

MARCH 2022

# Setup Guide

Web Services for Horizon 6.2.2



SirsiDynix®

*The information contained herein is the proprietary, confidential and/or trade secret of SirsiDynix. All rights not expressly granted in writing are reserved by SirsiDynix. This manual shall not be reproduced, transmitted, stored in a retrieval system, duplicated, used or disclosed in any form or by any means for any purpose or reason, in whole or in part, without the express written consent of SirsiDynix or except as provided by agreement with SirsiDynix. The information in this document is subject to change without notice and should not be construed as a commitment by SirsiDynix.*

SirsiDynix grants the right of copying the enclosed material solely for the internal business use of the end user if (1) this document has been legitimately obtained by purchase or by license agreement in conjunction with SirsiDynix products, and (2) this copyright statement is included with each copy. All other copying or distribution is strictly prohibited. Complying with all applicable copyright laws is the responsibility of the user.

SirsiDynix trademarks include but are not limited to BLUEcloud™, BookMyne®, Directors Station®, EOS.web®, eResource Central®, MobileCirc®, SirsiDynix®, SirsiDynix Enterprise®, SirsiDynix Horizon®, SirsiDynix Portfolio™, SirsiDynix Symphony®, Unicorn®, Web Reporter™, and WorkFlows™. Unauthorized use of any SirsiDynix trademark is prohibited.

Other product and company names herein may be the trademarks of their respective owners and SirsiDynix claims no ownership therein. All titles, versions, trademarks, claims of compatibility, etc., of hardware and software products mentioned herein are the sole property and responsibility of the respective vendors. SirsiDynix makes no endorsement of any particular product for any purpose, nor claims responsibility for its operation and accuracy.

SirsiDynix products are developed exclusively at private expense. Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in DFARS 252.227-7013(b)(3) and in FAR 52.227-19(b)(1,2).

# Contents

<b>About this guide</b> .....	<b>vii</b>
Summary of contents .....	vii
Possible differences between the software and this guide .....	viii
Documentation updates .....	viii
Comments and suggestions .....	ix
<b>Getting Started</b> .....	<b>1</b>
About Web Services for Horizon .....	1
System requirements .....	3
Hardware .....	3
Operating system .....	4
Java software .....	4
Apache Tomcat servlet container .....	5
<b>Installing Web Services</b> .....	<b>6</b>
Installation overview .....	6
Before you begin .....	7
Starting your installation .....	7
Running the installer .....	8
Changing the locale of the installer .....	9
Choosing the correct installation type .....	10
Installing Web Services with Tomcat .....	10
Installing Web Services only .....	13
Upgrading Web Services .....	15
Finding and setting Java environment variables .....	18
Installer configuration properties .....	19
Tomcat configuration properties .....	20

Horizon configuration properties .....	21
Web Services configuration properties .....	22
Horizon Information Portal configuration properties .....	23
Troubleshooting installation .....	24
<b>Advanced Installation .....</b>	<b>25</b>
Creating the properties file .....	25
Essential properties .....	26
hz-spring properties .....	30
hip-settings properties .....	32
admin-settings properties .....	34
Running the installer in Silent mode .....	34
<b>Configuring Web Services .....</b>	<b>36</b>
Web Services Admin Basics .....	37
Accessing the Admin console .....	37
Understanding the Admin console interface .....	38
Logging in to the Admin console .....	39
Logging out of the Admin console .....	40
Changing the admin username .....	40
Changing the admin password .....	41
Viewing the current status of Web Services .....	41
Viewing or updating a Web Services license key .....	42
Resetting Web Services caches .....	42
Fields: Status page .....	43
Updating ILS configuration options .....	44
Fields: ILS Configuration .....	45
Updating the HIP Profile Settings .....	47
Fields: Edit HIP Profile Settings .....	48
Updating the HIP Configuration options .....	49
Fields: HIP Configuration — Use HIP .....	50
Turning off HIP dependency .....	52
Fields: HIP Configuration — Don't Use HIP .....	52
Fields: Web Service Profile Settings .....	54

Configuring CAS single sign-on .....	56
Fields: Single Sign-on Setup .....	57
Fields: Create/Edit Single Sign-on URL .....	58
LDAP Setup .....	59
About LDAP Authentication .....	59
Managing LDAP Server Connections .....	61
Changing the LDAP Timeout Settings .....	62
Fields: LDAP Setup .....	62
Fields: Add/Edit LDAP Server .....	63
Securing endpoints .....	66
Managing endpoint security .....	66
Fields: Endpoint Security .....	67
Fields: Endpoint Security Configuration .....	68
Denying Staff Access .....	70
Fields: Staff Deny List .....	71
Whitelisting a Horizon table .....	72
Fields: Policy Whitelist Settings .....	72
Managing the log files .....	73
Viewing Web Services Logs .....	73
Changing the logging level .....	74
Fields: Logs .....	75
Managing offline assets .....	76
Viewing the properties of an offline asset .....	77
Deleting an offline asset .....	77
Fields: Offline Assets .....	78
Allowing access to the SDK .....	79
Fields: Manage SDK .....	79
Customizing or localizing labels and messages .....	80
<b>Uninstalling Web Services .....</b>	<b>82</b>
<b>Troubleshooting .....</b>	<b>83</b>
General Troubleshooting .....	83
Restoring access if you cannot log in .....	83

Starting up Tomcat .....	84
Troubleshooting connection issues .....	85
Verifying that Web Services is running .....	85
Examining log files .....	86
catalina logs .....	87
requests log .....	87
hzws log .....	88
BlackBox log .....	89
Troubleshooting common errors .....	89
BeanCreationException: Error creating bean .....	90
BindException: Address already in use: JVM_Bind .....	90
Context initialization failed .....	90
File permissions errors .....	91
Initial LDAP bind failed .....	91
listenerStart error .....	92
<b>Appendix A: Key Concepts .....</b>	<b>93</b>
Web Services base URL .....	93
<b>Appendix B: Advanced Tomcat configuration .....</b>	<b>94</b>
<b>Appendix C: Managing Password Lockout .....</b>	<b>95</b>
Configuring password lockout .....	95
Clearing the lockout cache .....	96
Fields: Lockout Settings .....	96
<b>Appendix D: Configuring Email Templates .....</b>	<b>99</b>
Configuring Checkout Receipt Email Template .....	99
Configuring the Reset My PIN Template File .....	101
<b>Index .....</b>	<b>103</b>

# About this guide

This *Setup Guide* explains how to install and set up Web Services for Horizon. It provides an overview of the software, including a brief summary of Web Services architecture, and describes system requirements and configuration properties.

This guide is intended for library system administrators who need to install and set up Web Services for Horizon for use with their SirsiDynix Horizon integrated library system. To use this guide, you should understand software administration and have a working knowledge of Java applications, Apache Tomcat in particular.

For more information about this guide, see the following topics:

<a href="#">Summary of contents</a> .....	<a href="#">vii</a>
<a href="#">Possible differences between the software and this guide</a> .....	<a href="#">viii</a>
<a href="#">Documentation updates</a> .....	<a href="#">viii</a>
<a href="#">Comments and suggestions</a> .....	<a href="#">ix</a>

## Summary of contents

This guide contains these major sections:

- **Getting Started** on page 1 provides overview information about Web Services.
- **Installing Web Services** on page 6 gives instructions on how to install Web Services on your system using either a GUI or Console mode.
- **Advanced Installation** on page 25 gives instructions on using the installer in Silent mode.
- **Configuring Web Services** on page 36 describes the tasks associated with using the Web Services Admin console.
- **Uninstalling Web Services** on page 82 gives instructions on how to uninstall Web Services from your system.
- **Troubleshooting** on page 83 details different problem scenarios and how to fix them.
- **Appendix A: Key Concepts** on page 93 details different Web Services concepts that are important when installing and configuring Web Services.
- **Appendix B: Advanced Tomcat configuration** on page 94 details the recommended Tomcat settings and tells where to get information about how to configure advanced Tomcat settings.

- **Appendix C: Managing Password Lockout on page 95** details how to set up a lockout system that prevents hackers from easily cracking a password by locking the account from access after a specified number of failed attempt.
- **Appendix D: Configuring Email Templates on page 99** details how to set up templates for email receipts and Reset My PIN.

## Possible differences between the software and this guide

The names, labels, and sample windows in this guide reflect the default settings that are delivered with most new installations. The settings on your system may be different from these defaults, depending on your library's implementation choices and the way your system administrator sets up your system. For example, your system administrator can change labels and set up security to limit access to certain features.

Additionally, as you use the software, you can resize windows or customize your workspace. Consequently, your software environment may look and function differently than the environment described in the tasks in this guide.

This document is compatible with Web Services for Horizon 6.2.2. Information in this document may also be compatible with later versions.

## Documentation updates

Updates to this guide are posted to the customer support website between releases, as necessary. These updates provide corrections to unclear, incorrect, or incomplete information. They also provide documentation for enhancements that were not complete at the time the guide was first published.

You may access the customer support website at <https://support.sirsidynix.com>.



The customer support website requires a username and password. If you do not already have a username and password, contact your system administrator to receive one. If you are the system administrator for your library and need a username and password for the support website, please contact SirsiDynix Customer Support to receive one.

Documentation updates can include, but are not limited to, the following formats:

- PDF (Portable Document Format)
- HTML Webhelp



- EPUB
- Microsoft Word

To view a PDF file, you must install Adobe's Acrobat Reader on your workstation. You can download Acrobat Reader free of charge at Adobe's web site, <http://www.adobe.com>. Several open source eReaders are also available online which can open other formats such as EPUBs. Please contact SirsiDynix Customer Support if you are having trouble finding this guide in the format that you need.

## Comments and suggestions

SirsiDynix welcomes and appreciates your comments on its documentation. We want to know what you think about our manuals and how we can make them better. If you have comments about this guide, please send them to [docs@sirsidynix.com](mailto:docs@sirsidynix.com).

Be sure to include the title and version number of the guide and tell us how you used it. Then tell us your feelings about its strengths and weaknesses and any recommendations for improvements.

# Getting Started

Welcome to Web Services for Horizon. You should read the entire guide before installing and setting up Web Services on your system. Also, make sure to read over the [Installation overview on page 6](#). The overview provides a Quick Steps Guide to the required steps for installing Web Services for Horizon on your system.

See the following topics for more information:

<a href="#">About Web Services for Horizon</a> .....	1
<a href="#">System requirements</a> .....	3
<a href="#">Hardware</a> .....	3
<a href="#">Operating system</a> .....	4
<a href="#">Java software</a> .....	4
<a href="#">Apache Tomcat servlet container</a> .....	5

## About Web Services for Horizon

Web Services for Horizon is a Web application that provides simplified remote access to features of your SirsiDynix Horizon integrated library system (ILS). This information is used to power BLUEcloud Discovery, Staff, and Marketplace applications such as BLUEcloud Cataloging, eResource Central, BLUEcloud PAC, MobileCirc, and BookMyne. Web Services can also provide this information to clients across platforms or programming languages.

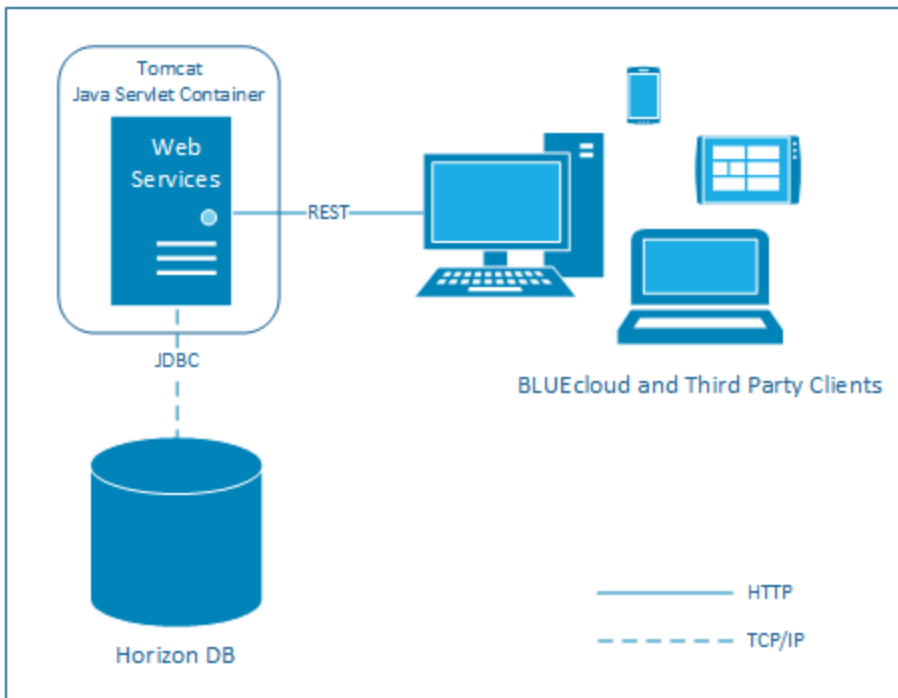
### Product compatibility

Web Services for Horizon 6.2.2 works with specific versions of other SirsiDynix products. In order to fully cover compatibility with different versions, SirsiDynix has created the *Upgrade Compatibility Matrix*, which lists the recommended and minimum product versions you can use. You can find the matrix document at <https://support.sirsidynix.com/kb/165510>.

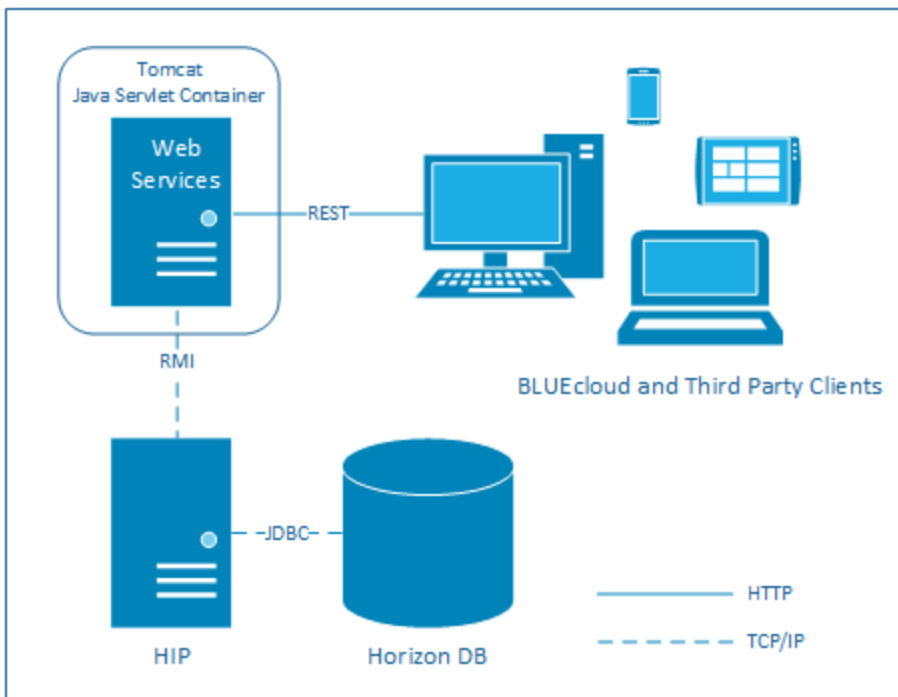
### Web Services Architecture

As a Java servlet, Web Services run in a Tomcat servlet container. Web Services can receive requests from both BLUEcloud and third-party clients, which in turn present that information to the library staff and patron users running the application. [Figure 1-1](#) illustrates the relationships of these components for the new Web Services framework. [Figure 1-2](#) illustrates the relationships of these components for the old Web Services framework (included with the new framework for backwards compatibility).

**Figure 1-1: New Web Services architecture**



**Figure 1-2: Old Web Services architecture**



## System requirements

Web Services for Horizon should be installed on a server-class system. For example, Web Services may be installed on the same server that runs your site's HIP server or ILS server.



Web Services for Horizon can now work without Horizon Information Portal being enabled. For customers who need to utilize legacy Web Services for Horizon calls, Horizon Information Portal 3.23.1 or later is required.

### Security requirements

At SirsiDynix, security of patron data is a high priority. All of our Web Services for Horizon testing is conducted using HTTPS. Implementing Web Services with HTTP is at your own risk. We also strongly recommend that all Web Services configurations include SSL or TLS encryption.

### Server software requirements

To use Web Services for Horizon, you must have the following software installed:

- Java SE Development Kit (JDK) or Java Runtime Environment (JRE) version 11 or greater or Amazon Corretto version 11.
- Apache Tomcat version 9.0 or higher (a distribution of Tomcat version 9.0.43.0 is included in the installer for your convenience). We recommend using the Tomcat version included with the installer for the best performance and compatibility with Web Services for Horizon.

**Note:** Remember to uninstall any previous versions of Tomcat before installing the latest version included with the installer.

See the following topics for more information:

<a href="#">Hardware</a> .....	3
<a href="#">Operating system</a> .....	4
<a href="#">Java software</a> .....	4
<a href="#">Apache Tomcat servlet container</a> .....	5

## Hardware

Web Services for Horizon supports 64-bit architectures.

During typical operation, Web Services for Horizon requires 256 MB of free memory and about 250 MB of disk space. If you install multiple instances of Web Services, each instance will require an additional 100 MB of disk space for logging and about 100 MB of free memory.

By way of example, a site with 50 concurrent users will probably see memory use of 220–270 MB on the tomcat server and 200–300 MB memory usage on the ILS server. Free disk space on the tomcat server would need to be around 250 MB.

Although the default settings should be suitable for most installations, you may need to allow more memory or disk space, depending on your system's configuration. For example, if you are running Web Services with SirsiDynix Enterprise, you may need to increase the amount of memory available to Web Services to account for potentially heavy traffic.

In addition to memory and disk space, you can also configure heap space, stack space, perm space, and threading options in order to get the best performance with Web Services. For more information, see [Appendix B: Advanced Tomcat configuration on page 94](#).

## Operating system

Web Services for Horizon is supported on the following operating systems:

- Microsoft Windows Server 2012 R2, 2016, or 2019
- Linux (Red Hat Enterprise Linux 6 or 7)

Only 64-bit operating systems are supported.

## Java software

Web Services for Horizon requires a Java Virtual Machine (JVM). The JVM can be either the Java SE Development Kit (JDK) or Java Runtime Environment (JRE).

### Java 11

Web Services for Horizon requires Java Virtual Machine (JVM) version 11 or greater in 64-bit or Amazon Corretto version 11 depending on your hardware and operating system. The JVM can be either Java SE Development Kit (JDK) or Java Runtime Environment (JRE).



SirsiDynix recommends using Amazon Corretto. Oracle's Java can be used, but has not been tested and verified for use. Java platforms other than Corretto may require licensing.

### Getting the latest version of Java

To download the required version of Corretto software, visit this site:

<https://docs.aws.amazon.com/corretto/latest/corretto-11-ug/downloads-list.html>

## Apache Tomcat servlet container

Web Services for Horizon requires Apache Tomcat 9.0 or higher in order to run.

For your convenience, a distribution of Tomcat 9.0.43.0 is included in the Web Services for Horizon installer (use the **Full Installation** option during installation).



We recommend using the Tomcat version included with the installer for the best performance and compatibility with Web Services for Horizon. Remember to uninstall any previous versions of Tomcat before installing the latest version that is included with the installer.

If you do not use the Full Installation option, Tomcat must be installed prior to running the Web Services installer. You can download Tomcat at <http://tomcat.apache.org>. You may also need to make changes to your Tomcat installation for Web Services to run correctly (for more information, see **Appendix B: Advanced Tomcat configuration on page 94**).

# Installing Web Services

This section explains how to install Web Services to run on your system. Please review the installation overview to become more acquainted with each of the required steps.

See the following topics for more information:

<a href="#">Installation overview</a> .....	6
<a href="#">Before you begin</a> .....	7
<a href="#">Starting your installation</a> .....	7
<a href="#">Running the installer</a> .....	8
<a href="#">Changing the locale of the installer</a> .....	9
<a href="#">Choosing the correct installation type</a> .....	10
<a href="#">Installing Web Services with Tomcat</a> .....	10
<a href="#">Installing Web Services only</a> .....	13
<a href="#">Upgrading Web Services</a> .....	15
<a href="#">Finding and setting Java environment variables</a> .....	18
<a href="#">Installer configuration properties</a> .....	19
<a href="#">Tomcat configuration properties</a> .....	20
<a href="#">Horizon configuration properties</a> .....	21
<a href="#">Web Services configuration properties</a> .....	22
<a href="#">Horizon Information Portal configuration properties</a> .....	23
<a href="#">Troubleshooting installation</a> .....	24

## Installation overview

Here are the essential steps that you need to take to install and run Web Services:

Task	Where to learn more
Review system requirements and gather required information.	<a href="#">Before you begin</a> on page 7
Install Web Services.	<a href="#">Starting your installation</a> on page 7
Configure Java variables (Linux only).	<a href="#">Finding and setting Java environment variables</a> on page 18
Start the Tomcat service (Windows) or Tomcat instance (Linux).	<a href="#">Starting up Tomcat</a> on page 84

## Before you begin

Before you install Web Services for Horizon, review the hardware and software requirements listed in [System requirements on page 3](#). In particular, be sure you are using a valid version of the Java Virtual Machine (JVM).

It will also be helpful to gather the following information before running the installer (field names that you will encounter later in the installer are included in parentheses):

- The database hostname and port for the Horizon ILS database that Web Services will connect to (Database Host and Database Port).
- The database type for your Horizon ILS Database, Sybase or MSSQL (Database Type).
- The name of the database on the server that contains your Horizon ILS data (Database Name).
- The user that will be used to access the Horizon ILS database (Database User).
- The password for that user (Database User Password).
- The time zone of your ILS server (Time Zone).
- The currency code for fines and payment transactions through web services (Currency).
- If you intend to connect Web Services to an instance of Horizon Information Portal (HIP), you will also need the connection details for the HIP server you want to connect to.

For more information about these parameters, see [Horizon configuration properties on page 21](#) and [Web Services configuration properties on page 22](#).

## Starting your installation

Web Services for Horizon may be installed on the following platforms:

- Windows
- Linux

During the installation process, you will specify configuration options. For more information about these options, see [Web Services configuration properties on page 22](#).

Before you can begin selecting options for your Web Services installation, you must first find and run the appropriate installer.



See the following topics for more information:

## Running the installer

The file you use to launch the installer depends on the operating system that you are installing Web Services on. The following table lists the path to the installer file for each platform, where *<install source>* is the location of your installer files (for example, a CD-ROM drive or a directory where you unpacked the files, depending on how you received the software).

System	Installer to use
Windows	<code>&lt;install source&gt;/Disk1/InstData/Windows/NoVM/hzInst.exe</code>
Linux	<code>&lt;install source&gt;/Disk1/InstData/Linux/NoVM/hzInst.bin</code>



The installer requires a valid version of the Java Virtual Machine (JVM) in order to run. For more information, see [Java software on page 4](#).



If you want to install a license at the same time as installing Web Services, please include the license file (.lic) in the same directory as the installer executable before running the installer.

The installer can be run in three different modes, depending on your system's configuration.

### Graphical User Interface (GUI) Mode

If the installer detects that you are using a GUI-based operating system, it defaults to GUI mode. You can also force the installer to run in a GUI mode (for systems that have a GUI but default to console mode) using the `-i gui` command-line argument. For example:

```
hzInst.exe -i gui (Windows) or hzInst.bin -i gui (Linux)
```

In GUI mode, you can click **Next** to move forward through the steps as you specify options. Click **Previous** to return to a previous step. You can also click **Cancel** to exit the installation process.

### Console Mode

If the installer cannot display a GUI, it defaults to console mode. For command-line environments (Linux), you can also force the installer to run in console mode using the `-i` console command-line argument. For example:

```
hzInst.bin -i console
```

In console mode, you can press **Enter** to advance through the install process. Type **back** to return to a previous step. You can also press **Ctrl+C** to exit the installation process.

### Silent Mode

For advanced users, the installer also supports running in silent mode. For more information about running the installer in silent mode, see [Running the installer in Silent mode on page 34](#).

## Changing the locale of the installer

When running the installer in either GUI or console mode, the installer will launch with the default locale that is set for your system. The installer will also prompt you to select a locale immediately after it is launched. In GUI mode, this is represented by a dropdown with each locale that you can select. In console mode, you will be asked to specify the locale by choosing a number that corresponds to a list of locales in the console window. If you do not see the locale that you are looking for, review the list below to make sure that your locale is supported, then follow the directions for launching the installer with a specific locale.

### To launch the installer in a different locale

1. Open a command prompt (Windows) or terminal window (Linux).
2. Navigate to the directory on your system where the installer executable is located.
3. Enter one of the following commands, depending on your operating system and desired locale. See the list below for a list of supported locales along with their language code. The example below would run the installer using the Chinese-Traditional (*zh\_TW*) locale.

```
hzInst.exe -l zh_TW (Windows)
```

```
hzInst.bin -l zh_TW (Linux)
```

### Supported Locales

The Web Services for Horizon installer currently supports the following locales:

- Chinese-Traditional (*zh\_TW*)
- Chinese-Simplified (*zh\_CN*)
- English (*en*)
- French-France (*fr*)
- French-Canadian (*fr\_CA*)
- Spanish (*es*)

## Choosing the correct installation type

If you are running the installer in GUI or console mode, the first steps of the installer will be the same until you are prompted to select an installation type. Please read about each of the installation types below and choose the type that matches your needs. You can find detailed instructions for each installation type within that type's section in this guide. If you can't decide which type of installation is appropriate for your system, contact SirsiDynix Customer Support.

- **Installing Web Services with Tomcat on page 10** — Use this installation type if you do not have Tomcat installed (Full Installation).
- **Installing Web Services only on page 13** — Use this installation type if you want to install additional instances of Web Services or if you want to install Web Services into your own installation of Tomcat (Web Services Only).

**Important:** If you choose this option, ensure that the existing Tomcat meets the requirements specified in **Apache Tomcat servlet container on page 5**.

- **Upgrading Web Services on page 15** — Use this installation type if you have an earlier version of Web Services and you want to replace it with the current version (Web Services Upgrade).

**Important:** If you choose this option, ensure that you have upgraded your Tomcat to meet the requirements specified in **Apache Tomcat servlet container on page 5**.

## Installing Web Services with Tomcat

This section describes how to perform a full installation. Web Services for Horizon requires Apache Tomcat 9.0 or higher. For convenience, a distribution of Tomcat 9.0.43.0 is included with the installer. This installation type installs both Web Services and Tomcat.



(For Windows users) If you plan to install Tomcat to run as a service, you must run the installer as a system administrator.

## To install Tomcat and Web Services

1. Review the information and requirements in [Before you begin on page 7](#).
2. Launch the installer. For more information, see [Running the installer on page 8](#).

**Important:** The installer requires a valid version of the Java Virtual Machine (JVM) in order to run. For more information, see [Java software on page 4](#).

3. Review and accept the terms of the SirsiDynix and third-party license agreements.

**Note:** Until you select **I accept the terms of the License Agreement**, the **Next** button will be inactive.

The software automatically scans for `java.exe` in expected locations.

4. Select the JVM instance to use for your Tomcat installation. If you do not select a JVM, the installer will use the first JVM from the list.

**Note:** For Linux, the JVM that you select will be used for either the `JAVA_HOME` or `JRE_HOME` environment variable.

**Note:** In GUI mode, if you do not see the JVM you want, you can use one of these options to find `java.exe` on your system:

Option	Description
Search Another Location	Lets you specify another directory to scan. Any Java executables that are detected in this directory will be added to the list.
Choose Java Executable	Lets you select a specific Java executable. <b>Note:</b> If the <code>java.exe</code> you select does not meet the minimum version requirements, the installer will prompt you to choose again.

**Note:** In console mode, if you do not see the JVM you want, you can select the **Choose a Java VM already installed on this system** option to specify the path to another Java executable.

5. Choose a name for this instance of Web Services. This name is used in the Tomcat webapps directory where the application is installed. This name also appears in URLs used to access specific services, so only use alphanumeric characters that are valid in a URL (no spaces or other punctuation).
6. Specify the directory where you want to install Tomcat. Web Services is also installed into this directory.
7. Select the **Full Installation** option.
8. Specify the configuration details for Tomcat. For more information about specific properties, see [Tomcat configuration properties on page 20](#).
9. Specify the connection information for your Horizon ILS. For more information about specific properties, see [Horizon configuration properties on page 21](#).
10. Specify the configuration options for Web Services. For more information about specific properties, see [Web Services configuration properties on page 22](#).
11. Select the timezone for your Horizon ILS server. For more information about specific properties, see [Timezone on page 23](#).
12. If you want to connect Web Services to an instance of Horizon Information Portal (HIP), enter the HIP connection details. For more information about specific properties, see [Horizon Information Portal configuration properties on page 23](#).

**Important:** In order to finalize your HIP configuration, you will need to confirm the HIP settings listed in the Admin console. Web Services will not be able to connect to HIP until you have confirmed these settings. After you have completed the Web Services installation and started up Tomcat, visit the HIP Configuration page in the Admin console to verify your HIP settings. For more information, see [Updating the HIP Configuration options on page 49](#).
13. Review the pre-installation summary. If you are satisfied, click **Install** (or press **Enter** in console mode) to proceed with the installation.

The installer completes the installation.
14. For Linux, you need to set your `JAVA_HOME` or `JRE_HOME` environment variable to the JVM that you selected in step 4. For more information, see [Finding and setting Java environment variables on page 18](#).
15. Congratulations! You've finished installing Web Services for Horizon on your system. Before you can use Web Services, you need to start the Tomcat service (Windows) or Tomcat instance (Linux). For more information, see [Verifying that Web Services is running on page 85](#).

**Note:** For most systems, the default configuration delivered in the Web Services installer will work without modification. However, depending on your system, there may be additional setup tasks you need to complete before running Web Services. For more information, see [Appendix B: Advanced Tomcat configuration](#) on page 94.

**Note:** After running Web Services, if the hzws logs show file permission errors, you may need to reset the Tomcat Log On properties. For more information, see [File permissions errors](#) on page 91.

## Installing Web Services only

This section describes how to perform an installation that includes only Web Services. If you already have a version of Apache Tomcat installed that meets the minimum requirements (see [Apache Tomcat servlet container](#) on page 5), or if you need to install an additional instance of Web Services, then select this installation type.

If you choose to install multiple instances of Web Services, keep these guidelines in mind:

- Installing multiple instances of Web Services requires additional disk space for the service files, as well as space for logging. The additional space for these files totals approximately 150 MB for each instance of Web Services.
- Depending on the number of instances you install and the volume of requests Web Services receives, you may need to increase memory settings for Tomcat. For more information, see [Appendix B: Advanced Tomcat configuration](#) on page 94.

### To install Web Services only

1. Review the information and requirements in [Before you begin](#) on page 7.
2. Launch the installer. For more information, see [Running the installer](#) on page 8.

**Important:** The installer requires a valid version of the Java Virtual Machine (JVM) in order to run. For more information, see [Java software](#) on page 4.

3. Review and accept the terms of the SirsiDynix and third-party license agreements.

**Note:** Until you select **I accept the terms of the License Agreement**, the **Next** button will be inactive.

The software automatically scans for `java.exe` in expected locations.

4. Select the JVM instance to use for your Tomcat installation. If you do not select a JVM, the installer will use the first JVM from the list.

**Note:** For Linux, the JVM that you select will be used for either the *JAVA\_HOME* or *JRE\_HOME* environment variable.

**Note:** In GUI mode, if you do not see the JVM you want, you can use one of these options to find `java.exe` on your system:

Option	Description
Search Another Location	Lets you specify another directory to scan. Any Java executables that are detected in this directory will be added to the list.
Choose Java Executable	Lets you select a specific Java executable. <b>Note:</b> If the <code>java.exe</code> you select does not meet the minimum version requirements, the installer will prompt you to choose again.

**Note:** In console mode, if you do not see the JVM you want, you can select the **Choose a Java VM already installed on this system** option to specify the path to another Java executable.

5. Choose a name for this instance of Web Services. This name is used in the Tomcat `webapps` directory where the application is installed. This name also appears in URLs used to access specific services, so only use alphanumeric characters that are valid in a URL (no spaces or other punctuation).

**Important:** If you install more than one instance of Web Services under the same Tomcat, then this name will need to be unique from any other instances of Web Services that are installed.

6. Specify the directory where Tomcat is installed. This is the directory where Web Services will be installed.
7. Select the **Web Services Only** option.
8. Specify the connection information for your Horizon ILS. For more information about specific properties, see [Horizon configuration properties on page 21](#).
9. Specify the configuration options for Web Services. For more information about specific properties, see [Web Services configuration properties on page 22](#).
10. Select the timezone for your Horizon ILS server. For more information about specific properties, see [Timezone on page 23](#).

11. If you want to connect Web Services to an instance of Horizon Information Portal (HIP), enter the HIP connection details. For more information about specific properties, see [Horizon Information Portal configuration properties](#) on page 23.

**Important:** In order to finalize your HIP configuration, you will need to confirm the HIP settings listed in the Admin console. Web Services will not be able to connect to HIP until you have confirmed these settings. After you have completed the Web Services installation and started up Tomcat, visit the HIP Configuration page in the Admin console to verify your HIP settings. For more information, see [Updating the HIP Configuration options](#) on page 49.

12. Review the pre-installation summary. If you are satisfied, click **Install** (or press **Enter** in console mode) to proceed with the installation.

The installer completes the installation.

13. For Linux, you need to set your *JAVA\_HOME* or *JRE\_HOME* environment variable to the JVM that you selected in step 4. For more information, see [Finding and setting Java environment variables](#) on page 18.

14. Congratulations! You've finished installing Web Services for Horizon on your system. Before you can use Web Services, you need to start the Tomcat service (Windows) or Tomcat instance (Linux). For more information, see [Verifying that Web Services is running](#) on page 85.

**Note:** For most systems, the default configuration delivered in the Web Services installer will work without modification. However, depending on your system, there may be additional setup tasks you need to complete before running Web Services. For more information, see [Appendix B: Advanced Tomcat configuration](#) on page 94.

**Note:** After running Web Services, if the hzws logs show file permission errors, you may need to reset the Tomcat Log On properties. For more information, see [File permissions errors](#) on page 91.

## Upgrading Web Services

This section describes how to perform an upgrade installation of Web Services. If you want to upgrade from an earlier version of Web Services for Horizon, you should select this installation type.





Before performing an upgrade, please make sure to back up the following configuration files if you had made changes to them for an older version of Web Services: `admin-settings.properties`; `hip-settings.properties`; and `hz-spring.properties`. This will prevent you from losing any of your old settings when the installer overwrites these files during installation.



If you are running an instance of Horizon Web Services (any version, 1.4.1 or older), you cannot upgrade this instance to Web Services for Horizon. If you are installing Web Services for Horizon for the first time, you must perform a full installation instead, since you will need the new version of Tomcat to host a Web Services for Horizon instance. Web Services for Horizon does include the old Horizon Web Services framework within it for backward compatibility with clients that need to use the old Web Services. Contact SirsiDynix Customer Support if you have additional questions.

## To upgrade Web Services

1. Shut down Tomcat.

**Note:** If you are running Tomcat as a service (Windows only), refer to the [Windows documentation](#) if you need information about stopping and starting services.

2. Review the information and requirements in [Before you begin](#) on page 7.
3. Launch the installer. For more information, see [Running the installer](#) on page 8.

**Important:** The installer requires a valid version of the Java Virtual Machine (JVM) in order to run. For more information, see [Java software](#) on page 4.

4. Review and accept the terms of the SirsiDynix and third-party license agreements.

**Note:** Until you select **I accept the terms of the License Agreement**, the **Next** button will be inactive.

The software automatically scans for `java.exe` in expected locations.

5. Select the JVM instance to use for your Tomcat installation. If you do not select a JVM, the installer will use the first JVM from the list.

**Note:** For Linux, the JVM that you select will be used for either the `JAVA_HOME` or `JRE_HOME` environment variable.

**Note:** In GUI mode, if you do not see the JVM you want, you can use one of these options to find `java.exe` on your system:

Option	Description
Search Another Location	Lets you specify another directory to scan. Any Java executables that are detected in this directory will be added to the list.
Choose Java Executable	Lets you select a specific Java executable. <b>Note:</b> If the <code>java.exe</code> you select does not meet the minimum version requirements, the installer will prompt you to choose again.

**Note:** In console mode, if you do not see the JVM you want, you can select the **Choose a Java VM already installed on this system** option to specify the path to another Java executable.

6. Choose a name for this instance of Web Services. This name is used in the Tomcat webapps directory where the application is installed. This name also appears in URLs used to access specific services, so only use alphanumeric characters that are valid in a URL (no spaces or other punctuation).

**Important:** You must specify the same instance name as when you previously installed Web Services, despite the default option of `hzws`. For example, if you previously installed Web Services as `mylibraryws`, you need to change the name of the Web Services instance here to match that name. If you are unsure about your Web Services instance name, check your Tomcat webapps directory.

7. Specify the directory where Tomcat and Web Services are installed. This is the directory where the latest version of Web Services will be installed during the upgrade.
8. Select the **Web Services Upgrade** option.
9. Specify the connection information for your Horizon ILS. For more information about specific properties, see [Horizon configuration properties on page 21](#).
10. Specify the configuration options for Web Services. For more information about specific properties, see [Web Services configuration properties on page 22](#).
11. Select the timezone for your Horizon ILS server. For more information about specific properties, see [Timezone on page 23](#).

12. If you want to connect Web Services to an instance of Horizon Information Portal (HIP), enter the HIP connection details. For more information about specific properties, see [Horizon Information Portal configuration properties](#) on page 23.

**Important:** In order to finalize your HIP configuration, you will need to confirm the HIP settings listed in the Admin console. Web Services will not be able to connect to HIP until you have confirmed these settings. After you have completed the Web Services installation and started up Tomcat, visit the HIP Configuration page in the Admin console to verify your HIP settings. For more information, see [Updating the HIP Configuration options](#) on page 49.

13. Review the pre-installation summary. If you are satisfied, click **Install** (or press **Enter** in console mode) to proceed with the installation.

The installer completes the installation.

14. For Linux, you need to set your *JAVA\_HOME* or *JRE\_HOME* environment variable to the JVM that you selected in step 4. For more information, see [Finding and setting Java environment variables](#) on page 18.
15. Congratulations! You've finished installing Web Services for Horizon on your system. Before you can use Web Services, you need to start the Tomcat service (Windows) or Tomcat instance (Linux). For more information, see [Verifying that Web Services is running](#) on page 85.

**Note:** For most systems, the default configuration delivered in the Web Services installer will work without modification. However, depending on your system, there may be additional setup tasks you need to complete before running Web Services. For more information, see [Appendix B: Advanced Tomcat configuration](#) on page 94.

**Note:** After running Web Services, if the hzws logs show file permission errors, you may need to reset the Tomcat Log On properties. For more information, see [File permissions errors](#) on page 91.

## Finding and setting Java environment variables

To run Tomcat (Linux), you must set either your *JAVA\_HOME* or *JRE\_HOME* variable to the correct path. Which variable you need to set depends on whether you selected a JDK or JRE Java executable for your JVM when you installed Web Services. Setting your Java environment variable correctly ensures that Tomcat uses the correct version of the JVM to run.



You do not need to set your Java environment variable if you are using Windows. The correct variable should have been selected automatically.

### To find the current value for *JAVA\_HOME* or *JRE\_HOME*

1. Open a terminal window.
2. Enter one of the following commands, depending on whether you are using a Java JDK or JRE for your JVM:

```
env | grep JAVA
```

```
env | grep JRE
```

The system lists all environment variables that contain the string *JAVA* or *JRE*. This list will include values for *JAVA\_HOME* or *JRE\_HOME*, depending on which command you entered.

Once you have checked the value of *JAVA\_HOME* or *JRE\_HOME*, you may need to set one of them to the correct value. Depending on your system, you may want to create either a user- or system-level environment variable for *JAVA\_HOME* or *JRE\_HOME*. The instructions below show a common setup for a user-level environment variable. For additional details on setting user- and system-level environment variables, see the documentation for your operating system.

### To set a user-level environment variable

1. Open a terminal window.
2. Enter one of the following commands, depending on whether you are using the Java JDK or JRE for your JVM:

```
export JAVA_HOME=/usr/java/jdk11/bin/java
```

```
export JRE_HOME=/usr/java/jre11/bin/java
```

The system sets the environment variable according to the path you specified.

## Installer configuration properties

This section explains the configuration properties that you encounter while installing Web Services. Each property's name is provided along with the default value from the installer (where applicable) and a detailed description of how that property affects your Web Services installation.

See the following topics for more information:

## Tomcat configuration properties

The following Tomcat properties should be specified when installing Web Services for Horizon. The default property values are valid for most installations. If the Tomcat HTTP, HTTPS, and shutdown ports you specify are in use by other services or applications, you will receive errors while running Web Services.

Property	Installer default	Description
Tomcat Service Name (Windows only)	tomcat9	<p>Specifies the name of the Tomcat service. The name should be short and include only letters and numbers (no spaces or other punctuation). The name that appears in the Windows Local Services Manager will be this name appended to "Apache Tomcat". For example, if my Web Services name was <i>mylibraryws</i>, I would find the service under <i>Apache Tomcat mylibraryws</i>.</p> <p><b>Important:</b> This name must be unique. If the name you specify is already in use by another service, the installer will not be able to install Tomcat as a service.</p> <p><b>Note:</b> If you leave Tomcat Service Name blank, Tomcat will not be installed as a service. You will need to start and stop it manually from the command line instead.</p>

Property	Installer default	Description
Tomcat HTTP Port	8080	Specifies the network port Tomcat will listen on for HTTP requests.  <b>Important:</b> If the port you specify is already in use by another application, Tomcat will fail to start (see <a href="#">BindException: Address already in use: JVM_Bind on page 90</a> ). This port must be open to public access if using HTTP.
Tomcat HTTPS Port	8443	Specifies the network port Tomcat will listen on for HTTPS requests.  <b>Important:</b> This port must be open to public access if using HTTPS.
Tomcat Shutdown Port	8009	Specifies the network port that Tomcat will listen on for shutdown requests.

## Horizon configuration properties

The following Horizon connection properties should be specified when installing Web Services for Horizon. The default property values are valid for most installations.



All properties are required. If a property does not have a default value, you must supply a value appropriate to your ILS. If you do not specify valid values, you will receive errors while running Web Services.

Property	Installer default	Description
Database Host	no default	Specifies the IP address of the Horizon ILS database.

Property	Installer default	Description
Database Port	no default	Specifies the port number to use to connect to the Horizon ILS database.
Database Type	no default	Indicates whether the Horizon ILS database is a Sybase or Microsoft SQL (MSSQL) database.
Database Name	no default	Specifies the name of the database that contains the Horizon ILS data.
Database User	no default	Specifies the user that is used to access the Horizon ILS database.
Database User Password	no default	Specifies the password for the Database User.
Minimum Connections	1	The minimum number of database connections to keep open. You may want to increase this value if your Web Services instance handles a high volume of requests. This value must be a number.
Maximum Connections	15	The maximum number of database connections to keep open. You may want to increase this value if your Web Services instance handles a high volume of requests. This value must be a number.  <b>Important:</b> This value must be greater than or equal to the value of <i>Minimum Connections</i> .

## Web Services configuration properties

The following Web Services properties should be specified when installing Web Services for Horizon. The default property values are recommended for most installations.

### General Options

Property	Installer default	Description
Currency	no default	Specifies the default currency code that will be used by this instance of Web Services for fines and payment requests. This value can be any valid ISO 4217 currency code.
Logging Prefix	<web application name>	Specifies the prefix to use on log files for this instance of Web Services. The default prefix is the name you specified for this instance of Web Services.
Logging Directory	../logs	Specifies the directory where Web Services will store any log files that it generates. By default, this directory is placed in the Tomcat directory.

### Timezone

Specifies the time zone of the Horizon instance, which the ILS includes whenever it returns datetime data. The datetime for the client is controlled by Web Services. The time stamp is converted on incoming requests to the Web Services time zone, and the system assumes that outgoing responses are in the same time zone.

## Horizon Information Portal configuration properties

If you want to connect Web Services to an instance of Horizon Information Portal (HIP), the following properties should be specified when installing Web Services for Horizon.





In order to finalize your HIP configuration, you will need to confirm the HIP settings listed in the Admin console. Web Services will not be able to connect to HIP until you have confirmed these settings. After you have completed the Web Services installation and started up Tomcat, visit the HIP Configuration page in the Admin console to verify your HIP settings. For more information, see [Updating the HIP Configuration options on page 49](#).

Property	Installer default	Description
HIP Host	no default	Specifies the hostname or IP address to use when connecting to the HIP server.
HIP Port	no default	Specifies the port number to use when connecting to the HIP server.

## Troubleshooting installation

In Linux, installer messages go to stdout, so they appear in the terminal window you use to launch the installer if you start from a command line.

In Windows, installer messages are displayed in the installer window or in dialog boxes.


On completion, the installer also creates an installation log on all platforms in the target Tomcat directory. The name of this log file includes the name you specified for your instance of Web Services.

If you encounter errors during installation, refer to these resources.

# Advanced Installation

This section explains how to install Web Services using silent mode. This installation mode allows you to configure an `installer.properties` file in advance that the installer uses to perform the installation for your system. When the installer is run in silent mode, there is no console or GUI display, and you do not have to step through the installer.

This functionality can be very helpful for libraries that need to routinely perform a high number of installations. After configuring the `installer.properties` file for each instance of Web Services, the installations can be scripted to run together as a batch.



Because the silent mode installation requires a more advanced knowledge of each of the settings used to configure Web Services, this installation mode is not recommended for most installations. If you still have additional questions about silent mode installation after reading this section, contact SirsiDynix Customer Support.

See the following topics for more information:

<a href="#">Creating the properties file</a>	25
<a href="#">Essential properties</a>	26
<a href="#">hz-spring properties</a>	30
<a href="#">hip-settings properties</a>	32
<a href="#">admin-settings properties</a>	34
<a href="#">Running the installer in Silent mode</a>	34

## Creating the properties file

Before you can run the installer in silent mode, you must first create an `installer.properties` file that contains the settings and options the installer will use. This section of the guide explains the different sections that can be included in the `installer.properties` file and the details which are required, depending on the type of installation you are trying to perform (Full Installation, Web Services Only, or Web Services Upgrade).





Templates of the `installer.properties` file are available on the SirsiDynix Support Center website for download. These templates are pre-populated with useful examples. We recommend downloading these templates and reviewing them along with this guide. For additional support in using these templates, please contact SirsiDynix Customer Support.

See the following topics for more information:

## Essential properties

The following properties must be included in the `installer.properties` file for all installation types. A table is provided which describes each of the properties shown in the example. When multiple lines of the same property are included, some will be commented out (shown with a `#` at the beginning of the line). This indicates that a choice must be made between a set of possible options for that property (all possible options are included).

### *Required properties for all installation types*

```
#Choose Installer Mode (Optional)
#-----
INSTALLER_UI=SILENT
#INSTALLER_UI=CONSOLE
#INSTALLER_UI=GUI

#Choose Properties Load Configuration Settings
#-----
LOAD_DEFAULT=FALSE
LOAD_FROMFILE=TRUE
LOAD_EXISTING=TRUE

#Select Java Virtual Machine
#-----
JDK_HOME=
JAVA_DOT_HOME=
JAVA_EXECUTABLE=

#Web Services Instance Name
#-----
WAR_NAME=

#Tomcat Installation Directory
#-----
USER_INSTALL_DIR=

#Choose Installation Type
#-----
```

```
#For full installation of both Web Services and the included Tomcat
CHOSEN_FEATURE_LIST=Tomcat,WS Install
CHOSEN_INSTALL_FEATURE_LIST=Tomcat,WS Install
#For installation of a new Web Services instance in an existing Tomcat
#CHOSEN_FEATURE_LIST=WS Install
#CHOSEN_INSTALL_FEATURE_LIST=WS Install
#For upgrading an existing Web Services instance
#CHOSEN_FEATURE_LIST=WS Upgrade
#CHOSEN_INSTALL_FEATURE_LIST=WS Upgrade

#Configure Tomcat
#-----
tomcat.service.name=tomcat9
tomcat.http.port=8080
tomcat.redirect.port=8443
tomcat.shutdown.port=8009
```

**Property Descriptions**

Property	Description
INSTALLER_UI	<p>Specifies the mode that the installer will run in. This includes the following options:</p> <ul style="list-style-type: none"> <li>• SILENT</li> <li>• CONSOLE</li> <li>• GUI</li> </ul> <p><b>Note:</b> This option should be left as <i>SILENT</i> in order to use the silent install mode.</p>
LOAD_DEFAULT	<p>Indicates whether the installer will load the default properties values that are included with the installer. For more information about the default properties values included with the installer, see <a href="#">Installer configuration properties on page 19</a>. This value should be left as <i>FALSE</i> while using the silent install mode.</p> <p><b>Note:</b> This value will be considered <i>TRUE</i> if it is not set to <i>FALSE</i>.</p>
LOAD_FROMFILE	<p>Indicates whether the installer will load properties values from configuration files that are included in the installer executable file's directory. This value should be set to <i>FALSE</i> if no such configuration files will be used or <i>TRUE</i> if they will be used.</p> <p><b>Note:</b> This value will be considered <i>TRUE</i> if it is not set to <i>FALSE</i>.</p>

Property	Description
LOAD_EXISTING	<p>Indicates whether the installer will load properties values from existing configuration files in the specified Tomcat directory (represented in the properties file by <i>USER_INSTALL_DIR</i> and <i>WAR_NAME</i>). This value should be set to <i>FALSE</i> if existing configuration files either do not exist or you do not want to use them.</p> <p><b>Note:</b> This value will be considered <i>TRUE</i> if it is not set to <i>FALSE</i>.</p>
JDK_HOME	<p>Specifies the path to the Java root directory if you are using the Java JDK for your JVM.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• <i>JDK_HOME=C:\Program Files\Java\jdk&lt;version&gt;</i> (Windows)</li> </ul> <p><i>JDK_HOME=/usr/java/jdk&lt;version&gt;/bin/java</i> (Linux)</p> <p>This property corresponds to the <i>JAVA_HOME</i> environment variable.</p> <p><b>Note:</b> You only need to define <i>JDK_HOME</i> if you are using the Java JDK for your JVM.</p>
JAVA_DOT_HOME	<p>Specifies the path to the Java root directory if you are using the Java JRE for your JVM.</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• <i>JDK_HOME=C:\Program Files\Java\jdk&lt;version&gt;\jre</i> (Windows)</li> </ul> <p><i>JDK_HOME=/usr/java/jre11/bin/java</i> (Linux)</p> <p>This property corresponds to the <i>JRE_HOME</i> environment variable.</p> <p><b>Note:</b> You only need to define <i>JAVA_DOT_HOME</i> if you are using the Java JRE for your JVM.</p>
JAVA_EXECUTABLE	<p>Specifies the path to the Java executable. This will commonly be <i>JRE_HOME\bin\java</i> or <i>JAVA_HOME\bin\java</i>, depending on whether you are using the Java JDK or JRE as your JVM.</p>

Property	Description
WAR_NAME	<p>Specifies a name for this instance of Web Services. This name is used in the Tomcat webapps directory where the application is installed and is also the name that will appear in URLs used to access specific services, so only use alphanumeric characters that are valid in a URL (no spaces or other punctuation).</p> <p>For example:</p> <pre>#WAR_NAME=hzws</pre>
USER_INSTALL_DIR	<p>Specifies the directory where Tomcat will be installed (for a full installation) or where Tomcat already exists (for installing another instance of Web Services or upgrading).</p> <p>For example:</p> <ul style="list-style-type: none"> <li>• <i>USER_INSTALL_DIR=C:\Program Files\SirsiDynix\WebServices</i> (Windows)</li> <li>• <i>USER_INSTALL_DIR=~/.SirsiDynix/WebServices</i> (Linux)</li> </ul>
CHOSEN_FEATURE_LIST	<p>In combination with <i>CHOSEN_INSTALL_FEATURE_LIST</i>, specifies the installation type. Both properties must be included and are already grouped according to the different types of installation you can perform. Be sure to remove the comment markers (#) from both lines for your desired installation type, and then comment the lines of the installation types that you will not be using.</p>
CHOSEN_INSTALL_FEATURE_LIST	<p>In combination with <i>CHOSEN_FEATURE_LIST</i>, specifies the installation type. Both properties must be included and are already grouped according to the different types of installation you can perform. Be sure to remove the comment markers (#) from both lines for your desired installation type, and then comment the lines of the installation types that you will not be using.</p>

Property	Description
<code>tomcat.service.name</code> (Windows only)	<p>Specifies the name of the Tomcat service. The name should be short and include only letters and numbers (no spaces or other punctuation). The name that appears in the Windows Local Services Manager will be this name appended to "Apache Tomcat". For example, if my Web Services name was <i>mylibraryws</i>, I would find the service under <i>Apache Tomcat mylibraryws</i>.</p> <p><b>Important:</b> This name must be unique. If the name you specify is already in use by another service, the installer will not be able to install Tomcat as a service.</p> <p><b>Note:</b> If you leave Tomcat Service Name blank, Tomcat will not be installed as a service. You will need to start and stop it manually from the command line instead.</p>
<code>tomcat.http.port</code>	<p>Specifies the network port Tomcat will listen on for HTTP requests.</p> <p><b>Important:</b> If the port you specify is already in use by another application, Tomcat will fail to start (see <b>BindException: Address already in use: JVM_Bind</b> on page 90). This port must be open to public access if using HTTP.</p>
<code>tomcat.redirect.port</code>	<p>Specifies the network port Tomcat will listen on for HTTPS requests.</p> <p><b>Important:</b> This port must be open to public access if using HTTPS.</p>
<code>tomcat.shutdown.port</code>	<p>Specifies the network port that Tomcat will listen on for shutdown requests.</p>

## hz-spring properties

The following properties should be included in the `installer.properties` file only if both `LOAD_FROMFILE` and `LOAD_EXISTING` are set to `FALSE` (for more information, see **Essential properties** on page 26). Otherwise, they are optional, as they will be overwritten by the settings found in these files.

*hz-spring properties*

```
#hz-spring.properties values
#-----
hz_dataSource.host=
hz_dataSource.port=
#pick one for hz_dataSource.type (sybase,sqlserver)
hz_dataSource.type=
hz_dataSource.dbname=
hz_dataSource.username=
hz_dataSource.password=
hz_dataSource.dbname=
hz_dataSource.username=
hz_dataSource.password=
hz_dataSource.minConn=1
hz_dataSource.maxConn=15
hz_timezoneID=
hz_currency=
```

**Property Descriptions**

Property	Description
hz_dataSource.host	Specifies the IP address of the Horizon ILS database.
hz_dataSource.port	Specifies the port number to use to connect to the Horizon ILS database.
hz_dataSource.type	Indicates whether the Horizon ILS database is a Sybase or Microsoft SQL (MSSQL) database. Possible values include: <ul style="list-style-type: none"> <li>• <i>sybase</i></li> <li>• <i>sqlserver</i></li> </ul>
hz_dataSource.dbname	Specifies the name of the database that contains the Horizon ILS data.
hz_dataSource.username	Specifies the user that is used to access the Horizon ILS database.
hz_dataSource.password	Specifies the password for the Database User.




Property	Description
hz_dataSource.minConn	The minimum number of database connections to keep open. You may want to increase this value if your Web Services instance handles a high volume of requests. This value must be a number.
hz_dataSource.maxConn	The maximum number of database connections to keep open. You may want to increase this value if your Web Services instance handles a high volume of requests. This value must be a number.  <b>Important:</b> This value must be greater than or equal to the value of <i>Minimum Connections</i> .
hz_timezoneID	Specifies the time zone of the Horizon instance, which the ILS includes whenever it returns datetime data. The datetime for the client is controlled by Web Services. The time stamp is converted on incoming requests to the Web Services time zone, and the system assumes that outgoing responses are in the same time zone.  <b>Note:</b> The value for your time zone can be any valid Java time zone ID. Commonly, these IDs are a continent followed by a city name, for example, America/New_York or Australia/Sydney.
hz_currency	Specifies the default currency code that will be used by this instance of Web Services for fines and payment requests. This value can be any valid ISO 4217 currency code.

## hip-settings properties

The following properties should be included in the `installer.properties` file only if both `LOAD_FROMFILE` and `LOAD_EXISTING` are set to `FALSE` (for more information, see [Essential properties on page 26](#)). Otherwise, they are optional, as they will be overwritten by the settings found in these files.

Additionally, you only need to add hip-settings properties if you will be connecting this instance of Web Services to Horizon Information Portal (HIP).



In order to finalize your HIP configuration, you will need to confirm the HIP settings listed in the Admin console. Web Services will not be able to connect to HIP until you have confirmed these settings. After you have completed the Web Services installation and started up Tomcat, visit the HIP Configuration page in the Admin console to verify your HIP settings. For more information, see [Updating the HIP Configuration options on page 49](#).

*hip-settings properties*

```
#hip-settings.properties values
#-----
hip_hip.url=
hip_hip.port=
```

**Property Descriptions**

Property	Description
hip_hip.url	<p>Specifies the hostname or IP address to use when connecting to the HIP server.</p> <p><b>Important:</b> If the <i>LOAD_DEFAULT</i> property is set to <i>FALSE</i>, this field must contain a valid value such as the empty string <code>\$EMPTY_STRING\$</code>. If this field does not contain a value and the <i>LOAD_DEFAULT</i> property is set to <i>FALSE</i>, the silent Web Services installation update will fail.</p>
hip_hip.port	<p>Specifies the port number to use when connecting to the HIP server.</p> <p><b>Important:</b> If the <i>LOAD_DEFAULT</i> property is set to <i>FALSE</i>, this field must contain a valid value such as the empty string <code>\$EMPTY_STRING\$</code>. If this field does not contain a value and the <i>LOAD_DEFAULT</i> property is set to <i>FALSE</i>, the silent Web Services installation update will fail.</p>

## admin-settings properties

The following properties should be included in the `installer.properties` file only if both `LOAD_FROMFILE` and `LOAD_EXISTING` are set to `FALSE` (for more information, see [Essential properties on page 26](#)). Otherwise, they are optional, as they will be overwritten by the settings found in these files.

### *admin-settings properties*

```
#admin-settings.properties values
#-----
#It is recommended that the admin_logging.prefix match the WAR_NAME
admin_logging.prefix=
admin_logging.directory=../logs
```

### Property Descriptions

Property	Description
<code>admin_logging.prefix</code>	Specifies the prefix to use on log files for this instance of Web Services. The default prefix is the name you specified for this instance of Web Services.
<code>admin.logging.directory</code>	Specifies the directory where Web Services will store any log files that it generates. By default, this directory is placed in the Tomcat directory.

## Running the installer in Silent mode

The file you use to launch the installer depends on the operating system that you are installing Web Services on. The following table lists the paths to the installer files, where *<install source>* is the location of your installer files (for example, a CD-ROM drive or a directory where you unpacked the files, depending on how you received the software).

System	Installer to use
Windows	<code>&lt;install source&gt;/Disk1/InstData/Windows/NoVM/hzInst.exe</code>
Linux	<code>&lt;install source&gt;/Disk1/InstData/Linux/NoVM/hzInst.bin</code>



The installer requires a valid version of the Java Virtual Machine (JVM) in order to run. For more information, see [Java software on page 4](#).



If you want to install a license at the same time as installing Web Services, please include the license file (.lic) in the same directory as the installer executable before running the installer.

### To run the installer in Silent mode

1. Prepare your `installer.properties` file according to the directions in [Creating the properties file on page 25](#), and put the `installer.properties` file in the same directory as the installer executable.
2. Locate the correct installer executable using the information listed above.
3. Open a command prompt or terminal window and navigate to the directory where the installer executable is located.
4. If you set `LOAD_FROMFILE` to `TRUE` in your `installer.properties` file (for more information, see [Essential properties on page 26](#)), ensure that you have put the necessary configuration files in the same directory as the `installer.properties` file and the installer executable.
5. Run the installer by entering one of the commands below, depending on your operating system.

`hzInst.exe` (Windows)

`hzInst.bin` (Linux)

# Configuring Web Services

This section will introduce you to the basics of the Web Services Admin console and describe the configuration and management tasks that you might need to perform.

See the following topics for more information:

Web Services Admin Basics .....	37
Accessing the Admin console .....	37
Understanding the Admin console interface .....	38
Logging in to the Admin console .....	39
Logging out of the Admin console .....	40
Changing the admin username .....	40
Changing the admin password .....	41
Viewing the current status of Web Services .....	41
Viewing or updating a Web Services license key .....	42
Resetting Web Services caches .....	42
Fields: Status page .....	43
Updating ILS configuration options .....	44
Fields: ILS Configuration .....	45
Updating the HIP Profile Settings .....	47
Fields: Edit HIP Profile Settings .....	48
Updating the HIP Configuration options .....	49
Fields: HIP Configuration — Use HIP .....	50
Turning off HIP dependency .....	52
Fields: HIP Configuration — Don't Use HIP .....	52
Fields: Web Service Profile Settings .....	54
Configuring CAS single sign-on .....	56
Fields: Single Sign-on Setup .....	57
Fields: Create/Edit Single Sign-on URL .....	58
LDAP Setup .....	59
About LDAP Authentication .....	59
Managing LDAP Server Connections .....	61
Changing the LDAP Timeout Settings .....	62
Fields: LDAP Setup .....	62
Fields: Add/Edit LDAP Server .....	63

Securing endpoints .....	66
Managing endpoint security .....	66
Fields: Endpoint Security .....	67
Fields: Endpoint Security Configuration .....	68
Denying Staff Access .....	70
Fields: Staff Deny List .....	71
Whitelisting a Horizon table .....	72
Fields: Policy Whitelist Settings .....	72
Managing the log files .....	73
Viewing Web Services Logs .....	73
Changing the logging level .....	74
Fields: Logs .....	75
Managing offline assets .....	76
Viewing the properties of an offline asset .....	77
Deleting an offline asset .....	77
Fields: Offline Assets .....	78
Allowing access to the SDK .....	79
Fields: Manage SDK .....	79
Customizing or localizing labels and messages .....	80

## Web Services Admin Basics

The Web Services for Horizon Admin console allows you to configure and manage an instance of Web Services. This section describes the basic functions and concepts for the Web Services Admin console.

See the following topics for more information:

### Accessing the Admin console

The Web Services for Horizon Admin console is a Web application that you can use from anywhere that you have access to the internet.

The URL for accessing the Admin console is

```
<service-instance>/admin
```

where *<service-instance>* is the base URL for an instance of Web Services. For more information, see [Web Services base URL on page 93](#).

For example, if your Tomcat host name is *libraryapps.example.org*, and you used the default port (8080), and the default Web Services name (*hzws*), the base URL for your Web Services instance would be:

*http://libraryapps.example.org:8080/hzws/admin*

Please be aware of these browser requirements for using the Admin console:

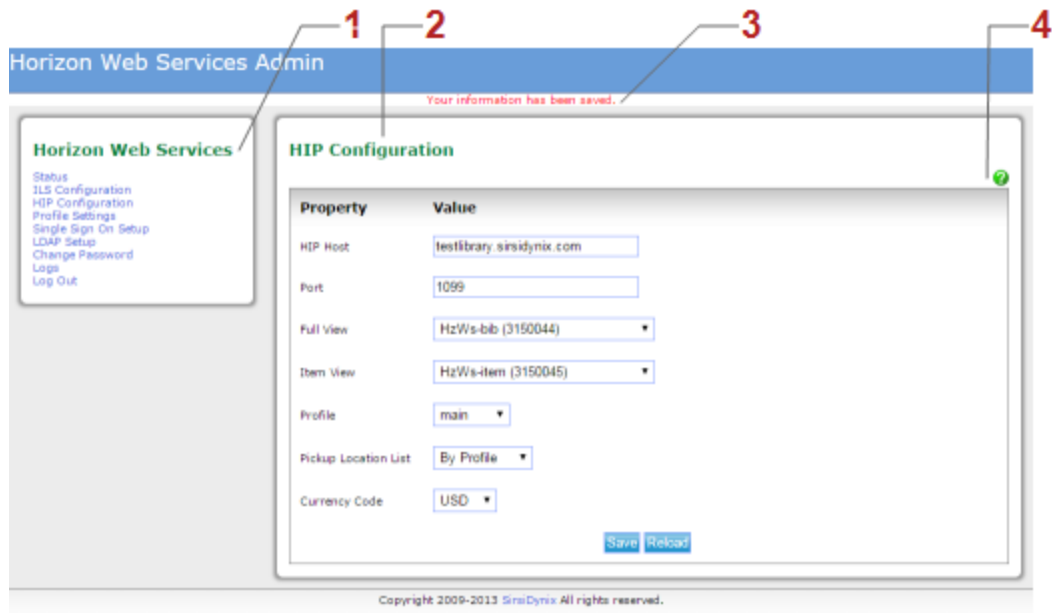
Browser	Supported Versions	Platforms
Chrome	Latest release and one version back	Windows/Macintosh
Edge		Windows 10
Firefox		Windows/Macintosh
Safari		Macintosh



As a Web application, the Admin console uses JavaScript and cookies. If either JavaScript or cookies is disabled, some features will not work.

## Understanding the Admin console interface

Here is a sample of the Web Services Admin console interface with a description of some of the key features referred to in this guide.



### Navigation pane

When you log in to the Admin console, a navigation pane (1) shows the different areas of the Admin console. Click on an option to view or configure settings.


### Workspace

When you click an option in the Navigation pane, the software displays additional settings or options in the Workspace area (2). Use the buttons, controls, and form fields to view or modify settings.

### Message bar

When you perform an action in the Admin console (for example, saving configuration changes), the software displays a message to indicate success or failure (3). If the operation failed, the message may include information about the cause of the failure.

### Help icon

A question mark icon  indicates that there is help available (4). Click on the icon to open the online help and view information about the options you see.

## Logging in to the Admin console

You must log in to use the Web Services Admin console.

When you first install Web Services, the default username and password for the admin console are both *admin*. Be sure to change the password to prevent unauthorized access (for more information, see [Changing the admin password on page 41](#)). You can also change the Admin console username if you want to (for more information, see [Changing the admin username on page 40](#)).

The username and password fields are case sensitive. If you forget your username or password, see [Restoring access if you cannot log in on page 83](#).

### To log in to the Admin console

1. Open the Log In page. For more information, see [Accessing the Admin console on page 37](#).
2. Type the Admin console username and password.
3. Click **Log In**.

If the username and password are correct, the software starts a new session for you and displays the Status page.



**Important:** Be sure to log out when you are finished using the Admin console to prevent unauthorized access. For more information, see [Logging out of the Admin console](#) on page 40.

## Logging out of the Admin console

For your security, if you do not perform any actions in Admin console for some time, the server will log you out. However, you should log out of the Admin console yourself when you finish configuring Web Services. This precaution will help to prevent unauthorized access.



Logging out using the Log Out option (instead of simply closing your browser) closes your session immediately, freeing up system resources. If you just close your browser, the session remains open on the server until it times out. Web Services uses the Tomcat session timeout. If you want to change the Tomcat session timeout or specify a timeout specific to a Web Services instance, refer to the Tomcat documentation.

### To log out of the Admin console

1. Click **Log Out** in the Navigation pane.

The software closes your session and confirms that you have been logged out.

## Changing the admin username

You can change the Web Services Admin console username at any time. You must log in to the Admin console to change the username. For more information, see [Logging in to the Admin console](#) on page 39.

### To change the Admin console username

1. Log in to the Admin console.
2. Click **Change Password** in the Navigation pane.
3. Enter the current console password in the **Current Password** field.
4. Enter a new username in the **New Username** field.
5. Click **Save**.

If the current password is valid, the software saves the new username and returns you to the Status page.

## Changing the admin password

You can change the Web Services Admin console password at any time. You must log in to the Admin console to change the password. For more information, see [Logging in to the Admin console on page 39](#).

### To change the Admin console password

1. Log in to the Admin console.
2. Click **Change Password** in the Navigation pane.
3. Enter the current Admin console password in the **Current Password** field.
4. Enter a new password in the **New Password** field.
5. Re-type the new password in the **Confirm New Password** field.

**Note:** Unless you want to create a new admin username, leave the **New Username** field blank.

6. Click **Save**.

If the current password is correct and the new passwords match, the software saves your change and returns you to the Status page.

## Viewing the current status of Web Services

The Status page gives you a quick glance at the current status of Web Services. You can see status information about the connection between Web Services and your Horizon ILS, check the version of Web Services, see which clients you have licensed with this instance of Web Services, and check the version of the Horizon ILS that Web Services is connected to. For more information regarding each of the fields on the Status page, see [Fields: Status page on page 43](#).

In addition to the information on the Status page, you can also add additional client licenses (for more information, see [Viewing or updating a Web Services license key on page 42](#)) and reset the Web Services caches (for more information, see [Resetting Web Services caches on page 42](#)).

If you are experiencing connectivity issues between Web Services and your ILS, see [Troubleshooting connection issues on page 85](#) for guidance on how to resolve the issue.

See the following topics for more information:

## Viewing or updating a Web Services license key

Each instance of Web Services can have its own license key. License keys are all inclusive; the licenses for every client that you have access to are included in a single file.

Only client IDs that have been added to the license file will be able to access information. Customer name information is included with the license file; this allows licenses to be independently audited.

Clients that are licensed are displayed on the Status page. Any temporary licenses that listed will also have an expiration date associated with the client ID.

### To view or update license details

1. Click **Status** in the Navigation pane if the Status page is not already displayed.

The Status page displays the licensed clients in the **Licensed Clients** field.

2. Click **update** at the end of the list of licensed clients.

The **Web Services License** page displays the current licensed client IDs and the license key if installed.

3. To install a license, click **Browse** or **Choose File** (depending on your browser).
4. Select the license file.
5. Click **Save** to save the license and return to the Status page.

If the license file you selected is valid, the new client IDs will display on the Status page. Otherwise, the software will display an error in the message bar.

## Resetting Web Services caches

To improve performance, Web Services caches information about some ILS policies and data. If you note discrepancies in data returned by Web Services after making changes in the ILS, you can reset the Web Services caches manually from the Status page. Resetting the Web Services caches should resolve any discrepancies that are occurring.

### To reset Web Services caches

1. Click **Status** in the Navigation pane.
2. Do one of the following:

- To reset all Web Services caches except for the security caches, click **Reset Services Only**. For more information about this choice, see [Reset Services Only on page 44](#).
- To reset all Web Services caches including the security caches, click **Reset All**. For more information about this choice, see [Reset All on page 44](#).

The Web Services caches are cleared and are repopulated as new requests are processed.

## Fields: Status page

The Status page displays information about the Web Services connection to the ILS, current software and Web Services versions, and current client licenses. You can also add additional client licenses and reset the ILS connection from this page.

### ILS Connection Status

Displays the status of the Web Services connection to the ILS. If the connection is active, it displays **Connected**.

If Web Services cannot connect to the ILS, it displays **Offline**. For guidance on resolving ILS connection issues, see [Troubleshooting connection issues on page 85](#).

### Web Services Version

Displays the current version information for this Web Services instance.

### Licensed Clients

Displays the Client IDs that this instance of Web Services is licensed for. You can also add additional licenses by clicking **update** at the end of the list. For more information, see [Viewing or updating a Web Services license key on page 42](#).

**Note:** If you have a temporary license, an expiration date also displays here.

### Licensed To

Displays the Customer ID and Customer Name for this group of client licenses.

### ILS Version

Displays version information for the SirsiDynix Horizon ILS that this Web Services instance is connected to.

**Note:** This field will be blank if the ILS Connection Status is **Offline**.

### Management Options

Option	Description
Reset All	<p>Lets you clear the following information that Web Services caches during normal operation:</p> <ul style="list-style-type: none"> <li>• Policy information</li> <li>• Other ILS data</li> <li>• Security caches</li> </ul> <p><b>Important:</b> When you clear security caches, all active staff and patron authentication sessions are closed. This requires any staff or patrons to log in again before they can continue to use their applications.</p> <p>For more information, see <a href="#">Resetting Web Services caches</a> on page 42.</p>
Reset Services Only	<p>Lets you clear the following information that Web Services caches during normal operation:</p> <ul style="list-style-type: none"> <li>• Policy information</li> <li>• Other ILS data</li> </ul> <p>For more information, see <a href="#">Resetting Web Services caches</a> on page 42.</p>

## Updating ILS configuration options

For Horizon, only the **Currency Code (Circulation)** field is editable from the ILS configuration page. All other fields must be edited directly in the `hz-spring.properties` file located in the `<tomcat\webapps\hzws>\WEB-INF\classes` directory, where `<tomcat\webapps\hzws>` is the path to your instance of Web Services.

### To update ILS configuration options

1. Choose **ILS Configuration** in the Navigation pane.
2. Update or change the options as needed.

**Important:** For Horizon, only the **Currency Code (Circulation)** field is editable from the ILS configuration page. All other fields must be edited directly in the `hz-spring.properties` file located in the `<tomcat\webapps\hzws>\WEB-INF\classes` directory, where `<tomcat\webapps\hzws>` is the path to your instance of Web Services.

**Important:** For details about each of the fields you encounter while updating ILS configuration options, see **Fields: ILS Configuration** on page 45.

3. Choose **Save**.

## Fields: ILS Configuration

The ILS Configuration page lets you edit the settings for your Horizon ILS database and allows you to update the Circulation Currency Code if desired.

### Database Host IP

Specifies the IP address of the Horizon ILS database.

This field is required.

### Database Port

Specifies the port number to use to connect to the Horizon ILS database.

This must be a valid port number (between 1 and 65535).

This field is required.

### Database Name

Specifies the name of the database that contains the Horizon ILS data.

This field is required.

### SYBASE or MICROSOFT

Indicates whether the Horizon ILS database is a Sybase or Microsoft SQL (MSSQL) database.

### Database Minimum Connections

The minimum number of database connections to keep open. You may want to increase this value if your Web Services instance handles a high volume of requests. This value must be a number.

This field is required.

### Database Maximum Connections

The maximum number of database connections to keep open. You may want to increase this value if your Web Services instance handles a high volume of requests. This value must be a number.

**Important:** This value must be greater than or equal to the value of *Minimum Connections*.

This field is required.

### ILS Timezone

Specifies the time zone of the Horizon instance, which the ILS includes whenever it returns datetime data. The datetime for the client is controlled by Web Services. The time stamp is converted on incoming requests to the Web Services time zone, and the system assumes that outgoing responses are in the same time zone.

**Note:** The value for your time zone can be any valid Java time zone ID. Commonly, these IDs are a continent followed by a city name, for example, *America/New\_York* or *Australia/Sydney*.

### Currency Code (Circulation)

Specifies the default currency code that will be used by this instance of Web Services for fines and payment requests. This value can be any valid ISO 4217 currency code.

### Always Require Authentication

Requires that all Web Services calls (with a few exceptions such as `login` and `version`) have valid authentication before they will be accepted by Web Services.

By requiring authentication for all calls, any client that makes a request must include a valid *sessionToken*.

### Allow Patron Search

Toggles the ability for staff users to search for patron accounts in Horizon.

### Allow Admin Access via Web Services

Toggles the ability to view administrative configuration by way of web service calls as well as through the Admin console. You can only edit the configuration through the Admin console.

### Borrower Authentication Field 1

Specifies the field to use for patron login and authentication. This is typically the borrower's barcode, although it could be the alternate ID or another uniquely identifying field. The default field is **bbarcode**.

**Borrower Authentication Field 2 (optional)**

Specifies which password field to use for patron login and authentication. This field is optional (you can select the blank option to indicate that no PIN or password is needed), although the default is **pin#**.

**Allow Admin Access via Web Services**

Specifies whether the options available through the Admin console can also be accessed through Web Services calls.

**Disable Legacy**

Specifies that no calls from previous versions of Web Services can be processed while legacy versions are disabled. If you are changing your client code to use only the ROA version, you can use this setting to verify that it does not include any legacy code. Legacy versions include any calls that are under the `rest/standard` path.

**Allow Patron Login without Barcode Prefix**

Specifies whether to allow logins using only the significant digits of the borrower's barcode. Significant digits don't include the barcode prefix or any leading zeros, as specified in the Location table in the Horizon client (for more information, see "Setting Up a Location Record" in the *System Administration Guide* of the Horizon online Help).

**Management Options**

Option	Description
Save	<p>Saves your changes to the ILS configuration.</p> <p>The software validates the new options by trying to connect to the ILS. This process may take a moment. If the connection is successful, the new configuration is saved.</p> <p>If the connection fails, verify that you have entered each of the values correctly.</p>
Reload	<p>Reloads the current configuration values from the server without saving changes.</p>

## Updating the HIP Profile Settings

The Profile Settings page allows you to make changes to HIP profile settings.





If Use HIP in HIP Configuration is disabled, no profiles are listed on this page. When HIP is disabled, profile settings are configured in the HIP configuration page. For more information, see [Fields: HIP Configuration — Don't Use HIP on page 52](#)

### To update HIP profile settings

1. Click **Profile Settings** in the Navigation pane.  
A list of HIP profiles appears.
2. Click on a profile from the list.  
The profile's details appear.
3. Change the profile's settings as necessary, then click **Save**.

**Note:** For more details about the fields you encounter while editing a profile's settings, see [Fields: Edit HIP Profile Settings on page 48](#).

## Fields: Edit HIP Profile Settings

The Profile Settings page lets you make changes to HIP profile settings. This settings affect how payment request logs are recorded in Horizon.

### Library Department

Specifies the library department that will be recorded in payment logs when requests are made with this profile.

### Workstation ID

Specifies the workstation ID that will be recorded in payment logs when requests are made with this profile.

### Cash Drawer ID

Specifies the cash drawer ID that will be recorded in payment logs when requests are made with this profile.

### User ID

Specifies the user ID that will be recorded in payment logs when requests are made with this profile.

### Management Options

You have these options:

Option	Description
Save	Saves your changes to the profile.
Reload	Reloads the profile's current configuration values from the server without saving changes.
Cancel	Returns to the previous page without saving any changes.

## Updating the HIP Configuration options

The HIP Configuration page allows you to update your HIP Configuration options. It lets you specify where the Horizon Information Portal host resides, how to connect to it, and which options to use when requesting item details. Your library should have already configured the options for these settings within HIP.

Web Services for Horizon natively supports all of the configurations that HIP provides. If your library doesn't use HIP or would like to discontinue using it, you can choose to not use HIP and instead configure those settings in the Web Services for Horizon Admin Console.



If you are configuring HIP for the first time after an installation of Web Services, you may also be visiting this page to finalize your Web Services installation. If this is the case, simply choose **Save** once to pull the default settings from HIP, verify those settings for each of the fields, and then choose **Save** again to save your HIP configuration.

### To update HIP configuration options

1. Click **HIP Configuration** in the Navigation pane.
2. Update or change the options as needed.

**Note:** For details about each of the fields you encounter while updating HIP configuration options, see [Fields: HIP Configuration — Use HIP](#) on page 50.

3. Click **Save**.

If you have provided a hostname and port number for a new HIP server, the system will pull the default values for the other fields directly from the HIP server. You will need to confirm these settings and then click **Save** again in order to save them.

If the connection to the HIP server fails, verify that you have entered the hostname and port number correctly.

## Fields: HIP Configuration — Use HIP

The HIP Configuration page lets you specify where the Horizon Information Portal host resides, how to connect to it, and which options to use when requesting item details. Your library should have already configured the options for these settings within HIP.

Web Services for Horizon natively supports all of the configurations that HIP provides. If your library doesn't use HIP or would like to discontinue using it, you can choose to not use HIP and instead configure those settings in the Web Services for Horizon Admin Console.

### Use HIP

Specifies whether Web Services for Horizon should use Horizon Information Portal to manage certain settings or if it should access those settings through the Horizon profile. For information about setting the Horizon profile settings, see [Fields: HIP Configuration — Don't Use HIP on page 52](#).

**Note:** If you change the Use HIP setting, you must choose **Save** to retain the setting. Otherwise, the setting will revert back to its original state when you leave the HIP Configuration page.

### HIP Host

Specifies the hostname or IP address to use when connecting to the HIP server.

This field is required.

### Port

Specifies the port number to use when connecting to the HIP server.

This field is required.

### Full View

Specifies the search index that will be used for full views. Full views represent the details that are shown on a title's details screen. The default value (*HZWS-bib*) is recommended.

**Item View**

Specifies the search index that will be used for item views. Item views represent the details that are shown on an item's details screen. The default value (*HzWs-item*) is recommended.

**Profile**

Specifies the default HIP profile that will be used when processing requests through Web Services. Additional details for each profile can be changed on the **Profile Settings** page. For more information, see [Updating the HIP Profile Settings on page 47](#).

**Pickup Location Set**

Indicates whether the pickup location list that is used for placing holds will be based on location or profile.

**Management Options**

Option	Description
Save	<p>Saves your changes to the HIP configuration.</p> <p>If you have provided a hostname and port number for a new HIP server, the system will pull the default values for the other fields directly from the HIP server. You will need to confirm these settings and then click <b>Save</b> again to save them.</p> <p>If the connection to the HIP server fails, verify that you have entered the hostname and port number correctly.</p> <p><b>Note:</b> If you change the Use HIP setting, you must choose Save to retain the setting. Otherwise, the setting will revert back to its original state when you leave the HIP Configuration page.</p>
Reload	<p>Reloads the current configuration values from the server without saving changes.</p>

**Related topics**

[Updating the HIP Configuration options on page 49](#)

## Turning off HIP dependency

Web Services for Horizon natively supports all of the configurations that HIP provides. If your library doesn't use HIP or would like to discontinue using it, you can choose to not use HIP and instead configure those settings in the Web Services for Horizon Admin Console.

### To off the HIP dependency

1. Choose **HIP Configuration** in the Navigation panel.
2. Choose Use HIP to remove the check mark and disable HIP dependency in Web Services for Horizon.

**Important:** You must specify a default profile before you can save the HIP configuration with HIP disabled. To do that, you need to first create a profile.

3. Choose **Add Profile** to create a Web Services profile.
4. Configure the **Profile to Location Mapping** and **Borrower Settings** as needed. For information about the options, see [Fields: Web Service Profile Settings on page 54](#).
5. Choose Save.

Now that the profile has been created, the Fee Payment Settings can be configured.

6. Configure the **Fee Payment Settings** as needed. For information about the Fee Payment Settings, see [Fields: Web Service Profile Settings on page 54](#).
7. When you have finished, choose **Save**.
8. Choose **Cancel** to return to the HIP Configuration page.
9. From the **Default Profile** drop-down list, select the profile you created.
10. Choose **Save** to apply the Use HIP and Default Profile settings.

### Related topics

[Updating the HIP Configuration options on page 49](#)

[Fields: HIP Configuration — Don't Use HIP on page 52](#)

## Fields: HIP Configuration — Don't Use HIP

The HIP Configuration page lets you specify where the Horizon Information Portal host resides, how to connect to it, and which options to use when requesting item details. Your library should have already configured options for these settings within HIP.

Web Services for Horizon natively supports all of the configurations that HIP provides. If your library doesn't use HIP or would like to discontinue using it, you can choose to not use HIP and instead configure those settings in the Web Services for Horizon Admin Console.

If your library currently does not use Horizon Information Portal as a public access catalog, you may benefit from turning off the HIP configuration. However, because Web Services for Horizon doesn't provide some functions that HIP provides, some clients may not have full functionality after HIP has been disconnected from Web Services for Horizon. The following table indicates the features that may or may not be available to you.

Client	My Lists	Search Catalog
SirsiDynix Enterprise	Supported	Supported
SirsiDynix Portfolio	Supported	Supported
BookMyne	Supported	Supported
BookMyne+	Unsupported, unless configured to use BLUEcloud.	Unsupported, unless configured to use BLUEcloud.
Social Library	Unsupported	Unsupported
3rd-party Clients	Unsupported, unless configured to use a different My List service, such as BLUEcloud.	Unsupported, unless configured to use a different search service, such as BLUEcloud.

If you have questions, contact SirsiDynix Customer Support.

**Use HIP**

Specifies whether Web Services for Horizon should use Horizon Information Portal to manage certain settings or if it should access those settings through the Horizon profile. For information about configuring the connection to HIP, see [Fields: HIP Configuration — Use HIP on page 50](#).

**Note:** If you change the Use HIP setting, you must choose Save to retain the setting. Otherwise, the setting will revert back to its original state when you leave the HIP Configuration page.

### Default Profile

Specifies the Web Services for Horizon profile you want to make the default. The default profile is used when a call is sent that does not include the Horizon profile. You cannot specify to not use HIP unless you have selected a default profile.

**Note:** If you change which Default Profile is selected, you must choose **Save** to retain the setting. Otherwise, the setting will revert back to its original state when you leave the HIP Configuration page.

### Management Options

Option	Description
Save	Saves the Use HIP and Default Profile settings. If you have changed either of these setting, when you leave the HIP Configuration page, those settings will revert to the previous settings.
Add Profile	Opens the Profile Settings page so you can create a new profile. For more information, see

### Profiles List

Option	Description
Profile	Lists the name of the profile.
Location	The library that the profile applies to.
Edit	Opens the Profile Settings page so you can modify the profile configuration.
Delete	Removes the profile from the list.

### Related topics

[Turning off HIP dependency on page 52](#)

[Fields: Edit HIP Profile Settings on page 48](#)

### Fields: Web Service Profile Settings

Profile Settings lets you set up profiles that provide configuration for Web Services for Horizon to handle borrower settings and fee payments.

## Profile to Location Mapping

Specifies the name and the library for the profile.

### **Profile**

Specifies the name of the profile. The name can be up to 30 alphanumeric characters and cannot include a space. You can also use the underscore character ( \_ ).

### **Location**

Specifies the library as defined in Horizon.

## Borrower Settings

Specifies settings specific to patron authentication.

### **Borrower Authentication Field 1**

Specifies the field to display for patron authentication. This is typically the borrower's barcode, although it could be the alternate ID or another uniquely identifying field.

### **Borrower Authentication Field 2**

Specifies a different field uniquely identifying field if a secondary login field is required.

### **Enable Reset PIN**

Turns the Forgot Password functionality on or off.

### **Enable Patron Self Registration**

Turns the functionality for patrons to register themselves for a library card.

## Fee Payment Settings

Specifies how payment request logs are recorded in Horizon.

### **Library Department**

Specifies the library department that will be recorded in payment logs when requests are made with this profile.

### **Workstation ID**

Specifies the workstation ID that will be recorded in payment logs when requests are made with this profile.



**Cash Drawer ID**

Specifies the cash drawer ID that will be recorded in payment logs when requests are made with this profile.

**User ID**

Specifies the user ID that will be recorded in payment logs when requests are made with this profile.

**Management Options**

You have these options:

Option	Description
Save	Saves your changes to the profile.
Reload	Reloads the profile's current configuration values from the server without saving changes.
Cancel	Returns to the previous page without saving any changes.

**Related topics**

[Turning off HIP dependency on page 52](#)

[Fields: HIP Configuration — Don't Use HIP on page 52](#)

## Configuring CAS single sign-on

The Single Sign-on Setup page allows you to take advantage of a Central Authentication Service (CAS) server for authentication. From this page you can manage each of your CAS-trusted URLs. For more information about the fields on this page, see [Fields: Single Sign-on Setup on page 57](#).

**To configure CAS single sign-on URLs**

1. Log in to the Admin console.
2. Click **Single Sign-on Setup** in the Navigation pane.
3. Do one of the following:

- Click **Add URL** to create a new Single Sign-on URL.  
Fill in the **CAS Server URL** and **CAS Service ID**, then click **Save**.
- Click **Edit** in the row of a Single Sign-on URL that you want to edit.  
Make necessary changes and click **Save**.
- Click **Delete** in the row of a Single Sign-on URL that you want to delete.  
The Single Sign-on URL is deleted.

**Note:** For more details about the fields you encounter while adding or editing a Single Sign-on URL, see [Fields: Create/Edit Single Sign-on URL](#) on page 58.

## Fields: Single Sign-on Setup

Single Sign-on Setup allows you to manage your trusted CAS URLs.

### Single Sign-on server list

Displays a list of all Single Sign-on URLs that may be used with Web Services.

**Important:** Only the URLs listed in this table may be used for single sign-on authentication.

The list displays this information:

Column	Description
CAS Server	Displays the URL to the CAS server that is running single sign-on services.
CAS Service ID	Displays the URL to the Web Services instance that is using this CAS server.

### Management Options

Option	Description
Add URL	Allows you to create a new Single Sign-on URL. For more information see <a href="#">Configuring CAS single sign-on</a> on page 56.
Edit	Allows you to edit an existing Single Sign-on URL. For more information see <a href="#">Configuring CAS single sign-on</a> on page 56.

Option	Description
Delete	<p>Allows you to delete a Single Sign-on URL from Web Services.</p> <p><b>Important:</b> Deleting the URL happens immediately upon clicking <b>Delete</b>; no warning message displays.</p>

## Fields: Create/Edit Single Sign-on URL

In order for single sign-on to function, you must add a valid **CAS Server URL** and **Service ID**.

### Property

Displays the CAS Server label.

### URL

Specifies the URL for the CAS server that will be used for single sign-on.

**Important:** The URL must use the SSL/TLS protocol and should be a fully qualified URL.

**Important:** If this URL will be used for BLUEcloud Central logins, you need to add `/cas` to the end of the URL.

### CAS Service ID

Specifies the URL to the Web Services instance that will be using the CAS server. Typically, this is the base URL to this instance of Web Services. For example, *http://testlibrary.sirsidynix.com/hzws*.

### Borrower Table Column

Specifies the column in the Horizon Borrower Table that matches the CAS validation field. Make sure you choose a column in which the values are unique; otherwise, the CAS log in will produce an error.

**Important:** The value entered in the CAS Service ID field overrides the Borrower Table Column. To use the Borrower Table Column, remove any values from the CAS Service ID field.

### Version

Specifies the CAS version to use for logins. Typically, you will use the CAS version that is supported by your server.

**Note:** If you need to maintain compatibility with the `user/patron/login` and `security/loginUserCAS` actions, use CAS 1.0.

**Note:** If you are connecting to BLUEcloud Central, you can use either CAS 2.0 or CAS 3.0, depending on your server.

**Type**

Specifies the user type that will be using this URL for logins. Specifying the type can speed up login by excluding different types of SSO logins. You can use Both to allow all types of SSO logins to be included.

**Management Options**

Option	Description
Save	Saves the new URL (creating) or saves changes to the existing URL (editing).
Cancel	Returns to the previous page without saving any changes.

**Related topics**

[Configuring CAS single sign-on on page 56](#)

[Fields: Single Sign-on Setup on page 57](#)

## LDAP Setup

Web Services allows you to specify one or more LDAP servers to authenticate users as they make Web Services client requests.

See the following topics for more information:

### About LDAP Authentication

The Lightweight Directory Access Protocol (LDAP) provides the ability to search and manage data in a network-accessible directory service. An LDAP service is commonly used to store data about users, such as the user's name, contact information, department, and so on. It can also be used as a common source for user authentication (for example, allowing multiple applications to validate login credentials, such as a user ID and password).

If your library already uses LDAP authentication for your OPAC, you will likely want to configure the same LDAP servers for use with Web Services.



In order to use LDAP authentication in Web Services, you must supply a Web Auth ID as part of the patron record in the ILS for each library user that will authenticate using LDAP. Contact SirsiDynix Customer Support if you need help configuring or importing Web Auth IDs.

The Web Auth ID for a patron record must be the same as the value of the *Search Attribute* (for more information, see [Fields: Add/Edit LDAP Server on page 63](#)) for that user in the LDAP directory (using either the same case or all uppercase). Understanding how Web Services uses LDAP will help to illustrate.

### Example of a Web Services and LDAP exchange

Web Services login requests require a login token (a user ID, for example) and a password for a user. Say, for example, that a client needed to authenticate Sally Smith whose user ID is *ssmith*.

If you configure LDAP servers in the Web Services Admin, when Web Services receives a request to authenticate or log in a user, it will attempt to contact the first LDAP server in the list. It first searches for the user using the Search Attribute you specify for the server and the login token in the request, for example *uid=ssmith*.



If the LDAP server does not allow anonymous searching, Web Services attempts to bind (log in) to the server before searching.

If it finds an entry for *ssmith*, it uses the distinguished name for that LDAP entry and the password supplied in the request to attempt to bind to the directory as that user.

If the bind succeeds, Web Services then uses the value of the *Search Attribute* (in this case, the value of the *uid* attribute in the directory response) to look for a user in the ILS with *ssmith* as the Web Auth ID.

Case is significant in this exchange. If the LDAP directory reports the value as *SSmith*, the Web Services software searches for a patron record with the Web Auth ID of *SSmith*. If no match is found, Web Services tries to match a Web Auth ID of *SSMITH*. If the Web Auth ID for the patron record is entered as *ssmith* (all lowercase), it will not match.

If the user is not found in the first LDAP directory, Web Services tries the next LDAP server and so on until it succeeds or until it has tried all LDAP servers.

If Web Services is unable to connect to an LDAP server, it will log an error in the *hzws* log (see [Examining log files on page 86](#)).

By default, if authentication fails for all LDAP servers, Web Services will attempt to authenticate the user with the ILS. This allows you to authenticate users who may exist only in the ILS and not on LDAP servers. If you want Web Services to use only LDAP authentication, enable the LDAP Only Authentication option (for more information, see [Fields: LDAP Setup on page 62](#)).



If LDAP is taking too long to fail the authentication, you can change the timeout values (see [Changing the LDAP Timeout Settings on page 62](#)).

## Managing LDAP Server Connections

The LDAP Setup page lets you specify and manage LDAP servers used by Web Services for user authentication and login.

Each new server you add to the list appears at the top. The order of servers in the list determines the order that Web Services will use as it authenticates users. That is, when a request is made to authenticate or log in a user, Web Services will contact the first LDAP server in the list. If authentication fails, it will try the next server in the list, and so on until it successfully authenticates or has tried all servers.

By default, if authentication fails for all LDAP servers, Web Services will attempt to authenticate the user with the ILS. If you want Web Services to use only LDAP authentication, enable the LDAP Only Authentication option.

For more information about the fields on this page, see [Fields: LDAP Setup on page 62](#).

### To add, edit, and remove LDAP Server Connections

1. Log in to the Admin console.
2. Click **LDAP Setup** in the Navigation pane.

The software displays the list of currently configured LDAP servers.

3. Do one of the following:
  - Click **Add LDAP Server** to create a new LDAP server.  
Fill in the required fields, and then click **Save**.
  - Click **Edit** in the row of a LDAP Server that you want to edit.  
Make necessary changes and click **Save**.

- Click **Delete** in the row of a LDAP server that you want to delete.

The LDAP server is deleted.

For more details about the fields you encounter while adding or editing a Single Sign-on URL, see [Fields: Add/Edit LDAP Server on page 63](#).

## Changing the LDAP Timeout Settings

If login requests through LDAP take too long to fail when the user is not matched in the LDAP repository, you can change the timeout value.

### To change the LDAP timeout settings

1. Log in to the Admin console.
  - a. Click **LDAP Setup** in the Navigation pane.
 

The software displays the list of currently configured LDAP servers.
  - b. Do one of the following:
    - Click **Add LDAP Server** to create a new LDAP server.
    - Click **Edit** in the row of a LDAP Server that you want to edit.
2. In the **Connect Timeout** field, enter the amount of time in milliseconds when Web Services for Horizon stops attempting to authenticate to the LDAP server.
3. In the **Read Timeout** field, enter the amount of time in milliseconds when Web Services for Horizon stops waiting for a reply from the LDAP server.
4. When you have finished, click **Save**.

## Fields: LDAP Setup

The LDAP Setup page lets you specify and manage LDAP servers used by Web Services for user authentication and login.

Each new server you add to the list appears at the top. The order of servers in the list determines the order that Web Services will use as it authenticates users. That is, when a request is made to authenticate or log in a user, Web Services will contact the first LDAP server in the list. If authentication fails, it will try the next server in the list, and so on until it successfully authenticates or has tried all servers.

By default, if authentication fails for all LDAP servers, Web Services will attempt to authenticate the user with the ILS. If you want Web Services to use only LDAP authentication, enable the LDAP Only Authentication option.

### LDAP server list

Displays a list of all the LDAP servers that Web Services will use to authenticate users.

The list displays this information:

Column	Description
LDAP Host	Displays the host name or IP address for the listed server.
Base Distinguished Name	Displays the base distinguished name specified for the listed server.

### Management Options

Option	Description
LDAP Only Authentication	<p>Specifies how Web Services should handle user authentication. Click <b>disable</b> or <b>enable</b> to toggle this setting.</p> <p><b>disabled:</b> If LDAP authentication fails, attempt to authenticate with the ILS server. Use this option if you have some users that validate through LDAP and others that are not part of LDAP directories.</p> <p><b>enabled:</b> Only authenticate with LDAP (more secure).</p> <p><b>Note:</b> This option only appears when there are servers in the list.</p>
Add LDAP Server	Allows you to create a new LDAP server. For more information see <a href="#">Managing LDAP Server Connections</a> on page 61.
Edit	Lets you edit the selected server.
Delete	Deletes the selected server configuration and removes it from the list.

## Fields: Add/Edit LDAP Server

Add/Edit LDAP Server lets you configure connection properties for an LDAP server.



**LDAP Host**

Specifies the host name or IP address of the LDAP server. For example, *ldap.example.org* or *10.1.1.116*.

This field is required.

**Port**

The port number for the LDAP service on the server. The default LDAP port is 389, or 636 for LDAP over SSL. If you are using Microsoft Active Directory, this would typically be the port for the global catalog. This must be a valid port number (between 1 and 65535).

This field is required.

**SSL Authentication**

Specifies whether Web Services should attempt to connect to the LDAP server using the *ldaps:* scheme. Select Yes if the LDAP directory requires SSL. The default value is No.

**Note:** By default, Web Services accepts all security certificates. If you want to validate certificates, you will need to edit the `applicationContext.xml` file in the WEB-INF directory and change `acceptAllCerts` to `false`. You must also import certificates using a tool such as *keytool* or *javacpl*.

For more information on client and server authentication, refer to the documentation for Apache Tomcat and Java. Managing a Tomcat trust store is beyond the scope of this document.

**Base Distinguished Name**

Specifies the base distinguished name for entries in the LDAP directory. For example, for the user *uid=myuser,ou=student,dc=ldap,dc=example,dc=org*, the base distinguished name would be *ou=student,dc=ldap,dc=example,dc=org*.

Web Services will do a recursive tree search from this level of the directory hierarchy, including any referrals returned by the directory.

This field is required.

**Search Attribute**

Specifies the unique attribute that distinguishes an entry in the directory. Commonly, this is the *uid* attribute.

For example, in a directory with unique entries such as *uid=ssmith,ou=student,dc=ldap,dc=example,dc=org*, *uid* would be the value to use for Search Attribute.

This field is required.

### **Distinguished Name for BIND**

Specifies the full distinguished name for a named entry in the directory. For example, *uid=searchuser,ou=admin,dc=ldap,dc=example,dc=org*.

If your LDAP directory requires BIND (that is, it requires a client to authenticate before searching and it does not allow anonymous searching), you must specify a valid distinguished name for bind and provide the password for that entry in BIND Password.

This field is optional. Leave this field blank if the LDAP directory allows anonymous searching.

### **BIND Password**

Specifies the password for the named entry you entered in **Distinguished Name for BIND**.

This field is optional. Leave this field blank if the LDAP directory allows anonymous searching.

### **Confirm BIND Password**

Confirms that the **BIND Password** was entered correctly. Retype the BIND password.

**Note:** If the values of **BIND Password** and **Confirm BIND Password** don't match exactly, the LDAP server will not be saved.

This field is required if you have typed a password into **BIND Password**.

### **Connect Timeout**

Specifies the amount of time in milliseconds from attempting to authenticate to the LDAP server without a response until the Web Services for Horizon server stops attempting and logs an error to the LdapAuthenticator log. The default Connect Timeout interval is 500 milliseconds.

### **Read Timeout**

Specifies the amount of time in milliseconds from sending a request to the LDAP sever without a response until the Web Services for Horizon server stops attempting and logs an error to the LdapAuthenticator log. The default Read Timeout interval is 5000 milliseconds.

### **Borrower Table Column**

Specifies the column in the Horizon Borrower Table that matches the LDAP validation field.

Management Options

Option	Description
Save	Saves the changes you have made to the LDAP server configuration.  <b>Note:</b> If you navigate somewhere else in the Admin console before clicking <b>Save</b> , your changes will be discarded.
Cancel	Closes the Add/Edit LDAP Server page without saving the changes and returns you to LDAP Setup.

Related topics

[About LDAP Authentication on page 59](#)

[Fields: LDAP Setup on page 62](#)

[LDAP Setup on page 59](#)

# Securing endpoints

Endpoint Security gives your library an added level of Web Services security. With Endpoint Security you can turn off specific resources for different clients by user roles and web service methods.

This section includes these topics:

- [Managing endpoint security ..... 66](#)
- [Fields: Endpoint Security ..... 67](#)
- [Fields: Endpoint Security Configuration ..... 68](#)

## Managing endpoint security

The Endpoint Security page lets you restrict the access of specific Web Services for Horizon resources by a resource's methods.

### To enable or disable an endpoint

1. Log in to the Admin console.
2. Choose **Endpoint Security** in the Navigation pane.

A table of all the endpoints in your Web Services instance displays.



3. Use the filters to narrow the list so you can easily locate the endpoint you want to enable or disable.
4. Click the **Change** button on the same line as the endpoint.

The Endpoint Security Configuration page opens.

5. Click the checkbox next to the method or methods to either enable or disable the endpoints.
6. When you have finished, click **Save**.
7. Click **Close** to return to the Endpoint Security page.

The page closes and the filtered page displays with all of the disabled endpoint methods crossed out.

**Related topics**

[Managing endpoint security on page 66](#)

[Fields: Endpoint Security on page 67](#)

## Fields: Endpoint Security

The Endpoint Security pages lets you manage which web service methods are available to the clients in your library system. This lets you turn off features that are not used by the client or by specific types of users of a feature.

**Endpoint list**

Displays the list of endpoints available in Web Services for Horizon. You cannot sort the list, but you can filter the list to quickly locate the endpoints you want to enable or disable.

The Endpoint list includes these columns:

Column	Description
Client ID	Displays the client that the endpoint belongs to.
URL	Displays the path to the endpoint.
ROLE	Displays the privilege needed to access the endpoint.
Method	Displays the method or methods allowed for the endpoint. The endpoints are enable and disabled according to the method. Methods that are disabled are crossed out.

Column	Description
Change	Lets you modify the security settings for the corresponding endpoint.

### Management options

The management options at the top of the list let you filter the list to show endpoints depending on specific criteria. The filters listed below act together with a Boolean AND—the list displays only those endpoints that match all of the filter conditions.

Option	Description
Client ID Filter	Displays only the client ID that you select from the list.
URL Filter	Displays only the endpoints in which a portion of their URL includes the string in the text box.
Role Filter	Displays only the endpoints of the selected role. <b>Note:</b> To clear the role filter, click the selected role.
Reset	Removes all of the specified filters to show all endpoints.

### Related topics

[Securing endpoints on page 66](#)

[Managing endpoint security on page 66](#)

[Fields: Endpoint Security Configuration on page 68](#)

## Fields: Endpoint Security Configuration

The Endpoint Security Configuration page lets you specify which endpoints can be accessed, the methods that can be used, and the fields that can be displayed or edited by staff and patron users. The elements that can be configured changes depending on the endpoint, so while the methods can be secured on all of the available endpoints, not all of the endpoints include fields.

The Endpoint Security Configuration page is divided by endpoint, method, fields, and policy.

**Endpoint**

Displays the details of the currently selected endpoint.

Column	Description
Client ID	Displays the client that the endpoint belongs to.
URL	Displays the path to the endpoint.
Role	Displays the privilege needed to access the endpoint.

**Method options**

Lists the methods that can be used to access the endpoint. A check in the box indicates that this endpoint can be accessed through the method.

**Field options**

Lists the fields that are available in the endpoint. Not all endpoints have fields associated with them.

Column	Description
Field Name	Displays the name of the field that can be configured.
Value	<p>Specifies whether users have access to the field contents, and in some cases, whether the field contents can be edited by the user. You have these options:</p> <ul style="list-style-type: none"> <li>• Hide—The field is disabled and cannot be accessed through Web Services.</li> <li>• Visible—The field is readable to users but cannot be edited through Web Services.</li> <li>• Editable—The field is readable and its contents can be modified through Web Services.</li> </ul> <p><b>Note:</b> This option may not be available for all fields.</p>

**Policy options**

Lets you enable access to resources that contain a given policy. For example, you can hide a block detail line from a specific policy, such as a staff-only note.

**Note:** If no policy keys are listed, all of the policies for the endpoint are enabled and are visible.

Column	Description
Policy Key	Displays the name of the policy.  The drop-down list lets you select from the policies associated with the endpoint to add to the list.
Value	Specifies whether users have access to the policy contents, including the ability to edit the contents. You have these options for each policy: <ul style="list-style-type: none"> <li>• Hide—The policy is disabled and cannot be accessed through Web Services.</li> <li>• Visible—The policy is readable to users but cannot be edited through Web Services.</li> <li>• Editable—The policy is readable and its contents can be modified through Web Services.</li> </ul>
Remove	Deletes the associated policy from the list.
Add	Adds the selected Policy Key and Value to the list as a new policy.

### Related topics

[Securing endpoints on page 66](#)

[Managing endpoint security on page 66](#)

[Fields: Endpoint Security on page 67](#)

## Denying Staff Access

The Staff Deny List lets you restrict staff access to Web Services from specific staff accounts. The list is maintained in a text document (`staffDeny.txt`) that is stored on the server. You can download the file to edit the list or upload a new document to replace the current list of restrictions.

### To deny access to a staff user

1. Log in to the Admin console.
2. Choose **Staff Deny List** in the Navigation pane.

The Staff Deny List page opens. For more information, see [See "Fields: Staff Deny List"](#)

3. If you do not have a copy of the `staffDeny.txt` document, click the **staffDeny.txt** link to download it.

**Note:** The `staffDeny.txt` file is blank until you upload a file with staff user IDs.

4. In the text file, type the user IDs of each staff member you want to restrict from logging in. Enter each user ID on a new line.
5. Save the file.
6. In the Admin console, click **Choose File**.

The Open dialog box displays.

7. Locate the `staffDeny.txt` file you edited or created, then click **Open**.
8. Click **Save**.

The file is uploaded to the system. The restrictions should come into effect immediately.

## Fields: Staff Deny List

Web Services for Horizon Admin console > Staff Deny List

Staff Deny List lets you specify user IDs to prohibit them from logging in to Web Services for Horizon.

### Download

#### **staffDeny.txt**

Downloads the document that currently lists the staff users that are excluded from logging in to Web Services.

**Note:** The `staffDeny.txt` file is blank until you upload a file with staff user IDs.

### Upload

#### **Choose File**

Lets you select the `staffDeny.txt` file you want to be used to restrict logins. This file should be a text file that lists the Web Services user IDs that you want restricted on separate lines.



## Whitelisting a Horizon table

Policy Whitelist Settings specifies the Horizon tables that are available to access through Web Services for Horizon. The lower list includes all of the tables, with their Web Services policy names, that are necessary for Web Services to fully function. The upper table lets you add any other table in your system so that they can be accessed through Web Services. Adding a table to the whitelist lets Web Services read the configuration settings in the table. It does not allow Web Services to change the configurations set in the tables.

### To add a Horizon table to the profile whitelist

1. Click **Policy Whitelist Settings** in the Navigation panel.
2. In the **Table Name** drop-down list, select the Horizon table you want Web Services for Horizon to have access to read.
3. If you want to make policy keys accessible to Web Services, type the name of the Horizon table column in the Policy Key Column(s) field.

**Note:** To add multiple policy keys, separate each column name with a colon, such as, "column\_a:column\_b:column\_c".

4. Click **Add** when you want to add another table as a profile in Web Services.

### To delete a Horizon table from the profile whitelist

1. Click **Policy Whitelist Settings** in the Navigation panel.
2. Click **Delete** for the table you want to remove from the whitelist.

## Fields: Policy Whitelist Settings

Specifies the Horizon tables that are available to access through Web Services for Horizon. The lower list includes all of the tables, with their Web Services policy names, that are necessary for Web Services to fully function. The upper table lets you add any other table in your system so that they can be accessed through Web Services. Adding a table to the whitelist lets Web Services read the configuration settings in the table. It does not allow Web Services to change the configurations set in the tables.

 Adding large tables to the whitelist can result in poor performance or cause the system to halt while Web Services gathers all of the entries in the table.

You have these options:

Setting	Description
Table Name	Specifies the table from your Horizon system that you want to make available to Web Services as a policy.
Policy Key Column(s)	Specifies the table columns that you want to make available to Web Services as keys.
Add	Adds the currently selected table to the policy whitelist.
Save	Saves any edits that have been made in the Policy Key Column(s) field.
Remove	Removes the table from the policy whitelist.

## Managing the log files

Web Services for Horizon keeps logs on a variety of interactions within Web Services. You can use these log files to locate and fix any bugs that you might be experiencing in your implementation. You can also enable a debug mode for specific loggers to display more data that can help you isolate issues in the code.

This section includes these topics:

<a href="#">Viewing Web Services Logs</a> .....	73
<a href="#">Changing the logging level</a> .....	74
<a href="#">Fields: Logs</a> .....	75

### Viewing Web Services Logs

The Admin console provides the capability to access and view the log files for Web Services.

## To view Tomcat logs

1. Log in to the Admin console.
2. Choose **Logs** in the Navigation pane.

A list of all the logs for your Web Services instance displays. The system looks in the Tomcat logs directory for logs that start with your Web Services instance name and end with the .log extension.

**Important:** If the Logs option does not display, the path to the default log directory is incorrect and needs to be updated. To update the path, change the value for the `logging.directory` property in the `admin-settings.properties` file of the Web Services instance, for example:

```
<tomcat\webapps\hzws>\WEB-INF\classes\admin-settings.properties
```

where `<tomcat\webapps\hzws>` is a path to your instance of Web Services.

3. Choose a log name from the list to open or download the log file to your computer.

**Note:** Although the requests log may appear in the logs list, it may be empty if you have not enabled request logging. For more information, see [requests log](#) on page 87.

## Related topics

[Managing the log files](#) on page 73

[Changing the logging level](#) on page 74

## Changing the logging level

You can toggle between the INFO and DEBUG log levels. The Log Level column displays the current logging status in the Apache Tomcat server.

1. Log in to the Admin console.
2. Choose **Logs** in the Navigation pane.

A table of all the loggers for your Web Services instance displays below the list of log files.

3. Choose **Change Level** to toggle the level of the current logging level.

**Note:** Choosing Change Level switches the logging level from the current level to DEBUG. When the level is DEBUG, Change Level sets the logging level to INFO. From Web Services, you cannot change the logging level to OFF or any other level besides DEBUG or INFO. To change logging to a different level other than DEBUG or INFO, you must change it from within Apache Tomcat.

**Related topics**

[Managing the log files on page 73](#)

[Viewing Web Services Logs on page 73](#)

[Fields: Logs on page 75](#)

## Fields: Logs

Logs lets you view or download Tomcat server logs for your instance of Web Services. You can also enable the debug level of logging for specific loggers.

**Log list**

Displays the names of all of the logs for your Web Services instance. The admin lists all logs that start with your Web Services instance name and end with the “.log” extension that are in the Tomcat logs directory. By default, this is in C:\Program Files\Apache Software Foundation\Tomcat <version>\logs.

Click on a log to view or download it. The log is a simple text file.

**Logger list**

Displays the loggers that create the logs. This list lets you view and change the level at which the loggers report issues that they find.

Column	Description
Logger Name	Displays the name of the logger.
Log Level	Specifies the current level of logging set in the Tomcat server, including OFF. For more information about the log levels, see your Apache Tomcat documentation.

**Management Options**

Option	Description
Delete Contents	Removes the logging data from the corresponding file. The log file remains in the Logs list, but is empty until the logger starts adding data to the file.  <b>Important:</b> The deleted content cannot be restored.

Option	Description
Delete File	<p>Permanently removes the file from the list. This option appears only for compressed files (that is, .zip and .gz files).</p> <p><b>Important:</b> The deleted file cannot be restored.</p>
Change Level	<p>Toggles between the DEBUG and INFO logging levels.</p> <p><b>Important:</b> The Log Level column displays the current logging status in the Apache Tomcat server. Choosing Change Level switches the logging level from the current level to DEBUG. When the level is DEBUG, Change Level sets the logging level to INFO. From Web Services, you cannot change the logging level to OFF or any other level besides DEBUG or INFO. To change logging to a different level other than DEBUG or INFO, you must change it from within Apache Tomcat.</p> <p><b>Note:</b> There is very little meaningful difference between INFO and OFF.</p>

**Related topics**

- [Managing the log files on page 73](#)
- [Viewing Web Services Logs on page 73](#)
- [Changing the logging level on page 74](#)

## Managing offline assets

The PrepareOffline call lets clients prepare a file that contains a list of delinqObject entries. These objects are used when a client is not connected to the ILS to allow users to continue to make transactions, which are recorded in the ILS when the client is once again connected. Offline Assets lets you view the properties of an offline asset file and delete any offline asset that is no longer needed.

This section includes these topics:

- [Viewing the properties of an offline asset .....77](#)
- [Deleting an offline asset ..... 77](#)
- [Fields: Offline Assets ..... 78](#)

## Viewing the properties of an offline asset

The offline assets file list displays each asset file that has been created by any of the clients in the system. Each asset file entry is listed by name in alphabetical order. You can expand the asset file entry to view the Library from which the file was created, the fields that were included when the file was created, and the date and time when the file was last modified.

### To view file properties

1. Log in to the Admin console.
2. Click **Offline Assets** in the Navigation pane.  
The software displays the list of offline asset files.
3. Click the filename or the arrow to the right of the filename.  
The Library, Include Fields, and Last Modified fields are displayed.

### Related topics

[Managing offline assets on page 76](#)

[Deleting an offline asset on page 77](#)

[Fields: Offline Assets on page 78](#)

## Deleting an offline asset

You can delete any of the offline assets when it is no longer needed.



Be careful when you delete an online asset file. There will be no confirmation when you delete one or more files and you cannot undo a deletion.

### To delete an offline asset

1. Log in to the Admin console.
2. Click **Offline Assets** in the Navigation pane.  
The software displays the list of offline asset files.
3. Do one of the following:

- Click the check box next to each asset file you want to delete.
  - Click **Select All** to select every asset file.
4. Choose **Delete Selected** to delete each of the selected files.

**Related topics**

- [Managing offline assets on page 76](#)
- [Viewing the properties of an offline asset on page 77](#)
- [Fields: Offline Assets on page 78](#)

## Fields: Offline Assets

The Offline Assets page lets you view and delete the files that are created and modified for offline transactions. The file entries are listed in alphabetical order and can be expanded to view their properties.

**Offline Assets list**

Displays a list of all offline asset files that have been created for offline transactions.

The list displays this information:

Column	Description
Select	Lets you choose a file to delete.
Asset File	<p>Displays the name of the asset file.</p> <p>By clicking the name or the arrow to the right of the name, you can view the properties of the file:</p> <ul style="list-style-type: none"> <li>• Library—Displays the name of the library where the offline transaction was created.</li> <li>• Include Fields—Displays the fields that are included in the asset file.</li> <li>• Last Modified—The date and time when the file had been most recently added to or modified.</li> </ul>

**Management Options**



Option	Description
Select All	Lets you mark the checkbox of each asset file in the list.
Delete Selected	<p>Lets you delete each marked asset file in the list.</p> <p><b>Important:</b> Deleting the asset files happens immediately upon clicking <b>Delete</b>; no warning message displays and the files cannot be recovered.</p>

## Allowing access to the SDK

The Web Services for Horizon and Symphony Software Development Kit (SDK) includes reference material and instructions for programming to Web Services for Horizon and Symphony. You can access the SDK at the root level of the Web Services at `sdk.html`. By default, the SDK is available for you and others on your network to access. However, in Manage SDK you can disable the SDK from the Admin console to restrict others from accessing it.

### Enabling the SDK

1. Log in to the Admin console.
2. Click **Manage SDK** in the Navigation pane.

The Manage SDK page opens. For more information, see [Fields: Manage SDK on page 79](#).

3. Click the **Enable SDK** check box.
4. Click **Save**.

**Note:** When the SDK is enabled, you can click the **Link to SDK** link to open the SDK.

### Fields: Manage SDK

The Manage SDK page lets you enable or disable access to the Web Services for Horizon and Symphony Software Development Kit (SDK) and open the SDK when it is enabled.



**Enable SDK**

Makes the SDK documentation available for users to view.

**Link to SDK**

Opens the SDK documentation in a new tab in the browser when the SDK is enabled.

## Customizing or localizing labels and messages

You can create a list of labels to replace those that Web Services for Horizon and Symphony uses by default. Your changes are retained through any upgrades to Web Services that may follow. In addition, you can create translations for labels that are used whenever Web Services responds to requests that include that language.

When sending a request, include the language code in the `x-sirs-locale: en-US` header.

### To create a customized labels properties file

- Do one of the following:
  - To customize labels in the Web Services Admin Console, in the `WEB-INF/classes` directory, create a text file named `adminResource_lg_lc_custom.properties` where *lg\_lc* is the language/locale code for the labels.
  - To customize exception messages, in the `WEB-INF/classes` directory, create a text file named `IlsWsExceptionResource_lg_lc_custom.properties` where *lg\_lc* is the language/locale code for the labels.
- Locate the resource file for the customized file you are creating:
  - The administration labels are located in `WEB-INF/classes/adminResources.properties`.
  - The exception messages are located the `IlsWsExceptionResource.properties` file in `WEB-INF/lib/ilsws-util.jar`. (You will need an archive extraction tool, such as 7-Zip to open the file.)

**Important:** You will not edit these files. Any changes made to these files will be overwritten the next time you upgrade Web Services.

- Open the resource file and locate the string you want to customize.

Each line consists of a key/value pair, as shown in this example:

```
unableToLogin=Unable to log in.
```

4. Copy the key portion ("unableToLogin" in the example) of the line.
5. Paste the key into the `adminResource_Lg_Lc_custom.properties` or `ILSWsExceptionResource_Lg_Lc_custom.properties` that you created in step 1.
6. Type "=" and the string value for the customized message or label.

For example:

```
unableToLogin=Impossibile fare il log in.
```

7. When you have finished, save the file.
8. Restart Tomcat to activate the changed labels or messages.

# Uninstalling Web Services

When you install Web Services, the installer creates a directory named `_Web Services` for `Horizon_installation` in the target Tomcat directory. That directory includes an executable named `Uninstall Web Services for Horizon`.

To uninstall Web Services, simply launch the uninstaller executable. Any files you added or modified after installation will not be removed. The uninstaller will list files and directories that could not be removed so that you may remove them manually if you desire.



You may need to run the uninstaller as a system administrator user (Windows) or as the root user (Linux).



When installing on Windows, the installer also registers the uninstaller so that you can run it using Add or Remove Programs.

# Troubleshooting

This section provides information about where to look for logs to detect problems you may encounter while running Web Services. It also provides troubleshooting information about common errors that you may encounter while using Web Services.

See the following topics for more information:

<b>General Troubleshooting</b> .....	<b>83</b>
Restoring access if you cannot log in .....	83
Starting up Tomcat .....	84
Troubleshooting connection issues .....	85
Verifying that Web Services is running .....	85
<b>Examining log files</b> .....	<b>86</b>
catalina logs .....	87
requests log .....	87
hzws log .....	88
BlackBox log .....	89
<b>Troubleshooting common errors</b> .....	<b>89</b>
BeanCreationException: Error creating bean .....	90
BindException: Address already in use: JVM_Bind .....	90
Context initialization failed .....	90
File permissions errors .....	91
Initial LDAP bind failed .....	91
listenerStart error .....	92

## General Troubleshooting

This section describes issues that you can encounter while using Web Services and gives instructions about actions you can take in each scenario to try to resolve the problem.

See the following topics for more information:

### Restoring access if you cannot log in

The username and password for the Admin console are stored in a file called `admin-settings.properties` in the Web Services instance, for example:

<tomcat base path\webapps\hzws>\WEB-INF\classes\admin-settings.properties

where <tomcat base path\webapps\hzws> is the path to your Web Services instance.

If you forget the username, you can simply look in this file to remind you. The password, however, is encrypted.

If you forget the password, you can delete the password in this file, save the file, and restart Tomcat.

When you next log in to the Admin console, the Admin console detects that the password is missing. The Admin console will allow you to log in using the default password, *admin*. Be sure to change the password once you log in.

## Starting up Tomcat

After you install Web Services you need to start the Tomcat service (Windows only) or Tomcat instance (Windows or Linux) before Web Services can start receiving requests from client applications. After starting Web Services, you can verify that they are running by using a couple of methods. If you did not install Tomcat as a Windows service, then you should follow the Windows instructions for starting up the Tomcat instance. For more information, see [Verifying that Web Services is running on page 85](#).

### Starting up the Tomcat Service (Windows only)

1. Open the **Local Services** window.
2. Locate *Apache Tomcat* <tomcat service name> in the lists of services, where <tomcat service name> is the name you specified for the Tomcat service when you installed Web Services.
3. Right-click the service in the row and select **Start**.

You can look at the status of a service in the **Status** column to verify that it is running. Services which are currently running display a status of **Started**.

### Starting up the Tomcat instance (Windows or Linux)

1. Ensure that you have changed your Java environment variable. For more information, see [Finding and setting Java environment variables on page 18](#). (Linux)
2. Open a command prompt (Windows) or terminal window (Linux).
3. Navigate to the Tomcat root directory for this instance of Web Services.
4. Run the `startup.bat` script (Windows) or `startup.sh` script (Linux) to start the Tomcat instance.

## Troubleshooting connection issues

The Admin console Status page reports the status of the Web Services connection to the ILS. If for some reason Web Services cannot connect, it will report “Offline”. For more information see [Fields: Status page on page 43](#).

Here are some reasons the connection may be offline:

Cause	Remedy
The database or ILS is not running.	Verify that the ILS and the database are running.
The database or ILS is inaccessible.	Verify that there are no firewalls blocking access. Inspect for port conflicts.
The hostname or IP address of the database may be incorrect.	Verify the hostname or IP address on the ILS Configuration page. For more information, see <a href="#">Fields: ILS Configuration on page 45</a> .
There is a problem resolving the hostname.	Verify that DNS is correctly resolving the hostname by using <code>nslookup</code> or a similar tool. For more information, see the documentation for your operating system.
The database port is incorrect.	Verify the port number on the ILS Configuration page. For more information, see <a href="#">Fields: ILS Configuration on page 45</a> .
There is a problem with the database login information.	Verify that valid values are used on the ILS Configuration page for Database Name, Database User, and Database User Password. For more information, see <a href="#">Fields: ILS Configuration on page 45</a> .

For additional tips and information about specific errors, see [Troubleshooting common errors on page 89](#).

## Verifying that Web Services is running

After you install Web Services and start Tomcat, you can verify that Web Services is running by pointing a Web browser to the Web Services Admin console (for more information, see [Accessing the Admin console on page 37](#)) and logging in (for more information, see [Logging in to the Admin console on page 39](#)).

If Web Services is running and properly configured, ILS Connection Status will display “Connected” and you will see version information for Web Services and for the ILS.

If you do not see the expected result, see [Troubleshooting common errors on page 89](#) for help with any errors that may have been logged.

Alternately, you can verify that Web Services is running by using a Web browser to send a version request to the URL for your service instance.

For example, if your Tomcat host name is *libraryapps.example.org* and you used the default port (8080) and the default application name (`hzws`), the URL for a version request would be:

```
http://libraryapps.example.org:8080/hzws/rest/standard/version
```

If Web Services is running and properly configured, the software will return an XML document with version information about Horizon and HIP (if you have entered HIP Connection information), for example:

```
<VersionResponse xmlns="http://schemas.sirsidynix.com/hzws/standard">
  <version>
    <product>HIP</product>
    <version>3.23.1_6655</version>
  </version>
  <version>
    <product>HzWs</product>
    <version>v5_0_4879M 2014-10-14 16:16:10</version>
  </version>
</VersionResponse>
```

If you do not see the expected result, see [Troubleshooting common errors on page 89](#) for help with any errors that may have been logged.

If network cards or firewalls in your network are configured to close connections that have been idle for some qualified time, you may also want to set the Keep Alive Timer after installation. For more information, see [Fields: ILS Configuration on page 45](#).

## Examining log files

Errors encountered while starting and running Web Services for Horizon are recorded in log files. Some of these log files are used only by Tomcat, while others are used only by Web Services for Horizon. These logs can be helpful in detecting and diagnosing problems. This section describes where to find the different types of log files, and details the information that you will find in each file. For more information about specific errors, see [Troubleshooting common errors on page 89](#).

See the following topics for more information:

## catalina logs

Errors encountered while starting Web Services are logged in the standard catalina log file. By default, catalina logs are created in the logs directory of your Tomcat installation, for example:

```
<Tomcat directory path>/logs/catalina.2018-11-04.log
```

In some cases, errors may also be logged to the localhost log in the Tomcat logs directory.



Because catalina logs are created and used only by Tomcat, please see the Tomcat documentation for more information about messages that occur in the catalina log files.

## requests log

Each request received by Web Services may be logged to a requests log in the Tomcat logs directory.

The requests log uses the name you specified for your Web Services instance. For example, if you used the default application name, *hzws*, when you installed Web Services, the requests log would be

```
<Tomcat directory path>/logs/hzws-requests.log
```

If instead you used, for example, *mylibraryws* as the application name, the hzws log file would be

```
<Tomcat directory path>/logs/mylibraryws-requests.log
```

The format of entries in this log may change in future revisions.

Requests logging is disabled by default. To enable requests logging, you must modify `logback.xml` in the Web Services classes directory.



Changes you make to `logback.xml` are not persistent across upgrades. If you enable request logging and later upgrade your instance of Web Services, you will need to restore the changes after upgrade.

### To turn on request logging in logback.xml

1. Open `<tomcat/webapps/hzws>/WEB-INF/classes/logback.xml` in a text editor (where `<tomcat/webapps/hzws>` is the path to your Web Services instance).



2. Locate the following logger elements:

```

<!-- to enable client request logging change OFF settings to INFO -->
<logger
name="com.sirsidynix.hzws.protocol.rest.handlers.HeaderHandler"
additivity="false">
  <level value="OFF"/>
  <appender-ref ref="REQUEST"/>
</logger>
<logger
name="com.sirsidynix.hzws.protocol.soap.handlers.HeaderHandler"
additivity="false">
  <level value="OFF"/>
  <appender-ref ref="REQUEST"/>
</logger>
<logger name="com.sirsidynix.ilsws.license.WSLicenseFilter"
additivity="false">
  <level value="OFF"/>
  <appender-ref ref="REQUEST"/>
</logger>

```

3. Change the level value from *OFF* to *INFO*:

```
<level value="INFO"/>
```

4. Save the changes to the logback.xml file.

5. Restart Tomcat.

## hzws log

Web Services runtime errors and information messages are logged in the hzws log in the Tomcat logs directory.

The hzws log uses the name you specified for your Web Services instance. For example, if you used the default application name, *hzws*, when you installed Web Services, the hzws log would be

```
<Tomcat directory path>/logs/hzws.log
```

If instead you used, for example, *mylibraryws* as the application name, the hzws log file would be

```
<Tomcat directory path>/logs/mylibraryws.log
```

You can access these log files through the Admin console. For more information, see [Viewing Web Services Logs on page 73](#).

## BlackBox log

Web Services for Horizon includes a logger for viewing all of the JSON requests and responses that are made in the system. The `blackbox.log` file logs these transactions. You can turn on the BlackBox transaction logger from within the `logback.xml` file.



Because the BlackBox logger creates a highly detailed log, you can use it to troubleshoot specific calls in a controlled environment over a limited time span. However, if you leave the BlackBox logger activated for an extended time period, the log files could easily grow to fill your server's hard drive.

### To activate the BlackBox logger

1. Open the `logback.xml` file in the `classes` directory.
2. Locate the following "BlackBox" logger element in the file.

```
<logger name="BlackBox" level="OFF" additivity="false">
  <appender-ref ref="blackbox"/>
</logger>
```

3. Change the level value from *OFF* to *DEBUG*.
4. Save the file.
5. Either wait about a minute for Tomcat to process the edited file or restart Tomcat.

After Tomcat has processed the file, the logging begins. As Web Services for Horizon runs requests, they are added to the `blackbox.log` file.

**Note:** The BlackBox logger does not log legacy web services transactions.

6. When you have finished logging transactions, disable logging by returning the logging level to *OFF* in the `logback.xml` file and saving it. The logging stops after Tomcat has processed the changes to the file.

## Troubleshooting common errors

This section describes some of the error messages you may encounter while using Web Services. Errors are recorded in various Web Services logs (see [Examining log files on page 86](#)).

See the following topics for more information:

## BeanCreationException: Error creating bean

This startup error indicates a Java incompatibility or configuration error.

### Possible Causes

- You are using a Java version earlier than 11.
- Required configuration values, such as host or port, are missing.

### Solutions

- Make sure you are using the correct Java version. For more information, see [Java software on page 4](#).
- Verify that the host name or IP address and port for the database are correct. For more information, see [Fields: ILS Configuration on page 45](#).

## BindException: Address already in use: JVM\_Bind

This startup error indicates that a port needed by Tomcat is already in use.

### Possible Causes

- One of the ports specified in the Tomcat `server.xml` configuration file (in the Tomcat `conf` directory) is already in use by another application or by another instance of Tomcat already running.

### Solutions

- If the port conflict is for HTTP (default 8080) or HTTPS (default 8443), you can reinstall and specify different ports that are not used, or you can modify the `server.xml` directly.
- If the port conflict is for server shutdown (default 8005) or AJP 1.3 (default 8009), you must modify `server.xml` to specify ports that are not used.

Refer to the Tomcat documentation for information about `server.xml`. Refer to your operating system documentation for information about troubleshooting port conflicts, including the use of the `netstat` command to view ports in use.

## Context initialization failed

This startup error typically indicates a Java incompatibility.

### Possible Causes

- This error is commonly caused by using an earlier version of Java (older than 11).

### Solutions

- Make sure you are using the correct Java version. For more information, see [Java software on page 4](#).

## File permissions errors

If you just upgraded to Tomcat 9, this could indicate improperly set Log On permissions.

### Possible Causes

- The Local Service account has been overridden.

### Solutions

- In the **Log On** tab of the Apache Tomcat Properties, select **Local System Account**.

## Initial LDAP bind failed

This error indicates a problem connecting to an LDAP server. The error includes the URL Web Services used to connect to the server.

### Possible Causes

- The server is inaccessible.
- Required configuration values, such as host or port, are invalid.
- The server does not allow anonymous searching, or the BIND distinguished name or BIND Password you specified are invalid.

### Solutions

- Make sure the server is available and is not blocked by firewalls or other network issues.
- Verify that the host name or IP address and port for the LDAP server are correct. For more information, see [LDAP Setup on page 59](#).
- Verify that the values for Distinguished Name for BIND and BIND Password are valid. For more information, see [LDAP Setup on page 59](#).

## listenerStart error

This startup error indicates a JAXB incompatibility. The service will fail to start.

### Possible Causes

- This error is commonly caused by using an earlier version of the JAXB API. JAXB 2.1 is required.

### Solutions

- Make sure you are using the correct Java version. For more information, see [Java software on page 4](#).

# Appendix A: Key Concepts

This section explains various Web Services concepts that are important to understand when configuring and managing Web Services.

See the following topics for more information:

## Web Services base URL

The base URL is made up of the host name and port for your Tomcat and the Web Services name that you specified when you installed Web Services.

For example, if your Tomcat host name is *libraryapps.example.org* and you used the default port (8080) and the default Web Services name (*hzws*), the base URL for your Web Services instance would be:

```
http://libraryapps.example.org:8080/hzws
```

# Appendix B: Advanced Tomcat configuration

The default Tomcat settings delivered with the installer are sufficient for most installations. The following JVM options are recommended when running Web Services as a single Tomcat instance:

```
-server  
-Xms128m -Xmx256m  
-XX:+UseParallelGC  
-Xss128k -XX:PermSize=128m
```

If you used the Tomcat distribution included in the Web Services installer, the `catalina.bat` (Windows) or `catalina.sh` (Linux) file has already been modified with these options.

If you are running multiple instances of Web Services in Tomcat, you need to increase the minimum and maximum heap size (`-Xms` and `-Xmx`) by 50–75% (depending on anticipated traffic) per additional Web Services instance. If you are running on a 64-bit architecture and you find response times to be slow or you receive an out-of-memory error, you may need to double the stack size (`-Xss`).

However, depending on your system's configuration, your library's requirements, and other factors, you may want different options entirely. Tomcat has many configuration options, including advanced settings for heap space, stack space, perm space, threading options, and many security options. For details on configuring advanced Tomcat settings, please see the Tomcat documentation.

# Appendix C: Managing Password Lockout

Staff and patron accounts are protected from hackers' brute force threats to access the accounts. A lockout system prevents hackers from easily cracking a password by locking the account from access after a specified number of failed attempts. Two levels of security can be implemented: a temporary lockout and a permanent lockout. These topics describe how to configure the account lockout feature and how the lockout can be cleared by patron and staff users.

For more information, see these topics:

<a href="#">Configuring password lockout</a> .....	95
<a href="#">Clearing the lockout cache</a> .....	96
<a href="#">Fields: Lockout Settings</a> .....	96

## Configuring password lockout

You can set up web services to lockout a user after a number of successive failed login attempts. There are two levels, temporary and permanent.

The temporary lockout occurs after a specified number of failed logins, and clears itself after a specified number of minutes where the user does not attempt to log in. After the time out expired, the user can try again.

The permanent lock is an absolute count. Each time the user fails a login, the count increments. When the maximum attempts is reached, login is disabled for that user until the user is reset, as explained in [Clearing the lockout cache on page 96](#).

### To configure password lockout

1. Log in to the Admin console.
2. Click **Lockout Settings** in the Navigation pane.
3. Enter the values for each lockout property. For more information, see [Fields: Lockout Settings on page 96](#).

**Note:** Setting any of the fields to "0" turns password lockout off for that user type.

4. When you have finished, choose **Save**.

### Related topics

[Appendix C: Managing Password Lockout on page 95](#)



[Clearing the lockout cache on page 96](#)

[Fields: Lockout Settings on page 96](#)

## Clearing the lockout cache

Both the temporary and permanent lockout caches are cleared when the user either logs in successfully using the same ID, using a different ID (such as with a barcode instead of the preferred ID), or using the "forgot my PIN" feature. Otherwise, an administrator can clear the lockout user's web services caches. When any of these remedies are completed, the user's lockout counters are reset to 0.

The temporary and permanent locks can be reset in a number of ways:

- The user successfully logs in.
- The user resets the password through the "Forgot Password" link.
- A library worker resets the lockout cache for all users by clearing the general lockout cache (for more information, see [Clearing the lockout cache on page 96](#)).
- An administrator restarts Web Services or resets all of the Web Services caches. This resets the lockout cache for all users.

Each of these reset actions resets the count for both the temporary and permanent locks.

The permanent lockout cache can also be reset by a staff user through the patron resource or staff resource. See the *Web Services for Horizon and Symphony Software Developers Kit* for more information.

### Related topics

[Configuring password lockout on page 95](#)

[Appendix C: Managing Password Lockout on page 95](#)

[Fields: Lockout Settings on page 96](#)

## Fields: Lockout Settings

You can set up web services to lockout a user after a number of successive failed login attempts. There are two levels, temporary and permanent.

The temporary lockout occurs after a specified number of failed logins, and clears itself after a specified number of minutes where the user does not attempt to log in. After the time out expired, the user can try again.

The permanent lock is an absolute count. Each time the user fails a login, the count increments. When the configured maximum is reached, login is disabled for that user until the lock is removed for that user or the locks are removed for all users.



Setting any of the fields to "0" turns password lockout off for that user type.

## Staff

Specifies the lockout settings for library worker accounts. The settings work the same as the Patron settings. Because of this, you can make the Staff lockout settings more or less restrictive, as needed.

### Attempts before lockout

Specifies the number of times the wrong password can be entered for the account before the account is temporarily blocked (for the time specified).

### Max attempts before total lockout

Specifies the number of times the wrong password can be entered for the account before the account is permanently blocked. A permanently blocked account must be reset by library system administrator.

### Time locked out before retry

The amount of time, in seconds, minutes, hours or days, that must pass before the user can log in with a successful user ID and password.

## Patron

Specifies the lockout settings for library worker accounts. The settings work the same as the Staff settings. Because of this, you can make the Patron lockout settings more or less restrictive, as needed.

### Attempts before lockout

Specifies the number of times the wrong password can be entered for the account before the account is temporarily blocked (for the time specified).

### Max attempts before total lockout

Specifies the number of times the wrong password can be entered for the account before the account is permanently blocked. A permanently blocked account must be reset by library system administrator.

**Time locked out before retry**

The amount of time, in seconds, minutes, hours or days, that must pass before the user can log in with a successful user ID and password.

## Buttons

**Remove all Locks**

Resets all of the counters of users' attempted logins to zero (0). This does not reset or affect the values in the Lockout Settings. Login locks can also be reset on an individual basis through your ILS.

**Related topics**

[Configuring password lockout on page 95](#)

[Clearing the lockout cache on page 96](#)

# Appendix D: Configuring Email Templates

This section includes these topics:

<a href="#">Configuring Checkout Receipt Email Template</a> .....	99
<a href="#">Configuring the Reset My PIN Template File</a> .....	101

## Configuring Checkout Receipt Email Template

Web Services for Horizon uses two files that together create the template the ILS uses to send checkout receipts via email. This topic contains information on how to customize these template files for use by your library. Both email template files are HTML-based. You can add to or edit the templates as you would any HTML file. The template files are found in the `WEB-INF/classes/emailTemplates/checkoutReceipts` directory on the web services server.



Your library system must have an email subsystem set up in the Horizon Client's Table Editor – `email_param` table to use this functionality. If you have a subsystem configured for emailing notice reports, the ILS will use this subsystem for emailing checkout receipts. For more information on setting up an email subsystem, contact SirsiDynix Customer Support.

If Web Services for Horizon cannot find the template files with the specified name, it will check the language directory appropriate to the patron's language for the default template files. If there are no template files in the appropriate language directory, Web Services for Horizon will check the `WEB-INF/classes/emailTemplates/checkoutReceipts` directory for files with the name specified in the **Template** field; if it cannot find the files, it will use the default template files delivered with Web Services for Horizon.

### The `.body` file

The `.body` file contains the template for email checkout receipts. The email message the ILS sends to patrons is based on the setup of the `.body` file.

Several of the first lines of the `.body` file contain comments on how to use the file. These lines do not show in the emails sent to patrons. The second line of the `.body` file, however, contains the return address for the checkout email. The default address is `noreply@sirsidynix.com`. If no `reply/from` address is specified in the template, Web Services for Horizon uses the `email_param` setup.

### Using tags

The following tags are included in the `default.body` file to deliver the appropriate information to your patrons. The Web Services for Horizon server fills these placeholders with the appropriate values. You can place these tags wherever you want.

Tag	Description
<NAME>	The name of the user.
<USERID>	The user ID of the user.
<ITEMS>	The information for the checked out items.  <b>Important:</b> The <ITEMS> tag is responsible for supplying the checkout receipt with the list of checkouts; in order for checked out items to display in checkout receipts, the <ITEMS> tag must be in the template.

### The `.item` file

The `.item` file contains the template for each row in the list of checked out items; the list this file creates displays where the `<ITEMS>` tag in the `default.body` file is located.

The following tags are delivered in the `default.item` file; the Web Services for Horizon server fills these placeholders with the appropriate values.

Tag	Description
<TITLE>	The title of the checked out item.
<AUTHOR>	The author of the checked out item.
<CALLNUM>	The call number of the checked out item.
<ITEMID>	The item ID of the checked out item.
<CHECKOUTDATE>	The date the checked out item was charged.

Tag	Description
<DUEDATE>	The date the checked out item is due back to the library.

## Configuring the Reset My PIN Template File

This topic contains information on how to customize the reset PIN template file for use by your library. The email template file is HTML-based. You can add to or edit the template as you would any HTML file. You can find the template on the web services server at `hzws\WEB-INF\classes\emailTemplates\resetPin`.

If Web Services for Horizon cannot find the template files with the specified name, it will check the language directory appropriate to the patron's language for the default template files. If there are no template files in the appropriate language directory, Web Services for Horizon will check the `WEB-hzws\WEB-INF\classes\emailTemplates\resetPin` directory for files with the name specified in the **Template** field; if it cannot find the files, it will use the default template files delivered with Web Services for Horizon.

You can set up the PIN recovery email by using any of the following tags:

- `<LINK>` — tag will be replaced with the newly formatted link. This is the `resetPinURL` given in this request, plus, if `<RESET_PIN_TOKEN>` was included in the URL, the system converts the `<RESET_PIN_TOKEN>` to a `resetPinToken`. Typically, this is used instead of `<PIN>`.
- `<RESET_PIN_TOKEN>` — tag will be replaced with the newly generated `resetPinToken`. Typically, this is included in the `resetPinURL` as part of this request instead of in the email template file.
- `<PIN>` — tag will be replaced with the user's current PIN. Typically, this is used instead of `<LINK>` to show the user their current PIN. This is useful for sites that do not want users to be able to change PINs. However, since this value gets sent in an email to the user, there may be a security risk.

The first line of the email template file should contain the reply-to address. The second line should contain the subject line of the email. The remainder of the template file contains the email body, including any of the above tags.

The following is an example of a template:

```
replyto@yourlibrary.com
PIN RESET
<html>
  <body>
```

## Appendix D: Configuring Email Templates

```
Please follow this link to <a href="<LINK>">reset your PIN</a>.<br/>
From,<br/>
<br/>
Your local library
</body>
</html>
```



As with the patron login credentials, `/user/patron/resetMyPin` includes separate fields that can be for authenticating. These include `login`, `preferredID`, `alternateID`, and `barcode`.

# Index

---

## A

### Admin console

- accessing 37, 83
  - Add/Edit LDAP Server (fields) 63
  - Add/Edit Single Sign-on URL (fields) 58
  - browser requirements 38
  - changing the password 41
  - changing the username 40
  - configuring CAS single sign-on 56
  - help 39
  - HIP Configuration page (fields) 50
  - ILS Configuration page (fields) 45
  - LDAP Setup 59
  - LDAP Setup page (fields) 62
  - logging in 39
  - logging out 40
  - message bar 39
  - Navigation pane 39
  - Profile Settings page (fields) 48
  - resetting ILS connections 42
  - restoring access 83
  - Single Sign-on Setup page (fields) 57
  - Status page 41
  - Status page (fields) 43
  - understanding the basics 37
  - understanding the interface 38
  - updating HIP configuration options 49
  - updating HIP profile settings 47
  - updating ILS configuration options 44
  - viewing Web Services logs 73
  - workspace 39
- ### Admin console buttons
- Add LDAP Server 63
  - Add URL (CAS) 57, 69-70, 79

- admin password
  - changing 41
  - lost 83
- admin username
  - changing 40
  - lost 83
- advanced installation
  - creating the properties file 25
  - introduction 25
  - running the installer 34
- authentication methods
  - CAS 56
  - LDAP 59

## B

- base URL 93
- BeanCreationException error 90
- bind exception error 90
- browser requirements 38

## C

- CAS
  - configuring single sign-on 56
- catalina log file 87
- configuring email checkout receipt template files 99
- context initialization error 90

## E

- errors
  - BeanCreationException 90
  - BindException 90
  - context initialization failed 90
  - Initial LDAP bind 91
  - listenerStart 92
  - port already in use 90



---

**F**

## fields

- Always Require Authentication 46
  - Base Distinguished Name 63-64
  - BIND Password 65
  - CAS Property 58
  - CAS Server 57, 69, 78
  - CAS Service ID 57-58
  - Cash Drawer ID 48, 56
  - Confirm BIND Password 65
  - Currency Code (Circulation) 46
  - Database Host IP 45
  - Database Maximum Connections 46
  - Database Minimum Connections 45
  - Database Name 45
  - Database Port 45
  - Distinguished Name for BIND 65
  - Full View 50
  - HIP Host 50
  - HIP Port 50
  - ILS Connection Status 43
  - ILS Timezone 46
  - ILS Version 43
  - Item View 51
  - LDAP Host 63-64
  - LDAP Only Authentication 63
  - LDAP Port 64
  - Library Department 49, 56
  - Licensed Clients 43
  - Licensed To 43
  - Pickup Location Set 51
  - Profile (HIP) 51
  - Search Attribute 64
  - SSL Authentication (LDAP) 64
  - SYBASE or MICROSOFT 45
  - URL (CAS) 58
  - User ID 48, 56
  - Web Services Version 43
  - Workstation ID 48, 55
- Full Installation
- steps 10

---

**H**

## help guide

- about vii

## HIP

- updating configuration options 49
- updating profile settings 47

## HIP properties

- host 24
- port number 24

## hzws log file 88

---

**I**

## ILS

- resetting connections 42
- updating configuration options 44

## ILS connection

- troubleshooting 85

## ILS properties

- database host 21, 45
- database name 22, 45
- database port 45
- database port number 22
- database type 22, 45
- database user 22
- database user password 22
- maximum database connections 22, 46
- minimum database connections 22, 45

## Initial LDAP bind exception 91

## installation

- advanced installation 25
- before you begin 7
- changing the locale 9
- configuration properties 19
- Console mode 8
- Full Installation 10
- getting started 1
- GUI mode 8
- HIP configuration properties 23
- ILS configuration properties 21
- installation types 10

---

- installing Web Services only 13
- installing Web Services with Tomcat 10
- overview 6
- running the installer 8
- Silent mode 25, 34
- starting up Tomcat 84
- starting your installation 7
- supported locales 9
- Tomcat configuration properties 20
- troubleshooting 24
- upgrading Web Services 15
- Web Services configuration properties 22
- installation type
  - choosing 10
  - Full Installation 10
  - Web Services Only 13
  - Web Services Upgrade 15
- installer
  - configuration properties 19
  - supported locales 9

**J**

- Java
  - environment variables
    - finding,setting 18
  - requirements 4
- JAVA\_HOME
  - finding,setting 18
- JRE\_HOME
  - finding, setting 18
- JVM\_BIND exception 90

**K**

- key concepts
  - base URL 93

**L**

- LDAP 59
  - about LDAP authentication 59
  - changing timeout settings 62

- managing server connections 61
- LDAP bind exception 91
- license keys
  - viewing or updating 42
- listenerStart error 92
- locales 9
- logging
  - catalina (Tomcat) 87
  - hzws activity 88
  - Web Service requests 87
- logging in 39
- logging out 40
- logs 75
  - examining log files 86
  - viewing Web Services logs 73

**O**

- online help
  - opening 39
- operating system
  - requirements 4

**P**

- properties file
  - admin-settings properties 34
  - creating 25
  - essential properties 26
  - hip-settings properties 32
  - hz-spring properties 30

**R**

- requests log file 87

**S**

- sessions
  - timeout 40
- single sign-on 56
  - configuring 56
- SSO 56
- system requirements 3

---

**T**

## timeouts

session 40

## Tomcat

advanced configuration 94

catalina log files 87

configuration 3

configuration properties 20

memory requirements 3

ports 90

recommended start up settings 94

requirements 5

session timeout 40

starting up 84

## Tomcat properties

HTTP port 21

HTTPS port 21

service name 20

shutdown port 21

## troubleshooting 83

Admin console access 83

common errors 89

connection issues 85

examining log files 86

general 83

installation 24

**U**

uninstallation 82

**V**

## view

logs 75

**W**

## Web Services

hzws log file 88

requests log file 87

## Web Services for Horizon

about 1

Admin console 36

configuring 36

hardware requirements 3

installing 6

Java requirements 4

key concepts 93

license keys 42

run-time status 41

supporting operating systems 4

system requirements 3

Tomcat requirements 5

troubleshooting 83

uninstalling 82

upgrading 15

verifying that Web Services are running 85

## Web Services Only Installation

steps 13

## Web Services properties

currency code 23, 46

logging directory 23

logging prefix 23

time zone 46

## web services requirements

hardware 3

Java requirements 4

operating system 4

system 3

Tomcat requirements 5

## Web Services Upgrade

steps 15