sage Employee Self Service database. You may need to change the name of the database if you restored a backed-up database and renamed it.
- **User Name and Password**. The valid SQL server user name and password, which is required to access the SQL server. This user account must have dbo (database owner) permissions to access the database on the SQL server.

Sage HRMS section

This indicates the Sage HRMS database type to which you are connecting. Select **SQL Server** to display the following:

- **Server Name**. Name of the SQL server where the Sage HRMS database is located.
- **Database Name**. Name of the Sage HRMS database. You may need to change the name of the database if you restored a backed-up database and renamed it.
- **Username and Password**. A valid SQL server username and password is required to access the Sage HRMS database. This SQL Server logon must have SA (System Administrator) permissions.

Email section

The premium version of ESS now supports two different email configurations: SMTP Server and Third-Party SMTP Service.

Configuring the Mail Server SMTP Service

If the version of your ESS windows server is prior to version 2025, you can continue to use the built-in SMTP Server.

- **Enabled**. This check box is automatically selected after installing Sage Employee Self Service. Leave this check box selected if you want Sage Employee Self Service users to receive an email whenever a notification is sent to the Message Center. If your company does not need email or does not have the SMTP service configured yet, clear the check box.
- **SMTP Server**. Email server used by Sage Employee Self Service. SMTP should always be installed on the local server and be configured to forward email. The SMTP server name must always remain **localhost** or **<Local Server Name>** unless directed by Sage HRMS Customer Support.

> **Note:** You can also use a third-party SMTP Service in this scenario. See the information below on how to configure the email section of the Configuration and Settings tab to work with this service.

Configuring a Third-Party SMTP Service

If the version of your ESS windows server is version 2025, enter the settings for the email service below:

- **Enabled**. Select this check box to enable the third -party SMTP service settings.
- **SMTP Server**. Enter the SMTP server provided by your SMTP service. To use a port, add a colon followed by the port number.
- **Require Authentication**. Select this check box if the service requires authentication.
- **User Name and Password**. If the third -party SMTP service requires a User Name and Password to authenticate, enter your account's SMTP User Name and SMTP Password in these fields.

Sage Employee Self Service section

- **Locked**. Select this check box to lock Sage Employee Self Service, which will log off any employee currently logged on and prevent other employees from logging on. This enables you to perform tasks such as backing up and restoring the Sage Employee Self Service database.

  > **Warning!** If anyone using Sage Employee Self Service makes changes between the time the Sage HRMS and Sage ESS databases are backed up and the time the databases are restored, those changes are lost (including notifications, employee requests, and pending changes) when you restore the database because the data was not yet posted to Sage HRMS. This means that anyone who made a change must re-enter his or her changes. To avoid this situation, lock the Sage ESS database before you do a backup and then unlock it only when you are sure you do not have to restore the database.

- **Session Timeout**. Duration of inactivity (in minutes) before someone is automatically logged off from Sage Employee Self Service. Enter a value between 0 and 999.
- **Serial Number and Installation Code**. Information provided by Customer Service that is used to determine the employee license count and the Sage Employee Self Service modules installed and available. The **Installed Components** and **User Licenses** reflect the current configuration and change accordingly if you enter a new serial number and installation code.

- **Save**. When clicked, the system validates the configuration and settings and returns a message if there are invalid entries.

- **Reset**. When clicked, the system returns all fields to the values prior to the most recent time you opened System Maintenance.

- **Generate Master Password**. When clicked, the system changes the Master user password to a secure code that can be copied to your clipboard and pasted when logging onto Sage Employee Self Service. You can change the Master password to a password of your choice in Sage Employee Self Service by selecting **Roles and Logon > Change Password**.

SQL Maintenance tab

Use this tab to back up or restore your Sage Employee Self Service database.

For the Sage Employee Self Service and Sage HRMS databases to stay synchronized, whenever you back up or restore your Sage Employee Self Service database, you must also do the same operation in Sage HRMS.

> **Warning!** If anyone using Sage Employee Self Service makes changes between the time the Sage HRMS and Sage ESS databases are backed up and the time the databases are restored, those changes are lost (including notifications, employee requests, and pending changes) when you restore the database because the data was not yet posted to Sage HRMS. This means that anyone who made a change must re-enter his or her changes. To avoid this situation, lock the Sage ESS database before you do a backup and then unlock it only when you are sure you do not have to restore the database.

> **Note:** Before using the **SQL Maintenance** tab:
>
> The **\Sage Software\Employee Self Service\CustomFiles** folder on the web server is not backed up during the backup procedure. This is the folder where custom style sheets and custom graphics are uploaded when you perform the Sage Employee Self Service Load to Server operation. If you have uploaded files, you should do a separate, manual backup of this folder whenever you back up your database.

- **Backup File Path**. This is the location and name of your Sage ESS database backup file. Confirm that it is correct.
- **Backup**. Click **Backup** and confirm the action to start the process. An indicator shows the process as it runs and a message displays when it is finished.
- **Restore**. Click **Restore** and confirm the action to start the process. An indicator shows the process as it runs and a message displays when it is finished.

> **Note:** If you restore a database that was backed up in a previous version of Sage Employee Self Service, the system automatically upgrades the database to the latest installed version during the restore process.

- **Upgrade Database**. Do not use this unless directed by Sage Customer Support.

- **Key Update**. Do not use this unless directed by Sage Customer Support.

- **Apply Fix File**. Do not use this unless directed by Sage Customer Support.

Server Errors tab

Use this tab to display a message for each critical Sage Employee Self Service error. In addition, you can review issues related to the APIs for the **Sage HRMS Mobile** app.

The messages contain the following information:

- The error message

- The user who caused the error

- Client information

- Server information

- The complete SQL trace, if applicable

Select a SQL error on the **Server Errors** tab to view a description of the error. You can also select any of the following items for additional information on the error: Environment, Message, Source, Stacktrace, Targetsite.

Because error messages written to the server's event log may contain user data, you can select the **Abbreviate Logged SQL Errors** check box for security purposes. The system will "crop" server error messages to the first few characters. However, because this is likely to strip off information that could help determine the cause of the error, you can also clear the check box to view the full server error message.

You can also click **Open File** and navigate to and open the error log on the server (**Sage Software\Employee Self Service\Log**). Note that when a server error occurs in Sage Employee Self Service, the employee sees a high-level description of the error and can send the error to the technical administrator.

If you are on the premium version of Sage Employee Self Service, you can also view the API log for issues related to the **Sage HRMS Mobile** app starting with the Q4 2024 release. Select the 'View API Log' button under the tab headers to review API issues reported by the app.

Benefit Calculation Errors tab

The system keeps a daily log of all benefit calculation errors and provides the ability to access the log files on this tab. You can click a file to see the expressions that caused the calculation error. However, this information does not provide the location in Sage HRMS where the errors occur.

The error log is also available on the server at **\Sage Software\Sage Employee Self Service\Log**.

Duplicate Key Report tab

Use this tab to run a report to display all Sage HRMS records that have identical keys. When someone working in Sage Employee Self Service attempts to open a page with records that contain duplicate keys, the system generates the "No records could be displayed. Contact your Human Resources department for assistance." message. For this reason, you should run this report and delete all duplicate records before allowing anyone to log on to Sage Employee Self Service for the first time.

> **Tip:** Run this report every couple of months at a time of day when the Sage HRMS database is not heavily used.

The duplicate key report examines Sage HRMS tables used by Sage Employee Self Service and displays each table where duplicate keys are found, a list of the columns that make up the key (the combination of all data in these columns should be unique), and a list of column value combinations (keys) that have multiple matching records in the table. Refer to Tables and Keys used by Sage ESS for a list of the keys in Sage HRMS tables used by Sage Employee Self Service.

You can resolve these conflicts through the Sage HRMS client by changing information in fields for the records listed or you can correct duplicate records directly in the SQL tables.

> **Caution!** If you do not have access to Microsoft SQL Server or do not have experience modifying tables, contact your implementation specialist before proceeding. You can also contact Customer Support for assistance.

For tables that contain records that are connected to individual employees, an additional column with the employee name is shown in the duplicate record listing. For example, when an employee has a duplicate record. the following **Skills** page for an employee in the Sage HRMS client shows two COMPUTER skill codes. To fix the duplicate record for this employee, delete one of the records.

To save or print the report as an .RTF file, click **Export**.

Remove Logins tab

Use this tab to open logins that are no longer associated with Sage HRMS employees. Select a **Login Name** and click **Remove Logins** to remove it from the Sage Employee Self Service Users database (tUSERS). An employee user license becomes available for each invalid login name that is removed.

You can also use this tab to see all users (with valid or invalid logons) in the Sage HRMS Employee database.

1. Double-click the image in the upper left corner of the System Maintenance utility to reveal the **Show All Users** check box.
2. Select the **Show All Users** check box to display all employees with logins to the system.
3. With all employees displayed, you can proceed to select and remove all employees from the Sage Employee Self Service Users database (tUSERS). This option is useful if you are moving customer data from a test environment to a live environment.

> **Warning!** If you select **Show All Users** and click **Remove Logons**, the system irrevocably deletes all employee, manager, and administrator data in Sage Employee Self Service for all invalid users. This includes notifications, pending benefit elections, and time-off requests. You should **always** create a backup of your Sage Employee Self Service database before removing logons.

Web Security tab

Use this tab to configure the URLs and Client IP addresses that can create a session using the internal and external entry points to Sage Employee Self Service. Also use this tab to restrict internal and external users' access to your Sage Employee Self Service system.

1. For **Start Page**, select one of the following pages to open when the user logs on:

    - **Employee / Administrator**. Opens the internal start page (the **Sage ESS Logon** page).

    - **View Consumer**. If you are using the Employee Analytics capability, this opens a page created with View Builder.

2. For **http(s)//**, enter the server/DNS name of all servers you want to allow when requesting the selected start page.

3. Click **Add** to add the name to the list; (if the list is empty, there are no restrictions). The following characters are not permitted as part of a server name: `` `~!@#$%^&()=|\{} [];\"'<>,/ ``

4. In the **IP** field, enter four sets of numbers that make up a Client IP address.

5. Click **Add** to add the number as an allowable address when requesting the selected start page; (if the list is empty, there are no restrictions). For each **IP** box, enter up to three characters. Only the following characters are allowed: `1 2 3 4 5 6 7 8 9 0 * ?`

6. Restart IIS whenever you make a change to Web Security. To restart IIS, either:

    - From an MS-DOS prompt, type `iisreset` and press **Enter**.

    - Click the Start menu and select **Administrative Tools > Services**. Right-click **World Wide Web Publishing Service** and select **Restart**.

Keys tab

Use the arrows on the tab bar to navigate to the **Keys** tab. Use this tab to generate keys (secure codes to link systems) to connect with third party applications.

Click **Generate Keys** to generate keys for single sign-on services for your employees.

> **Note:** To set up single sign-on service for Sage HRMS users (to log in to Sage ESS as the employee), you can click **Generate Keys** if no keys exist. Otherwise, the existing keys will be used by Sage HRMS when you configure Sage ESS. See Sage HRMS help for instructions to set up HRMS users with single sign-on access.

> **Tip:** You can always generate a new set of keys at any time by clicking the **Generate Keys** button.

Processes tab

Use this tab to see the status of the Sage HRMS Processes service. You can also Start and Stop the Sage HRMS Processes service from this tab. Click View Log to review the events triggered by the Processes. This service is used to process Sage HRMS tasks in the web.

Integrations tab

Use this tab to configure integrations with other Sage products or access with third-party applications using single sign-on authentication.

Sage 100 Setup

The **Sage 100 Setup** section allows you to enter the **Sage 100 Payroll Location**. Click the ellipses button and browse to the location where Sage 100 is installed and click Save. This information is stored in the SageHRMS_Live database along with other Sage 100 Payroll Link configuration details. In addition, use the **Sync Employee GUIDs** button to sync employee guids if Sage HRMS and Sage 100 get out of sync.

iRecruit Setup

Enter your iRecruit API Key in the iRecruit Setup section to set up single sign-on authentication to the iRecruit web application for specific user roles in iRecruit. The iRecruit pages will be available under the My Menus section of the ESS menu the next time a user who is in an appropriate iRecruit user role logs onto Sage ESS on a computer or on a mobile device. If the user is valid, ESS will open iRecruit in a new browser window or tab using single sign-on authentication. To remove access to iRecruit, delete the iRecruit API Key and click Save.

> **Note:** If an invalid API Key is entered in the iRecruit API Key field, iRecruit menu items will still appear under the My Menus section on the ESS menu. These pages are not valid pages; therefore the user will not be able to access the iRecruit application. To prevent this scenario, change the page access for these pages to 'No Access' under the Custom section on the Page Setup tab of the Employer Setup in ESS.

Pay History

Select the **'Enable Import Pay History in the web version of Sage HRMS'** check box to enable the Import Pay History feature on the Connected Service menu in the web version of Sage HRMS.

The Import Pay History feature allows users to manually import employee paycheck information into Sage HRMS using a CSV file format. Click here for more information on the **Import Pay History** process.

Recommended setup

Limit the **Employee / Administrator** page (internal entry point) to a DNS or wins name of the server that is designated for Sage Employee Self Service / internal use. Optionally, if employee access over the Internet is not desired, limit the Client IP addresses to only those that match the company intranet.

Limit the **View Consumer** page (internal entry point) to a DNS or wins name of the server that is designated for Sage Employee Self Service / internal use. Optionally, if view access over the

Internet is not desired, such as if you will only distribute View output as Microsoft Excel Web Query (*.iqy) files, limit the Client IP addresses to only those that match the company intranet.