



Web Server

Reference Guide

Includes:

Installation Guide

Administration Guide

Copyright

Information in this document is subject to change without notice. The software described in this document is furnished only under a separate license agreement and may be used or copied only according to the terms of such agreement. It is against the law to copy the software except as specifically allowed in the license agreement. This document or accompanying materials contains certain information which is confidential information of Hyland Software, Inc. and its affiliates, and which is subject to the confidentiality provisions agreed to by you.

All data, names, and formats used in this document's examples are fictitious unless noted otherwise. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright law, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Hyland Software, Inc. or one of its affiliates.

Hyland®, Hyland Software®, Hyland Healthcare, and Hyland product names are registered and/or unregistered trademarks of Hyland Software, Inc. and its affiliates in the United States and other countries. All other trademarks, service marks, trade names and products of other companies are the property of their respective owners.

© 2021 Hyland Software, Inc. and its affiliates. All rights reserved.

Document Name Web Server
Department/Group Documentation
Revision Number Foundation EP5

OVERVIEW

Web Client Types	1
Architecture	1
Enhanced Performance	2
Enhanced Security.....	2
API Support.....	3
Core Features	4
Oracle TNS for WebService	5
Licensing	5
Simplified Licensing	5
Legacy Licensing.....	5
Security & Browser Settings	6
Firewall Port Requirements	7
Exterior Firewall Ports	7
Interior Firewall Ports	8
Default File Traffic Ports	8
Internet Options Security Zone.....	8
Advanced Internet Options	10
Internet Explorer ActiveX Security Settings.....	10
Internet Explorer Miscellaneous Security Settings	11
Tabbed Browsing	11
Pop-up Blockers	11
Unsupported Environments	12
Adding the Web Server as a Pop-up Blocker Exception	12
Internet Explorer	12
Firefox	14
Firefox Dialog Box Suppression	15
User Account Control.....	15
Modifying Configuration Files	15
Internet Explorer Features	17
ActiveX Security Setting.....	18
Accelerators	19
Pop-up Blocker Requirement.....	19
Pinned Sites & Jump Lists.....	20
Jump Lists & Favorites	20

INSTALLATION GUIDE**INSTALLATION**

Overview	22
Requirements	22
General Requirements	22

IIS Requirements	22
Desktop Host Version Compatibility	22
Microsoft .NET Framework Installation.....	23
Web Client Additional Browser Requirements	23
Cookies and DOM Storage	23
Internet Explorer	23
Google Chrome	23
Firefox	24
Internet Explorer Disable Script Debugging	25
Proxy Server Setup	25
FormPop and PDFPop Browser Requirements	26
Hyland Software - Microsoft Windows Updates	27
Windows 10 Updates	27
Notes on Dedicated Web Server Hardware	27
Licensing.....	28
Upgrade Considerations	28
General User Interface Redesign.....	28
Web Server and Web Client Upgrade Considerations.....	29
Checksum Key Requirement Upgrade Considerations.....	30
Upgrading From Version 13 and Earlier.....	31
Installation	32
Installer Options	32
Installation Overview	34
Running the Installer	34
Change, Repair, or Remove an Installation	44
Controlling the Installer from the Command Line	45
Silent Installation Using setup.exe	45
Feature and Property Names	45
Feature Names	45
Property Names	46
Installation Locations	47
Configuration Options	47
APPSERVER_APPLICATION_NAME	47
DATASOURCE	47
IIS_ASPNET_USER.....	48
IIS_ASPNET_PASS.....	48
WEBSERVER_APPLICATION_NAME.....	48
WEBSERVER_APPSERVER_URL.....	48
WEBSERVER_IIS_ASPNET_IMPERSONATION	48
WEBSERVER_IIS_NTAUTH	49
WEBSERVER_IIS_TLS	49
WEBSERVER_IIS_WEBSITE_ID	49
WEBSERVER_SERVICECLIENTTYPE	50
WEBSERVER_URL	50

Post-Installation	51
Configuring Service Client Settings.....	51
Remoting	51
SOAP	51
Enabling Impersonation.....	52
Disabling Impersonation	53
Active Directory Authentication.....	54
Additional Active Directory Authentication Steps for Firefox	55
Integration for Single Sign-On	55
Configuring the Web Client for Two Authentication Types	56
Impact of Running Antivirus Software on the OnBase Web Server	56
Loss of Session Context	57
Decreased Performance and Scalability	58
Recommendation for Performance Issues on Servers and Client Workstations	58
Required Configuration Settings for Non-Interactive Active Directory Authentication.....	58
Registering a Service Principal Name (SPN) and Configuring Delegation in Microsoft Windows	59
Configuring the Application Server	60
Configuring Web Applications.....	62
Java API	64
Installing the Java API Interface	64
Updating an Existing Hyland.jar JAVA API Installation	64
Automatic Query Execution Upon Logon	65
URL Creation Methods.....	65
Modifying DocPop URLs for Web Client Use.....	65
Creating Web Client URLs Manually.....	66
Keyword Parameters	67
Keyword Parameters Example	68
Optional Parameters	69
Differences Between DocPop & Web Client URLs	70
Backup and Recovery	71
Backup	71
Exporting Application Pool and Virtual Directory Settings	71
Recovery	72
Restoring the Application Pool and Virtual Directory Settings	72
 DESKTOP HOST INSTALLATION	
Installing Desktop Host.....	74
Microsoft Windows Requirements.....	74
General Visual C++ Requirements	74
Upgrade Considerations	75
Upgrading an Installation on Windows	75
Upgrading an Installation on macOS	75
Running the Windows Installer.....	75
Change, Repair, or Remove an Installation for Windows	80

Installing Silently from the Command Line	80
Running the macOS Installer	81
Removing an Installation for macOS	86
Whitelisting a Domain.....	86
Configuring Desktop Host for Identity Providers.....	87
Creating Log Files for Troubleshooting.....	88
Troubleshooting Desktop Host	91
Whitelisted URL Does Not Open.....	91
Firefox Restricts Desktop Host	91
Firefox Does Not Connect in Windows 8.1 or Windows Server 2012 R2	92
Certificate Issues on macOS	93

WEB SERVER MANUAL INSTALLATION CHECKLIST

Web Server Installation Steps Checklist.....	95
Notes.....	114
Troubleshooting Permissions	115
Local System Account Testing.....	115
Domain User Account Testing.....	115
After Testing.....	115
W3wp.exe could not be started.....	116

ADMINISTRATION GUIDE

ADMINISTRATION IN THE WEB CLIENT

General Usage	118
Logging On.....	119
Login Banner	119
Locked Objects Notification	120
Database Mismatch Message	120
ActiveX Control Message	121
Concurrent Client Licenses Message	121
Last Login	121
Session Interruption.....	121
Session Timeout	122
Authentication Required	122
Changing Your Password	124
Viewing a Document's History	127
Printing OLE Documents	129
Printing in the OnBase HTML Web Client	129
Printing Thumbnails	129
Filtering a Document History	130
Viewing a Folder's History	132
User Administration	136

Required Administrative Rights	136
Managing User Connections	137
Accessing Administration	138
Navigation	139
Finding a User	140
Viewing All Users	140
Viewing Active Users	140
Viewing Users Consuming Licenses	141
Refreshing the User List	141
Selecting Multiple Users	142
Creating a New User	142
Configuring an Existing User	143
Configuring User Settings	144
Accessing User Settings	144
General Settings	145
User Assigned License	146
User Groups	148
Security Keywords	148
Assigning Security Keywords	149
Enabling and Disabling Workflow Trace	151
Locking & Unlocking Users	152
Unlocking a User Account	153
Locking a User Account	153
Disconnecting a User	154
Deleting a User	155
Sending a System Message to Active Users	155
Additional Web Server Documentation	158
ActiveX Web Client	158
HTML Web Client	158
DocPop	158
FolderPop	158
FormPop	158
LoginFormProc	158
PDFPop	158
StatusView	158
Troubleshooting	159
Users Cannot Log On Using Active Directory Authentication	159
Checking NTLM settings in IIS 8.x	160
Checking NTLM settings in IIS 10.x	160
Additional Steps	160
The Screen is Empty Upon Login	161
ActiveX Controls Fail to Load	161
ActiveX Controls Fail to Load in Internet Explorer	161
ActiveX Controls Fail to Load in Internet Explorer After an Upgrade	164

ActiveX Controls Fail to Load in a Virtualization Environment	164
Text Is Too Small.....	165
Thumbnails Are Blank.....	165
Using the Tab Key to Navigate the HTML Web Client in Safari.....	165
Scroll Bars Don't Display in Safari.....	166
Troubleshooting Microsoft Office Documents	166
The Web Client Loses Focus When Word Documents Are Opened	166
OLE Documents Are Opened Externally	167
Users Cannot Print Microsoft Word Documents	167
Users Cannot Open Microsoft Visio Documents	167
Excel Documents Opened Externally Are Unresponsive	168
Modifying the Web.config Setting for Office Documents	169
Changing the Order of Document Access	169
Users Cannot Open CSV Files in Excel	169
MHTML Documents Cannot Be Opened	169
Folders: Internet Explorer Is Unresponsive.....	170
Web Client Won't Load—Server Application Unavailable.....	170
Characters Are Cut Off in Text Documents	171
External Text Search: Documents Not Opened to Correct Page.....	171
Alternative Options	171
Print Formats Aren't Available in the HTML Web Client	172
Notes Configured to "Never Print" Are Printed.....	172
Notes Configured to Print After a Document are Printed Before.....	173
Document Printing Differs Between Core and OnBase Client.....	173
Color Documents Do Not Print in Black and White.....	173
Document Handle Search Results Differ Between Core and OnBase Client.....	174
Keyword Issues	174
Document Dates and Date Keywords Prior to 1/1/1753	174
E-Forms & HTML Content Don't Render Correctly	174
Saving E-Forms.....	175
Printing E-Forms.....	175
Error Messages and Errors.....	175
Access to the path "C:\inetpub\wwwroot\appnet\temp\icons" is denied	175
Another session is currently active	175
Authentication failed. Please check the configuration settings.	176
Cannot create channel sink to connect to URL	176
Client found response content type of 'text/plain; charset=utf-8'	177
Content length too large	177
Could not create Windows user token	178
Could not get database driver information for data source	178
The data that you have requested is currently off line	179
If impersonation is ENABLED	179
If impersonation is DISABLED	179
Error occurred Sharing Envelope	179
Failed to create object element for control	180

Failed to find Web Server license for data source	180
Failed to get session for session id	180
Failed to load Popup Blocker Assistant ActiveX control	182
Failed to receive valid XML Response from Server	182
File or directory not found	182
Login Page Error	183
Importing Documents Error	183
Handler "PageHandlerFactory-Integrated" has a bad module	183
Input stream is not a valid binary format	184
Input string was not in a correct format	185
Is not a valid Win32 application	186
Keyword does not validate as masked or unmasked	186
ODBC SQL Server Driver: Communication link failure	186
Please verify size of image has not exceeded the maximum size limit	187
The remote server returned an error. (404) Not Found.	187
The requested page cannot be accessed	187
Requested registry access is not allowed	188
Request timed out	188
The server encountered an error when logging in	189
This page is asking you to confirm that you want to leave - data you have entered may not be saved. .	189
Service Unavailable	190
System is currently locked out	191
There was an error when loading the document	191
Mismatched ActiveX Controls	191
Color Overlays	192
This document is not accessible by the current user	192
Unable to automatically add itself to the pop-up blocker white list	192
Unable to complete transform of the XML document	192
Web Server version cannot connect to Application Server version	193
IIS and .NET Framework Errors	193
Failed to Access IIS Metabase	193
Web Page Displays Code	193
Diagnostics Console	195
Diagnostics Console Executable Location	196
Saving a Log	196
Clearing a Log	196
Script Exceptions	196
Invalid Password Error	197
Locked User Error	197
Mail Services Errors	198
Web Diagnostics Page	198
Required Rights for Accessing Web Diagnostics	199
IE Security Requirements	199
Accessing the Web Diagnostics Page	199

Accessing the Diagnostics Page Directly	199
Accessing Diagnostics Through the Administration Layout	201
Diagnostics Status Symbols	202
Diagnostics Categories	203
Changing Logging Profiles	205
Restoring Default Logging Profiles	207
Viewing a Diagnostics Text Report	207
Diagnostics Using trace.axd	207
Web Server Availability.....	208
Contacting Support	208
Web Server Information Required When Contacting Support	208

CONFIGURATION

Configuration Module	209
OnBase Configuration Considerations	209
Web Server Client Considerations.....	209
Keyword Considerations.....	210
Required Keyword Types	210
Masked Keyword Types	210
Custom Query Configuration.....	210
Grouping Columns	210
User Groups & Rights	211
Disable Change Password.....	212
Modify Users.....	212
Granting Disk Group Access.....	212
Disk Group Fault Tolerance	213
Refreshing the Application Server After OnBase Configuration Updates	213
OnBase Authentication Schemes and Security.....	214
The Integrated Office Viewer Integration	215
Email Web Integration Settings.....	215
Enabling Google Gmail	215
Enabling Microsoft Office 365	217
Enabling Microsoft Exchange	218
Client and Server Configuration	220
Browser Session Cookies	221
Persistent Cookies or DOM Storage for Client Settings	221
Client Browser Deployments	222
Antivirus Software and Client-Side ActiveX Controls	223
Client Setup Page	224
Files Installed	225
Client Email Requirements	227
Audio and Video File Requirements.....	227
Video On Demand/Media Stream Requirements.....	227
Regional Formats for Currency, Dates, and Numbers	228

Application Server Session Timeout.....	228
Enabling Timeout	228
HTTP Compression.....	229
Configuring HTTP Compression in IIS 8.x	229
Configuring HTTP Compression in IIS 10.x	229
Windows Performance Monitor Counters	229
Changing the Data Source on the URL.....	230
3GB Startup Parameter for Windows.....	230
Ensuring Proper .NET Installation	231
Installation Order	231
Manually Changing the .NET Version	232
IIS and ASP.NET Configuration for Web Server Autologin	233
Overview	233
Interactive Autologin	233
Web Server	234
Application Server	234
Non-Interactive Autologin	234
Web Server	235
Application Server	235
Other Important Notes	236
Application Pool Configuration	237
Application Pool Best Practices	237
General	237
CPU	238
Process Model	238
Rapid-Fail Protection	238
Recycling	239
Application Pool Identity	239
Load Balancing	240
Installing the OnBase Servers	240
Configuring the Load Balancer.....	241
Module-Specific Load Balancer Requirements	241
OnBase Servers	242
Application Enabler	242
Configuring the Web Server for Load Balancing	242
Load Balancing Across Multiple Web Servers	242
Load Balancing Across Multiple Application Servers	243
If You Are Not Load Balancing Across Application Servers	243
Sample Load-Balancing Configurations	244
Load Balancing Across Web Servers Only: Single-Server Scenario	245
Load Balancing Across Web Servers Only: Split-Server (Dual) Scenario	246
Load Balancing Across Application Servers Only	247
Load Balancing Across Multiple Web Servers and Application Servers	248
Load Balancing Across Web Servers Only: Many-to-One Scenario	249
Load Balancing Web Server Modules	250

Exceptions	250
Integration for Microsoft Search	250
Web.config Configuration	251
appSettings.....	251
Configuring the Web Client Type	258
sessionState Timeout	259
maxconnection	259
httpRuntime	259
maxAllowedContentLength	260
X-Frame-Options	261
cookieSameSite	262
Context Menu Overrides and Viewer Vars	263
Context Menu Overrides for the HTML Only Viewer	263
Context Menu Overrides for the ActiveX Viewer	263
Viewer Vars	264
Disable Context Menu	265
Viewer Vars for the HTML Only Viewer	266
Viewer Vars for the ActiveX Viewer	266
ActiveX Viewer Toolbars	266
Thumbnail Auto Zoom Configuration	267
Security Keywords	267
Document Select Vars	267
Enabling Blocked or Overridden Function Keys	267
Allowing Insecure Connections	268
EnableLegacyChecksumFallback	268
EnableLoginAutocomplete	268
Folder Window Vars	269
DocPop Vars	270
PDFPop Vars	273
FormPop Vars	276
FolderPop Vars	279
Office Documents Setting	281
RTF Documents Setting	281
Thumbnail Hit List Viewer	282
Main Menu Panel Configuration.....	284
Navigation Panel Context Settings	285
Context Security Checks and Licensing	286
Custom Contexts	288
Auto-Display Options	289
Default Contexts & Home Pages	290
Custom Validation.....	291
Custom vs. Standard Validation	291
Restrictions and Limitations	291
Configuration	291
Identifying Application and Pages Elements	292

Procedure for Specifying Validation Functions	292
Validation Functions	292
Sample Function	293
Hyland.Logging	294
Enabling Event Viewer Logging	294
Diagnostics Profiles	294
Enabling Diagnostics Logging	295
Truncating Log Length	296
Setting the Logging Level	296
Setting the Tracing Level	298
Creating Log Files	298
Disabling IP Address Masking	298
Configuring for Third Party Diagnostic Programs	298
Configuring Hyland.Logging for Splunk	299
Configuring Hyland.Logging for ELK	299
Configuring Image Quality and Compression Settings.....	301
RawImagesAllowed	301
CompressionQuality	301

LOGINFORMPROC

Configuring the ASP.NET Version of LoginFormProc	302
Configuration	302
LoginFormProc Settings	302
Encrypting LoginFormProc Web.config Settings	303
Features	303
Submitting a new form to the database	303
Opening a read-only copy of the submitted form	304
Redirecting the user to the custom form	304
Setting the Language Parameter	305
Licensing.....	305

FORMPOP

Overview	306
Usage	306
Retrieving Forms Using FormPop	306
Editing Existing Forms Using FormPop	306
Configuration	307
FormPop Vars	307
Embedding FormPop Results in a Web Page.....	309

INTERNATIONALIZATION AND LOCALIZATION BEST PRACTICES

Requirements and Best Practices	310
Note Considerations	311
Web.config Encoding	312

Transaction Log Translations	312
Help Files Setup for Multiple Languages.....	312
Supported Translations and Formats.....	313
Supported Translations	314
Supported Formats	315
Locale Detection with Firefox.....	319

MODULE-SPECIFIC WEB.CONFIG SETTINGS

AFP or PCL Caching from Centera or Tivoli Web.config Settings	320
Application Client Connector Settings	320
Application Enabler Web.config Settings	320
Collaboration Web.config Settings	321
DKT.....	322
Enabling DKT	322
Prompting Users About Unread Documents	322
EDMS Web.config Settings.....	323
Enabling the EDM Briefcase	323
Configuring Settings	323
Integration for Esri Web.config Settings.....	324
Enabling the View Map Button	324
Enabling the Open Map Viewer Option	325
StatusView Web.config Settings.....	325
Ensuring StatusView is Enabled	325
Accommodating Very Large Folder & Workflow Solutions	326
Web Parts for Microsoft SharePoint Settings	326
Basic Authentication	327
Active Directory Authentication	327
Virtual Print Driver Web.config Settings	328
Workflow Web.config Settings.....	328
Viewer Vars	330
WorkView Settings in the Web.config File.....	330
Setting the Maximum Display Results	331
Setting WorkView to Open By Default	331

WEB SERVER BEST PRACTICES

General	332
Installation Recommendations	332
Antivirus/Backup/Indexing Software Configuration.....	333
IIS and ASP.NET Configuration for Web Server Autologin	333
Overview	334
Interactive Autologin	334
Web Server	335
Application Server	335
Non-Interactive Autologin	335

Web Server	336
Application Server	336
Other Important Notes	337
Application Pool Configuration	337
Overlays	338
Troubleshooting	338
High-Security Deployments	339
Load-Balanced Deployments	339

FEATURE MATRIX

Overview	340
License-Specific Considerations	340
Other Considerations	340
Categories of Features	341
Search & Retrieval	342
Document Select List	345
Viewer—Standard—Image Document	351
Viewer—Text Document Specific	367
Viewer—PCL Document Specific	370
Viewer—AFP/RSS Document Specific	370
Viewer—OLE Document Specific	371
Viewer—HTML/E-Form/Unity Form Document Specific	373
Viewer—Import/Scan/Index	375
Print Options	378
Content Management	380
User Options	387
Administration	391

The OnBase Web Server provides users with immediate access to their information and documents anywhere, anytime, through standard Web browsers. From an intuitive standard or customized user interface, users can view, print, annotate, and distribute information stored in OnBase. By increasing operational efficiency and user response, the OnBase Web Server changes the way companies do business with customers, suppliers, and remote offices. The OnBase Web Server enables an enterprise to create automated Customer Service applications that allow customers 24-hour, online access to account information, order status, historical data, and product information.

This module reference guide covers the administrator-level configuration and installation of the OnBase Web Server and Web Client. For end-user functionality, see the **Web Client** module reference guide or help file.

Web Client Types

Standard Web browsers function as secure OnBase Web Clients in both Internet and intranet environments. The following table describes types of Web Clients that are available to accommodate different software environments. For a list of features available for each Web Client type, see the [Feature Matrix on page 340](#).

Web Client Type	Description
ActiveX	The OnBase ActiveX Web Client provides advanced OnBase user features over the Internet, including standard OnBase features such as annotations, cross-referencing, and server-side full-text searching. To minimize network bandwidth consumption, the OnBase ActiveX viewer is intelligently cached on the browser client workstation to eliminate repeated downloading. New control downloads will only occur if deployed by the system administrator.
HTML	The OnBase HTML Web Client offers cross-platform and cross-browser compatibility. This mode offers Web Client functionality without requiring the deployment of ActiveX controls to each client workstation.

Architecture

The OnBase Web Server is an N-tier application that provides Internet access to existing OnBase document repositories as well as backward compatibility with existing OnBase document, security, user group, database, and file storage configurations. The OnBase Web Server co-exists in parallel with the OnBase Client module's configuration and import processing workstations.

Multiple OnBase Web Servers can be deployed in parallel server Web farms, including inexpensive, Web server appliances. For a list of supported IIS and Windows Server operating systems, see the Installation chapter of this manual. All communications are performed using standard Internet network protocols that are compatible with HTTPS bindings and VPN secure connections.

The OnBase Web Server relies on the OnBase Application Server to access the OnBase database and perform business logic. The Web Server and Application Server can accommodate several network configurations. The following topics describe how different configurations can enhance performance and security.

Enhanced Performance

The Web Server and Application Server can be installed on the same machine in separate application pools or on two separate machines. Both of these configurations allow for increased performance since each application can better utilize memory in its worker process.

This architecture also provides you the flexibility to optimize your deployment for the most efficient use of available hardware resources. For example, if you have three server machines available, you can install two Web Servers in two separate application pools on a single machine and then configure each Web Server to refer to different Application Servers that are installed on the two remaining machines.

The configuration that offers the best performance depends on both the number of users who will access the Web Server and the configuration of your OnBase system.

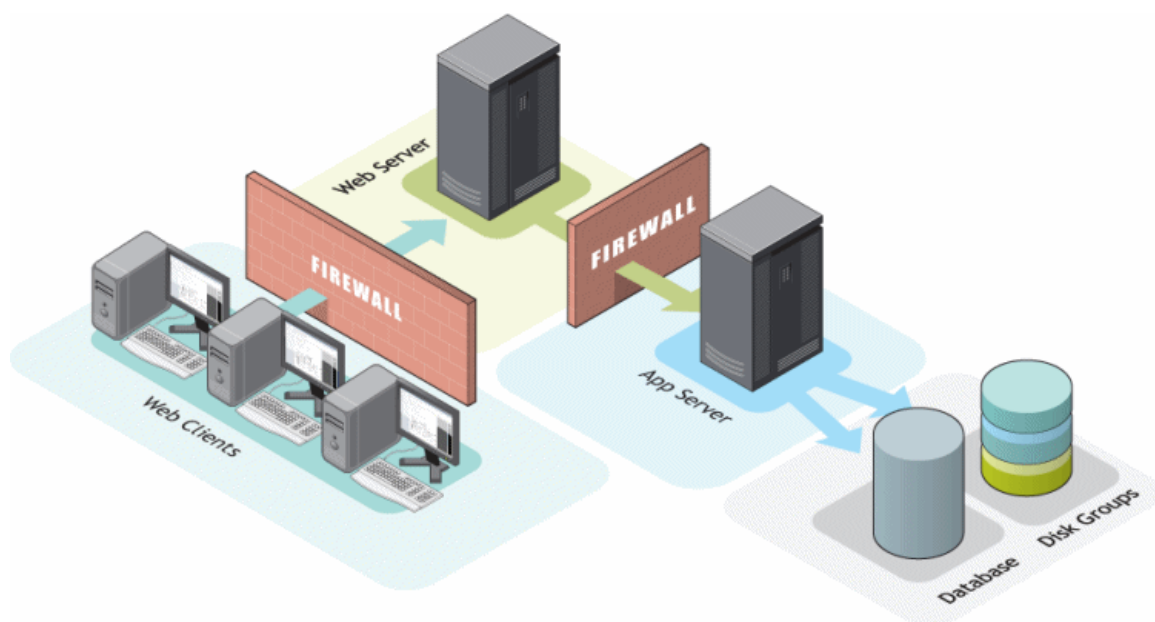
Most processing is performed by the Application Server, so when installing the Application Server and Web Server on separate machines, ensure the Application Server's machine has the resources that provide better performance.

If you need assistance determining the best deployment strategy for your solution, contact the OnBase Installations team.

Enhanced Security

If external or public users need access to OnBase, you should increase the security of your solution by installing the Web Server and Application Server on separate machines and placing a firewall between them. For example, you can install the Application Server on your corporate intranet and install the Web Server on your perimeter network (also known as the DMZ, or demilitarized zone). The perimeter network is a collection of subnets that expose your organization's intranet to external networks, such as the Internet, while also protecting your intranet from unauthorized access.

This configuration provides external Internet users access to the Web Server and its applications while allowing only the Application Server direct access to the OnBase database and disk groups. The data source connection and access to OnBase disk groups are configured only on the Application Server, which is protected on your internal network. The Web Server communicates database and disk group requests to the Application Server, which then receives these requests and retrieves the resources for the Web Server. If your perimeter network follows the two-firewall model, the external firewall filters external requests sent to the Web Server, and the internal firewall filters the Web Server's requests sent to the Application Server.



For information about configuring firewall ports in the above scenario, see [Firewall Port Requirements on page 7](#).

API Support

The OnBase API and XML Core Services expose Microsoft COM, .NET Interop, and XML programming interfaces to the core OnBase document management and Workflow services. Microsoft-focused developers can create OnBase compatible ASP and ASP.NET Web sites, C# and VB applications, and COM/DCOM/.NET components. Mixed-shop developers can create loosely coupled Web Services that allow cross-platform, distributed access to subsets of the API object model via SOAP and XML.

Most portal frameworks can be integrated with the OnBase API and XML interface.

The OnBase Software Development Kit (SDK) is available with interface details, sample scripts, and technical documentation.

A full reference set of ASP Web pages is provided with the OnBase Web Server for out-of-the-box document management, workflow, user administration, and remote diagnostic functionality through the Web browser environment.

Core Features

- Document retrieval.
- Persistent check-in/check-out of documents.
- Multiple document browser windows.
- Double-click cross-references.
- Remote creation and deletion of notes, annotations, redactions, and highlights.
- Workflow client viewing with full user task interactions.
- HTML / E-Form support.
- HTML Unicode format support.
- View and edit document keywords.
- View auto-display keyword types on open documents.
- Image rotation, rubber band zooming, and fit to page.
- Native Hyland viewer support for text, images, COLD, PCL, HPGL, and AFP data.
- Third-party plug-in support for viewing PDF, MS Office, Deja View, and other proprietary document formats.
- Toggle image overlays.
- Multiple page thumbnails.
- Re-index existing documents.
- Remote indexing of OnBase scanned batches.
- Import and scan new documents into the document repository.
- Document text search by text, number, etc.
- External server-side full-text search – single query searching of multiple Document Types.
- Full-text indexing support.
- Custom query retrievals.
- Server-side batch printing.
- Client-side local printing of documents with overlays.
- Client-side emailing of documents with overlays.
- Online user help files.
- Detailed administrator technical documentation.
- Network support for Internet, LAN, or WAN connections.
- Windows Active Directory domain authentication support.
- Compatible with HTTPS connections and Virtual Private Networks.
- No client-side data source connections required.
- API interfaces are documented for third party programming.
- The API supports rich Workflow functionality for BPM process integrations and workflow orchestration.
- Software Development Kit available.
- Native XML support in both the Web Server and API products.

- Support for SOAP protocol-based XML Web Services.
- The OnBase API and XML interfaces are compatible with most portal frameworks.

Oracle TNS for WebService

Oracle administrators must use Oracle TNS for the WebService.

As OnBase Web Servers are centrally administrated, there is already central data source administration.

Licensing

Beginning in OnBase Foundation EP5, new customers must use simplified licensing to access Web Server functionality. Existing customers upgrading from a version of OnBase prior to OnBase Foundation EP5 can continue to use legacy licensing to access this functionality.

If you are a new customer as of OnBase Foundation EP5 or greater, see [Simplified Licensing on page 5](#).

If you are upgrading from a version of OnBase prior to OnBase Foundation EP5, see [Legacy Licensing on page 5](#).

Simplified Licensing

The Essential User, Standard User, or Premier User license is required.

Legacy Licensing

The Web Server requires a Web Server license and a valid Client license.

Note: Each physical Web Server that connects to a database for OnBase requires a separate Web Server license. This typically occurs in a load-balanced environment.

Check your current licensing status by selecting **Utils | Product Licenses** from the Configuration module.

Security & Browser Settings

If your network or workstation security settings are too restrictive, they may conflict with normal OnBase functionality. If these settings are too relaxed, your network is more vulnerable to attack. The following sections provide information about configuring security settings so OnBase can operate effectively without compromising your network's security.

- [Firewall Port Requirements on page 7](#)
- [Internet Options Security Zone on page 8](#)
- [Advanced Internet Options on page 10](#)
- [Internet Explorer ActiveX Security Settings on page 10](#)
- [Internet Explorer Miscellaneous Security Settings on page 11](#)
- [Tabbed Browsing on page 11](#)
- [Pop-up Blockers on page 11](#)
- [Firefox Dialog Box Suppression on page 15](#)
- [User Account Control on page 15](#)

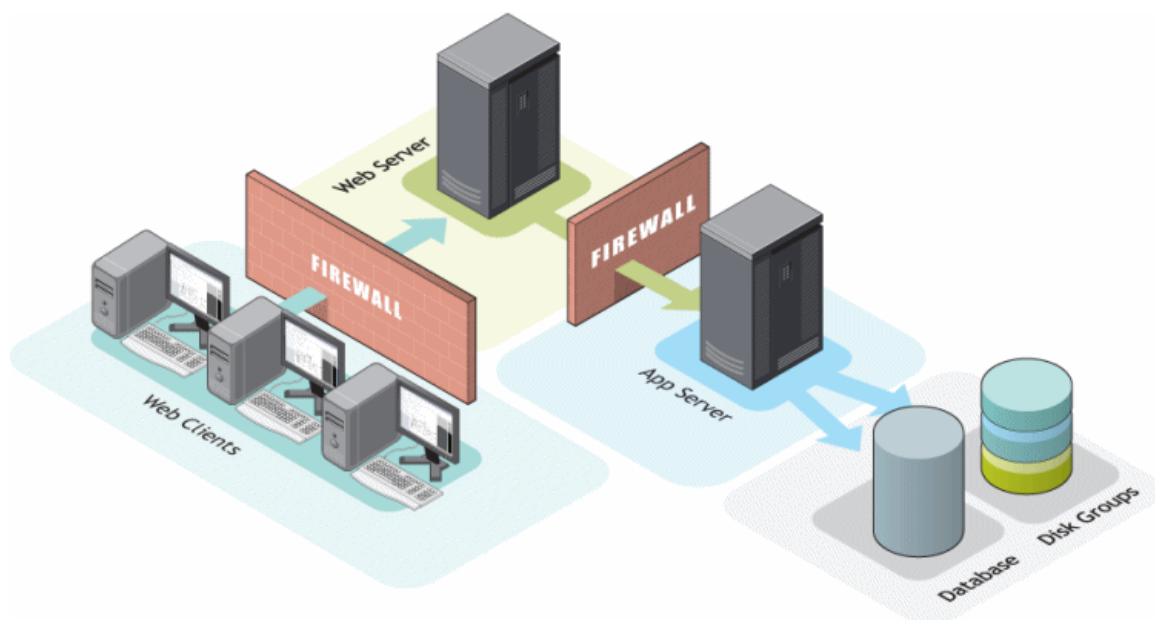
Firewall Port Requirements

Network and workstation firewalls must be configured to allow OnBase servers to communicate with each other and retrieve requested resources.

Exterior Firewall Ports

If the Web Server and Application Server are installed on the same machine, then open the standard port 80 for all incoming/outgoing HTTP traffic or port 443 for HTTPS secured traffic.

If the Web Server and Application Server are installed on separate machines, as shown in the following illustration, then you must configure the firewalls to allow the Web Server and Application Server to communicate with each other.



If your solution uses a configuration similar to this illustration, then follow these minimum guidelines to configure your firewalls:

- The front-end firewall between the perimeter network (DMZ) and external network must be configured to allow inbound traffic on port 80, or port 443 for HTTPS.
- The back-end firewall between the perimeter network and your internal network also must be configured to allow traffic on port 80, or port 443 for HTTPS. This firewall should only allow inbound traffic originating from the perimeter network and destined for the Application Server's IP address or subnet.
- The back-end firewall should only allow outbound traffic destined for the Web Server's IP address or subnet.

Interior Firewall Ports

The Application Server requires open ports for communications with internal network databases and file disk groups. The exact ports required may depend upon the specific configuration of the network protocols, database software, and other Web server applications being used. Typically the server requires the following interior firewall ports to be opened.

Default database traffic ports:

- SQL Server ports 1433
- Oracle ports 1521
- Sybase port 2638

Default File Traffic Ports

- SMB packets (Server Message Blocks - pure TCP/IP protocol) port 445
- NBT packets (NetBIOS over TCP/IP) port 139

In addition, it may be necessary to open the interior firewall to pass server name resolution and NT login authentication packets. The details on which ports are required, is dependent upon the actual network configuration involved.

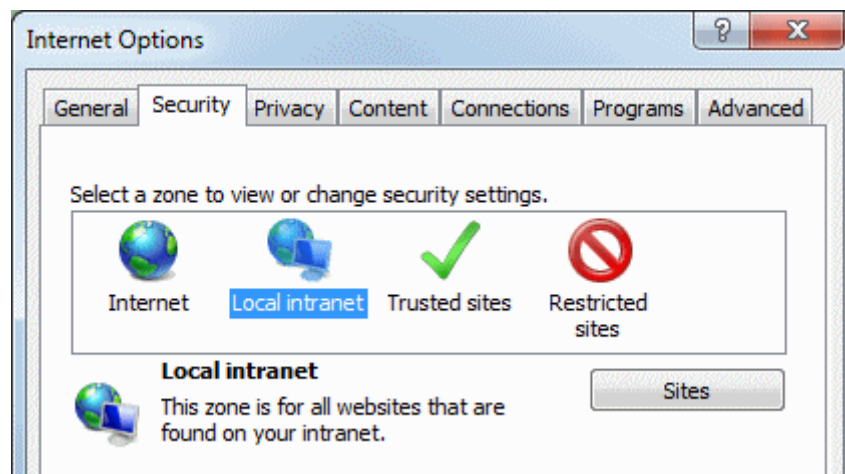
Internet Options Security Zone

Client workstations accessing the Web Client should have the Web Server residing in the **Local intranet** security zone within Internet Options for Windows. This configuration ensures the workstation has the correct security settings for the Web Client to work correctly.

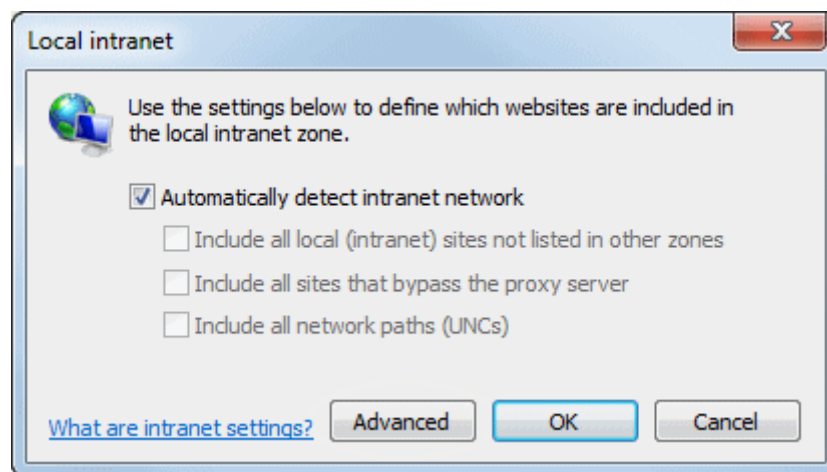
To add the Web Server to the **Local intranet** security zone:

1. Do one of the following to open the Internet Options settings:
 - In Internet Explorer, select **Tools | Internet Options**.
 - Select **Start** and search for **Internet Options**.
2. Click the **Security** tab.

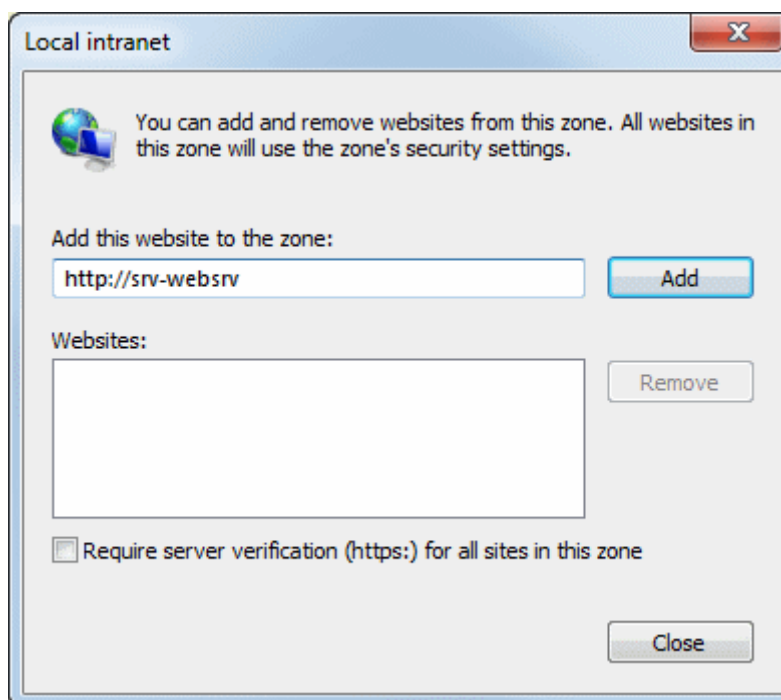
3. Select **Local intranet**.



4. Click **Sites**.
5. Click **Advanced**.



6. Enter the URL to the Web Server in the field provided.



7. Click **Add**.
8. Click **Close**.
9. Click **OK** to close the **Local intranet** dialog box.
10. Click **OK** to close **Internet Options**.

Advanced Internet Options

Client workstations accessing the Web Client using Internet Explorer should have their advanced Internet Options (settings on the **Advanced** tab) set to the default settings. See the Internet Explorer help files for steps and considerations for restoring default settings.

Internet Explorer ActiveX Security Settings

When configuring Internet Explorer security settings for client workstations, ensure that the ActiveX settings will allow the OnBase ActiveX controls to be downloaded.

- Workstations accessing the Web Client should have the **Script ActiveX controls marked safe for scripting** setting set to **Enable** or **Prompt**.
- If ActiveX controls will be pushed down to client workstations from the Web Server, ensure the workstations have the **Automatic prompting for ActiveX controls** setting set to **Enable** or **Prompt**. If this Internet Explorer setting is disabled, then the OnBase session may be lost when an ActiveX control attempts to install. If you used the Hyland Client Side Installer to install the ActiveX controls, then no changes are necessary.

- Due to the **Only allow approved domains to use ActiveX without prompt** setting, ActiveX controls may not load properly on workstations accessing the Web Client using Internet Explorer. If ActiveX controls fail to load properly in Internet Explorer, see [ActiveX Controls Fail to Load on page 161](#).

Internet Explorer Miscellaneous Security Settings

Workstations accessing the Web Client should have **Allow script-initiated windows without size or position constraints** set to **Enable**.

Disabling this setting can cause some right-click menus and HTML dialog boxes in the Web Client to display differently than others. Enabling this setting ensures that right-click menus and HTML dialog boxes have a consistent appearance.

Tabbed Browsing

As a best practice, Internet Explorer's Tabbed Browsing Settings should be configured to use either of the following pop-up settings:

- **Always open pop-ups in a new window**
- **Let Internet Explorer decide how pop-ups should open**

Using these settings will ensure the Web Client functions as intended.

Pop-up Blockers

Pop-up blockers are not supported and can prevent OnBase Web applications, such as the Web Client, from functioning properly. You must either disable any pop-up blockers or add the OnBase Web Server to the pop-up blocker's list of sites that allow pop-ups. If client workstations are configured to automatically download ActiveX controls, then an ActiveX control can detect whether Internet Explorer's or Google Toolbar's pop-up blocker is enabled and automatically add the OnBase Web Server to these pop-up blockers' lists of allowed sites.

For example, if a user logs on to the ActiveX Web Client and Internet Explorer's pop-up blocker is enabled, a message prompts the user to add the Web Server's URL to Internet Explorer's **Allowed Sites** list. If the user chooses **OK**, the Web Server's URL is added to the list and the user can log on without future prompting. If the user chooses **Cancel**, the user cannot log on until either the pop-up blocker is disabled or the Web Client is added to the pop-up blocker's list of allowed sites.

The ActiveX control does not work under all conditions. For more information, see [Unsupported Environments on page 12](#).

Note: Before the Web Server can be added to the Google Toolbar's whitelist, the whitelist registry key must exist. This registry key is created when Google Toolbar is used to add any Web site to the whitelist.

Unsupported Environments

The Web Server's ability to add itself as an allowed site is not supported under either of the following conditions:

- The user is running Internet Explorer 11. This variation of Internet Explorer does not allow the ActiveX controls to automatically add the Web Server as an allowed site.
- The client workstation does not allow ActiveX controls to be downloaded (for example, because the user is accessing the HTML Web Client, or because a pop-up blocker other than Internet Explorer's or Google Toolbar's is enabled).

To allow users to work with OnBase Web applications, you must either add the Web Server to the pop-up blocker's list of allowed sites, or you must disable the pop-up blocker.

Adding the Web Server as a Pop-up Blocker Exception

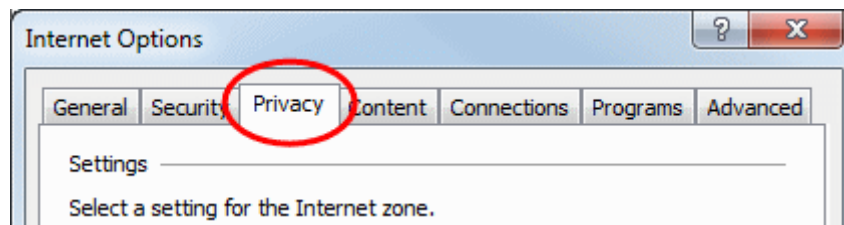
To add the Web Server as an allowed site for pop-ups, see the procedure provided for your browser:

- [Internet Explorer on page 12](#)
- [Firefox on page 14](#)

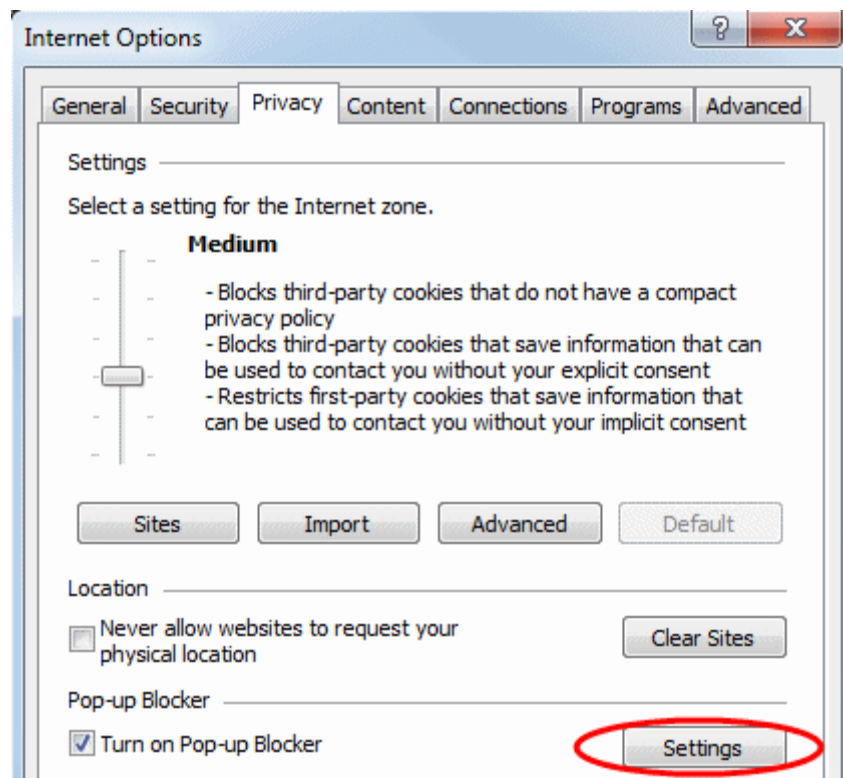
Internet Explorer

To add the Web Server to Internet Explorer's **Allowed sites** list, perform the following steps from the client workstation:

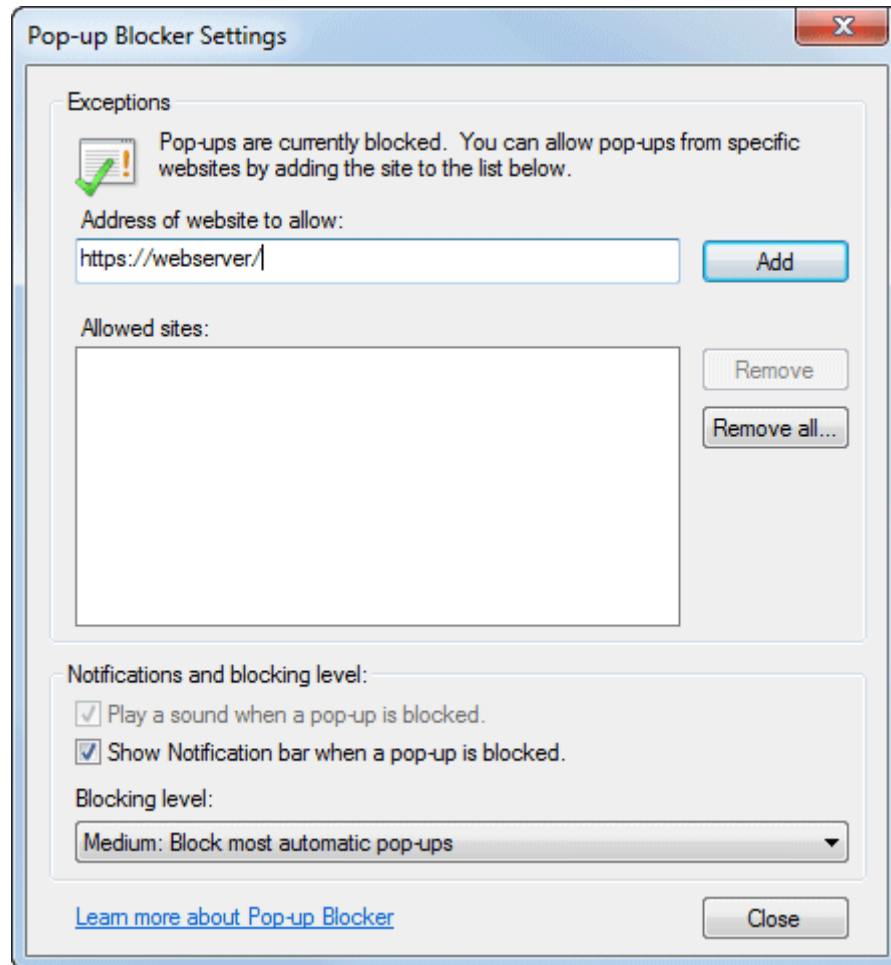
1. Select **Tools | Internet options**.
2. Click the **Privacy** tab.



3. Under **Pop-up Blocker**, click **Settings**. The **Pop-up Blocker Settings** dialog box is displayed.



4. Type the URL to the Web Server in the field provided.



5. Click **Add**.
6. Click **Close**.
7. Click **OK** to close **Internet Options**.

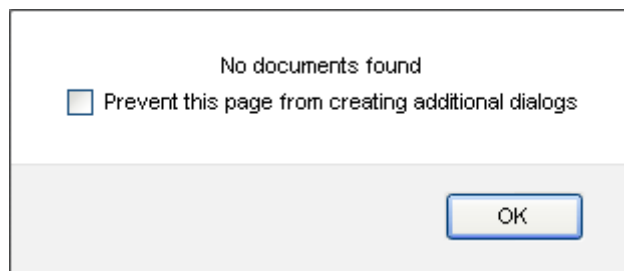
Firefox

To add the Web Server to Firefox's **Allowed Sites** list, perform the steps provided by Mozilla here:

<https://support.mozilla.org/en-US/kb/permissions-manager-give-ability-store-passwords-set-cookies-more>

Firefox Dialog Box Suppression

The OnBase Web Client creates and displays dialog boxes to communicate notifications and errors to the user. In Firefox, the option **Prevent this page from creating additional dialogs** may be displayed after multiple dialog boxes are opened from the same page.



Instruct users never to select this option in the Web Client. Doing so may result in unexpected behavior. For example, Firefox may suppress the Web Client's session timeout prompt, giving the user no indication that he or she is about to be logged out of OnBase.

If a user does select **Prevent this page from creating additional dialogs**, the dialog boxes are suppressed until the next time the user logs on to the Web Client.

User Account Control

User Account Control (UAC) is a security feature included with Windows operating systems. When a user logs on to a system with UAC enabled, the user is restricted from performing tasks that require administrative privileges, even if the user is an administrator. These tasks include modifying Web.config files and installing ActiveX controls.

See the following topics for more information:

- [Modifying Configuration Files on page 15](#)
- [When ActiveX controls are deployed through the Web browser on a system with UAC enabled, the user is prompted to install each control asking Do you want to allow the following program to make changes to this computer? on page 16](#)

Modifying Configuration Files

When UAC is enabled, administrators may be unable to modify Web.config or other *.config files. To address this issue, the administrator should open a text editor (such as Notepad) by right-clicking it and selecting **Run as administrator**. The administrator can then open the *.config file from within the text editor. Because the text editor is running with administrator privileges, the configuration file can be modified and saved using that application.

Another option is to use the Web Application Management Console, which provides a tabbed interface for editing Web.config options. For information about using this application, see the Web Application Management Console module reference guide.

When ActiveX controls are deployed through the Web browser on a system with UAC enabled, the user is prompted to install each control asking **Do you want to allow the following program to make changes to this computer?**

The prompt is displayed the first time each ActiveX control is needed. Users who are logged on as administrators can click **Yes** to install the specified ActiveX control. Once the control is installed, the user is not prompted again for that control.

If the user is logged on as a standard user rather than an administrator, then an administrator must provide his or her credentials before the control can be installed. To avoid this scenario, deploy the Web ActiveX controls using the Hyland Web ActiveX Controls installer.

Internet Explorer Features

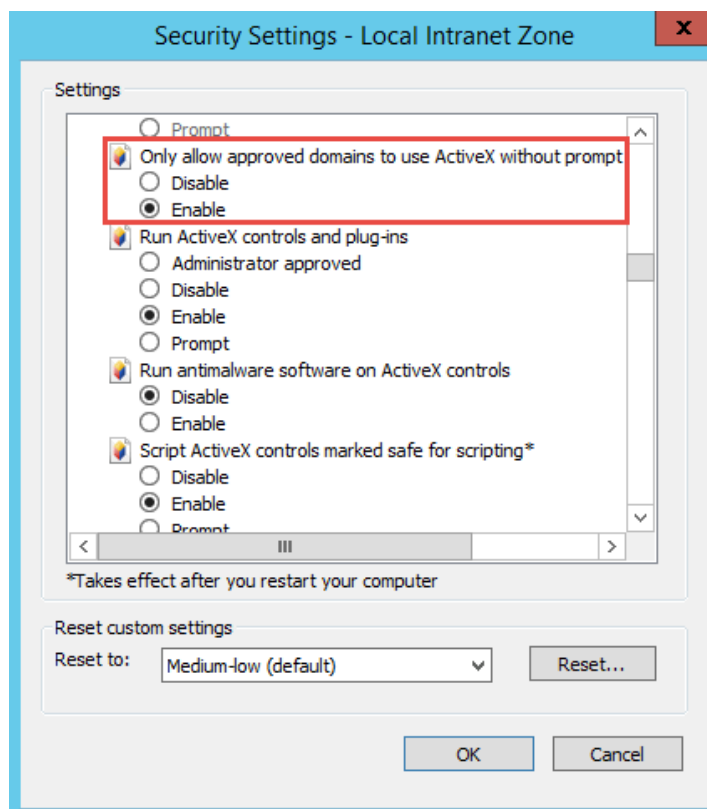
Internet Explorer includes features and behaviors that may affect users of the following OnBase Web Server applications: the Web Client, the Workflow Web Client, DocPop, PDFPop, and FolderPop. Among these features are the following:

- A new ActiveX security setting, **Only allow approved domains to use ActiveX without prompt**, can prevent ActiveX controls from loading properly. See [ActiveX Security Setting on page 18](#).
- Accelerators, which allow users to perform additional actions using highlighted text, including text selected from OnBase Web applications. See [Accelerators on page 19](#).
- In Internet Explorer, the pop-up blocker can prevent the Web Client from loading properly. See [Pop-up Blocker Requirement on page 19](#).
- In Internet Explorer, on certain operating systems, users can pin the Web Client to the Windows taskbar or Start menu. See [Pinned Sites & Jump Lists on page 20](#).

The following topics describe how these features can affect the OnBase user experience. They also discuss courses of action available to minimize these effects.

ActiveX Security Setting

Internet Explorer includes an ActiveX security setting that can affect OnBase users: **Only allow approved domains to use ActiveX without prompt**. When this setting is set to **Enable**, users may be unable to load ActiveX controls in the OnBase Web Client. This setting also affects other OnBase applications that deploy ActiveX controls through a browser, including the integrations for SharePoint and SAP and the Medical Records Management Solution.



If ActiveX controls fail to load on workstations running Internet Explorer, see [ActiveX Controls Fail to Load on page 161](#).

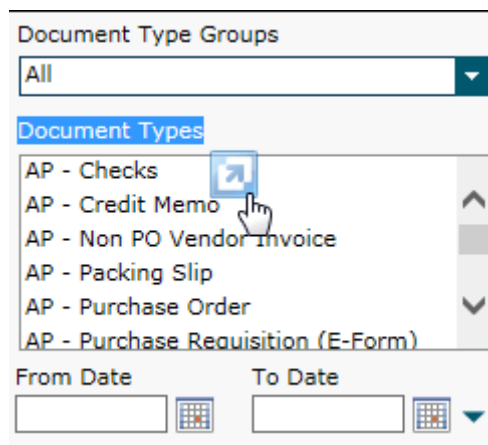
For more information about Internet Explorer security settings that affect the Web Server, see the following topics:

- [Internet Explorer ActiveX Security Settings on page 10](#)
- [Internet Explorer Miscellaneous Security Settings on page 11](#)

Accelerators

Internet Explorer allows users to search, define, email, and translate text selected on a Web page using accelerators, which are links that pass the selected text to Microsoft search services and other user-defined service providers. A user can access accelerators by clicking the blue button that is displayed when the user selects any text on a Web page.

The blue accelerator button is displayed when text is selected in OnBase Web browser-based applications accessed using Internet Explorer. This behavior may confuse OnBase users because accelerators appear to be a feature of the OnBase application rather than the browser.



Currently, accelerators can only be enabled or disabled for all Web sites, not for specific domains from a client workstation, nor for the server hosting the OnBase Web Client. Users should be informed that accelerators are a feature of Internet Explorer; they are not part of OnBase Web applications.

Note: Accelerators cannot be turned off programmatically for specific Web applications. The use of accelerators is controlled by the **Display Accelerator button on selection** advanced setting within Internet Options.

Pop-up Blocker Requirement

Unlike previous versions of Internet Explorer, Internet Explorer 11 does not allow the Web Server to be added automatically to the list of sites that allow pop-ups. As a result, Internet Explorer 11 users must have the Web Server manually added to this list. For more information, see [Pop-up Blockers on page 11](#).

Pinned Sites & Jump Lists

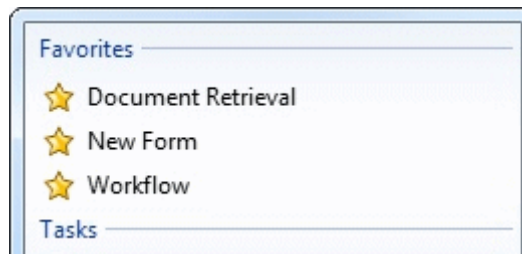
If users access the Web Client using Internet Explorer on a Windows operating system, then they can pin the Web Client site to the Windows taskbar or Start menu. Pinning allows users to quickly find and launch the Web Client with minimal interaction.

Note: Pinning must be performed from the Web Client login page. For information about pinning sites, see [http://msdn.microsoft.com/en-us/library/gg618532\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/gg618532(v=vs.85).aspx).

Jump Lists & Favorites

If users pin the Web Client using Internet Explorer, then they can access contexts in their Web Client **Favorites** list from the pinned site jump list. A jump list provides additional shortcuts into a pinned site, along with commands like closing or unpinning the site.

When a user adds, removes, or renames a favorite in the Web Client, the Web Client **Favorites** list is synchronized with the **Favorites** category in the jump list. For example, if a user adds a context to her Web Client **Favorites** list, then all favorites currently listed in the Web Client are made available in the jump list. The user can later select one of her favorites from the jump list to quickly open the Web Client to the associated context, even if the Web Client is not currently open.



For information about accessing and using jump lists, see [http://msdn.microsoft.com/en-us/library/windows/desktop/dd378460\(v=vs.85\).aspx#jump_lists](http://msdn.microsoft.com/en-us/library/windows/desktop/dd378460(v=vs.85).aspx#jump_lists).

Note: Web Client favorites are stored in a client-side cookie on the user's workstation. If the cookie is deleted from the workstation, then the **Favorites** list in the Web Client is cleared, but the **Favorites** category in the jump list remains populated. The two lists are synchronized only when the user adds, removes, or renames a favorite from within the Web Client.



Web Server

Installation Guide

Overview

The OnBase Web Server is an N-tier application that provides Internet access to existing OnBase document repositories and document, security, user group, database, and file storage configurations. The OnBase Web Server functions in parallel with OnBase Configuration and Client processing workstations. Multiple OnBase Web Servers can be deployed in parallel server web farms, and all communications are performed using standard Internet network protocols that are compatible with HTTPS and VPN connections.

Requirements

The following sections outline requirement information specific to Web Server in OnBase Foundation EP5.

General Requirements

For general requirement information that applies to Web Server and other modules, see the sections on the following topics in the **Installation Requirements** manual:

- Database requirements
- Operating system requirements
- Microsoft .NET Framework requirements
- Microsoft Visual C++ requirements
- Web browser requirements
- Hardware requirements

IIS Requirements

You must have IIS installed with at least one Web site in order to install the Web Server.

Desktop Host Version Compatibility

This version of OnBase Web Server is compatible with Desktop Host version 2.0.5.

Desktop Host is a component that enables cross-platform desktop capabilities and module-specific desktop functionality in the OnBase HTML Web Client. For more information, see the **Desktop Host Installation** chapter in this manual.

Microsoft .NET Framework Installation

OnBase requires Microsoft .NET Framework 4.7.2 or later. The .NET Framework can be obtained from the Microsoft Download Center at <http://www.microsoft.com/downloads>.

The .NET Framework must be installed after IIS has been installed on the server. In addition, the proper server roles and features must be added to the server. For more information, see [Ensuring Proper .NET Installation on page 231](#).

Web Client Additional Browser Requirements

Cookies and DOM Storage

Cookies and DOM storage are required when using the Web Client. Each supported browser provides the ability to enable these items.

Internet Explorer

To enable DOM Storage in Internet Explorer:

1. From the Internet Options dialog box, select the **Advanced** tab.
2. Scroll down to the **Security** section.
3. Select the **Enable DOM Storage** check box to enable DOM storage.
4. Click **Apply**.

To enable cookies in Internet Explorer:

1. From the Internet Options dialog box, select the Privacy tab.
2. Click **Advanced**.
3. Ensure that **Accept** is selected in the First-party Cookies and Third-party Cookies sections.
4. Click **OK**.

Google Chrome

To enable cookies and DOM Storage in Google Chrome:

1. From the Customize and Control options, select **Settings**.
2. Scroll to the bottom of the screen, and then select **Show Advanced Settings**.
3. From the Privacy section, select **Content Settings**.
4. In the Content Settings dialog box, select the **Allow local data to be set (recommended)** option.
5. Click **Done**.

Firefox

To enable DOM Storage in Firefox:

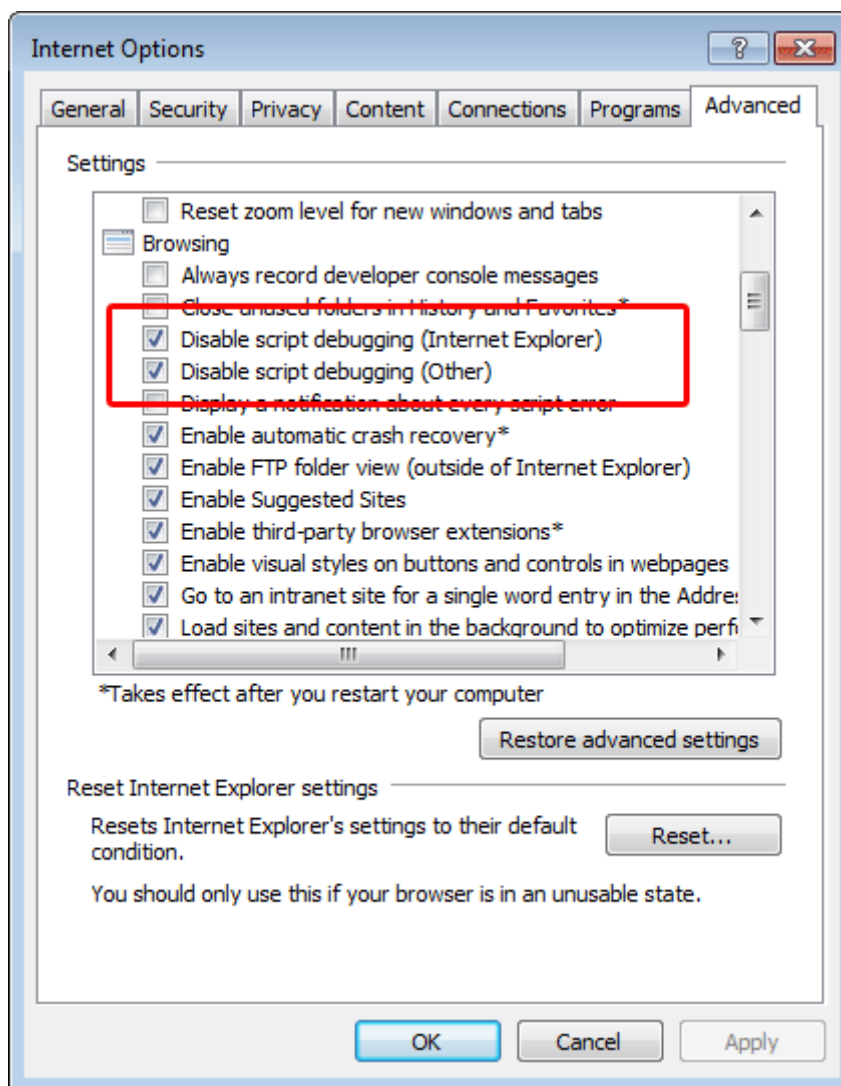
1. Type the following in the subject line: `about:config`.
2. Locate the `dom.storage.enabled` option. The value should be set to `True`. If it is set to `False`, right-click the `dom.storage.enabled` option and select **Toggle**.

To enable cookies in Firefox:

1. From the Firefox options menu, select the Options icon.
2. Select the privacy option on the left side of the screen.
3. From the drop-down list in the History section, select the Use custom settings for history option.
4. Ensure that the Accept cookies from sites option is selected.

Internet Explorer Disable Script Debugging

Internet Explorer Settings must have **Disable Script Debugging (Internet Explorer)** and **Disable Script Debugging (Other)** checked (from Internet Explorer, select **Tools | Internet Options... | Advanced**):

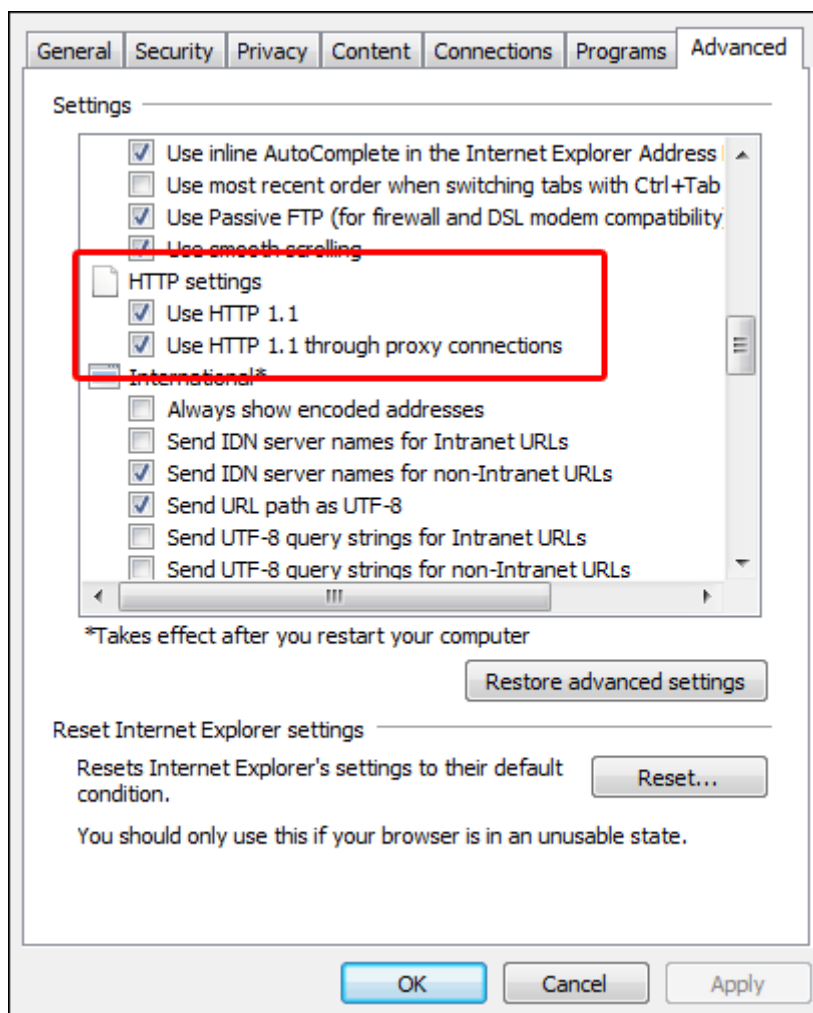


Proxy Server Setup

Ensure the following items are configured when using a Proxy Server:

Server side — If the Web server is using a proxy server, verify that the proxy is setup with HTTP 1.1.

Client side — In Internet Explorer, please ensure that **HTTP 1.1 through proxy connections** is checked when using a proxy.



FormPop and PDFPop Browser Requirements

The following web browsers are supported for use with FormPop and PDFPop:

Web Browser	Supported Versions
Internet Explorer	Internet Explorer 11
Edge	EdgeHTML 14 and higher
Firefox	Firefox 28 and higher (including non-ESR versions)

Web Browser	Supported Versions
Safari	Safari 9.1 and higher for OS X and macOS Safari for iOS
Google Chrome	Chrome 29 and higher

Hyland Software - Microsoft Windows Updates

The developers of OnBase are dedicated to ensuring the regular cumulative updates released by Microsoft® are compatible with OnBase. The R&D Department of Hyland Software regularly evaluates the cumulative fixes released and labeled as Critical or Important by Microsoft. The details of the update provided by Microsoft are reviewed for interaction with OnBase, and the update is installed when appropriate for testing its compatibility with OnBase. If you have questions regarding a specific Microsoft cumulative update and its compatibility with OnBase, please contact your support provider.

Windows 10 Updates

For Windows 10 updates, Microsoft has introduced a new release cadence called the Semi Annual Channel (SAC). The SAC reduces the security patch and support cycle for versions of Windows 10 to 30 months. Hyland Software does not expect to encounter incompatibilities with Windows 10 updates, and it does not plan to change its process for the continued release and support of new versions of OnBase because of the new Microsoft SAC cadence. In the unlikely event that a future Windows 10 update introduces an incompatibility that prevents OnBase from operating as designed, Hyland will make commercially reasonable attempts to address the incompatibility in the latest release and the prior release. If an issue is determined to be related to an incompatible version of Windows 10, you may be required to upgrade to the current OnBase release to resolve the issue and maintain compatibility with Windows 10.

Notes on Dedicated Web Server Hardware

Hyland Software specifies that OnBase Web and Applications Servers be installed on server machines that are dedicated to that sole purpose. We do not support Application Server installations that place other applications, servers, or services on the same physical device.

Web and Application Servers must be dedicated purpose servers; they must not be used as a domain controller, DNS server, non-OnBase Web server, email server, print/database/file server, index server, proxy server, network backup server, jukebox manager, network performance monitor, OnBase Client processing workstation, or Workflow/API OnBase Client broker. Network and disk I/O hardware should be optimized for performance and redundancy. Two network ports can reduce server bottlenecks by using a segmented network for external and internal requests, where external requests are sent to the Web clients and internal requests are sent to the file and database servers. A Gigabit Ethernet connection to the file server and minimal latency connection to the database server are recommended.

The OnBase Application Server, combined with the OnBase Web Server, delivers both static and dynamic content utilizing Microsoft Internet Information Services and Microsoft ASP.NET technology. When both the OnBase Web Server and the OnBase Application Server reside on the same Microsoft Windows Server, high utilization may be seen during peak times. Retrieving search results lists in XML, rendering document images, executing text searches, and various retrieval-related queries place great demand on the Windows Server's hardware, especially the CPU(s) and I/O systems. The server is further loaded down when Microsoft IIS itself is required to perform HTTPS connection services on all content being served to attached browsers through HTTPS connections.

Workflow timers and OnBase processing, both manual and scheduled, should be run on separate servers or workstations. Due to the nature of IIS and how the Web Server utilizes memory, running these processes on the same machine can consume memory, bandwidth, and CPU resources at critical times when users or customers may be accessing the server. The risk of restarting IIS or rebooting the machine must also be kept to a minimum because either of these actions will cause connected users to lose their sessions and possibly lead to data loss.

With all these processing-intensive demands, it is imperative that dedicated server hardware be deployed for each OnBase installation. This will maximize performance, reliability, and maintainability.

Licensing

See [Licensing on page 5](#) for licensing requirements.

Upgrade Considerations

The following upgrade considerations have been compiled by OnBase subject matter experts. These upgrade considerations are general and applicable to most OnBase solutions and network environments and should be considered each time an upgrade is performed.

Carefully consider the impact of making any changes, including those listed below, prior to implementing them in a production environment.

For additional general information about upgrading OnBase, refer to the Upgrade Guidelines reference manual, and visit the Hyland Community at: <https://www.hyland.com/community>.

General User Interface Redesign

As of OnBase 17, the Unity Client and Web Client have a new user interface design. The design changes do not affect functionality, but end users may find the new interface unfamiliar. If you are upgrading from a version of OnBase prior to OnBase 17, review the changes to the user interface with end users, and ensure that any custom end-user documentation is updated accordingly.

Web Server and Web Client Upgrade Considerations

64-bit Web Server and IIS Settings — As of OnBase 18, the Web Server is a 64-bit application. If you are upgrading the Web Server from version 17 or earlier, using the Web Server installer automatically handles the transition from 32-bit to 64-bit, including enabling the application pool for the Web Server for 64-bit execution. However, if you are performing a manual installation, ensure that the following settings are configured in IIS:

- Configure the application pool for the Web Server with **Enable 32-Bit Applications** set to **False**.

Server Machine Considerations — The following should be considered with regard to server machines:

- Check to see if any OnBase Web applications are no longer supported and plan for a replacement.
- Back up the Web Server's Web.config file. This can be referenced when updating specific settings in the new version of OnBase.
 - Note any customized Web.config settings, as well as settings that have been modified from their default values.
- Note the authentication settings for the Web application in IIS.
- Note the settings for the Web Server's Application Pool in IIS.

End-User Workstation Considerations — The following should be considered with regard to end-user workstations:

- Delete the browsing history on end-user workstations.
- Delete the Temporary Internet Files cache for Internet Explorer.
- Configure antivirus software on the client workstation to exclude ActiveX controls downloaded from the web browser into the **C:\Windows\SysWOW64** directory. Because these files contain the version number in the file names, you must whitelist these files every time you upgrade to a new major version.

General Deployment Considerations — In addition to the previous considerations, the following should be considered with regard to general deployments:

- Use of VBScript is not supported in the Web Client. This is because VBScript is deprecated in Internet Explorer. To function in the Web Client, any functionality that depends on VBScripts should be updated to use JavaScript. For more information, see Microsoft's documentation on Disabling VBScript execution in Internet Explorer.
- The <CASH> tag for formatting negative numbers in Auto-Name strings is not supported in the Web Client. If your solution depends upon using the <CASH> tag in the Web Client and you are upgrading from a version of the Web Client in which this tag was supported, you will need to update the solution.

Embedded pages and X-Frame-Options — As of OnBase Foundation EP1, the Web Server is configured by default to require that embedded pages (such as in a frame or iframe) must come from the same domain as the parent page. If your solution includes embedding content from the Web Server into a different domain, you can change the X-Frame-Options setting in the Web Server web.config file to allow embedding Web Server content into a specified URI. For more information on configuring the X-Frame-Options response header and how each web browser supports it, consult an HTTP reference.

Hyland Desktop Host — As of OnBase Foundation EP3, in order to enable certain module-specific desktop capabilities in the HTML Web Client, the Hyland Desktop Host must be properly installed on workstations used to access the Web Client. To determine if a module requires Desktop Host, see the documentation for that module. For more information on installing Desktop Host, see the section on Hyland Desktop Host installation in the **Web Server** module reference guide.

Embedded pages and SameSite cookie attribute — Beginning in early 2020, major web browsers and Microsoft moved to a secure-by-default strategy for cookies, including session cookies. The **SameSite** cookie attribute controls how the browser sends third-party cookies (also referred to as cross-site or cross-origin cookies). If your solution includes embedding content from the Web Server into another web application in a different domain, you must configure the Web Server to instruct the browser to send cookies across domains by modifying the **SameSite** cookie attribute to have a value of **SameSite=None**. For the Web Server this is done by modifying the **cookieSameSite** setting in the Web Server web.config file. Using **SameSite=None** requires an HTTPS connection for the Web Server.

Checksum Key Requirement Upgrade Considerations

This version of OnBase has additional Upgrade Considerations when upgrading to it from one of the following earlier versions:

- Any pre-Foundation releases prior to 18 SP 2
- Foundation EP1
- Foundation EP2
- Foundation EP3, prior to Patch 23
- Foundation EP4

If your solution depends on using checksums for validating Pop integration URLs, you are now required to configure a unique checksum key value, which is used to create the checksum value added to the URL.

If your solution did not previously use a unique string value to create checksum values, you must take the following actions in order for any previously created Pop integration URLs to validate:

- In the Web Server web.config file:
 - Enter a unique checksum key value in the **checksum** setting for the Pop integration being used (for example, the **checksum** setting within the **Hyland.Web.DocPop** element).
 - Set the **EnableLegacyChecksumFallback** setting to **true**.

Note: Setting the **EnableLegacyChecksumFallback** setting to **true** should be considered a temporary method of validating legacy checksums until you can recreate and replace the Pop integration URLs using the unique string value as the checksum key.

In addition to these actions, if your solution also uses an Application Server that generates Pop integration URLs outside of the Web Server, you must also take the following action to ensure successful checksum generation and validation:

- In the Application Server web.config file, enter the same unique checksum key value in the **ChecksumKey** setting within the **Hyland.Web.AppServerPop** element. The values in the Application Server **ChecksumKey** setting and Web Server **checksum** setting must match exactly.

If your solution was already using a unique string value to create checksum values, any Pop integration URLs that were previously created will continue to validate with no additional action needed.

Upgrading From Version 13 and Earlier

If you are upgrading from OnBase 13 or an earlier version, when attempting to use previously generated checksums with Pop integration URLs, the queries will no longer validate. Depending on how these legacy checksums were originally generated, you may be required to regenerate the Pop integration URLs:

- If a unique string value was not previously configured to create the legacy checksums, you must regenerate the Pop integration URLs. A unique checksum key value is required for checksum creation and validation, and a URL created without a checksum key will not validate.
- If a unique string value was previously configured to create the legacy checksums, you can still validate the URLs by taking the following actions.

Legacy checksums may be required for certain OnBase environments, such as environments where multiple versions of OnBase are used (for example, an Incremental Parallel Upgrade environment). If your solution requires checksums generated in OnBase 13 or earlier to still validate after an upgrade, then you must modify the following web.config setting for the Web Server:

- In the Web Server web.config file, set **EnableLegacyChecksumFallback** to **true**.

If you are using a version 14 or later Application Server that will be generating Pop integration URLs to be used with a version 13 or earlier Web Server, then you must modify all of the following web.config settings for the Application Server and Web Server:

- In the Application Server web.config file, set **EnableLegacyChecksumCreation** to **true**, and enter a checksum key value for the **ChecksumKey** setting.
- In the Web Server web.config file, set **EnableLegacyChecksumFallback** to **true**, and enter the same checksum key value for the **checksum** setting. The values in the Application Server **ChecksumKey** setting and Web Server **checksum** setting must match exactly.

By default, the legacy checksum settings are set to **false**, allowing only new checksums to be validated. Setting **EnableLegacyChecksumFallback** to **true** will allow previously generated checksums to be used.

If **EnableLegacyChecksumCreation** is set to **true**, then **EnableLegacyChecksumFallback** must also be set to **true**. When both settings are set to **false**, checksums will be created using the new method and legacy checksums will not be validated.

Note: It is recommended to keep **EnableLegacyChecksumCreation** set to **false**. If it is set to **true** to work with earlier OnBase versions, it should be set back to **false** once the earlier versions of OnBase Web Servers have been retired.

Installation

The Web Server and Application Server are installed using their own installers. You can install them using their installers, or you can install them manually.

Installer Options

Standard (EXE or MSI) Installers — There are two methods for running OnBase installers: Interactive and silent. An interactive installation requires user interaction with dialog boxes during the installation process. A silent installation does not require user interaction during the installation process.

OnBase installers may consist of both an executable file (.exe) and a Windows Installer Package file (.msi). When performing an interactive installation, and both an executable file and MSI are available, use the executable file to ensure a complete installation. The executable validates that all prerequisites are met before proceeding with the installation. If any missing prerequisites are identified, the installer alerts the user. Most missing prerequisites can be installed directly from the installer before continuing the installation process.

Note: The Microsoft .NET Framework prerequisite must always be installed separately before running either the EXE or MSI installer.

When performing a silent installation, and both an executable file and MSI are available, use the MSI. Since the MSI package does not validate prerequisites, you must ensure that Windows Installer 3.0 or greater is installed on each workstation and that all other prerequisites are met before running the MSI. If any prerequisites are not met, a silent installation from the MSI will fail without alerting the user.

For more information about configuring a silent installation, see <https://docs.microsoft.com/en-us/windows/win32/msi/command-line-options>.

ClickOnce Installers – Some OnBase modules are installed for deployment using ClickOnce. ClickOnce is a Microsoft technology that installs a deployment package to a central server. This package can then be accessed by users to install the application on their local workstations. The application is installed entirely under the user's profile, ensuring that it cannot interfere with other applications installed on the workstation.

ClickOnce deployments also have the following advantages:

- Previously installed versions of the module can be easily and automatically updated to the latest version with little or no user interaction, as long as the deployment server and deployment instance name are not changed.
- The module is installed on a per-user basis and does not require administrator privileges for local installation.
- There can be multiple instances of the module deployed, allowing for different versions of the module to be installed on a per-user basis, to match the version requirements of the workstation it is being installed to.

For more information on Microsoft's ClickOnce technology see <https://docs.microsoft.com/en-us/visualstudio/deployment/clickonce-security-and-deployment>.

Note: ClickOnce-deployed applications are not supported by Microsoft within a Remote Desktop environment.

OnBase modules that are deployed using ClickOnce should either take advantage of the ClickOnce deployment method as an alternative to a Remote Desktop deployment, or the module should be installed using a standard installer and deployed using the Remote Desktop methodology.

Note: Not all OnBase modules that support ClickOnce have a standard installer available. Contact your first line of support if you are unsure how to install and deploy a specific module.

User Account Control (UAC) — If Windows User Account Control (UAC) is enabled, the installer must be run with elevated administrator privileges, even if an administrator is currently logged on. This can be accomplished by right clicking on the installer executable and selecting **Run as Administrator** from the right-click menu. MSI files cannot be run using the **Run as Administrator** option. Instead, you must launch the MSI package using the command line. For more information on installing files through the command line, refer to your Microsoft support information or see <https://docs.microsoft.com/en-us/windows/win32/msi/command-line-options>.

Silent Installation Using setup.exe — If you are running setup.exe silently from the command line you must use the **/q** switch and the **/CompleteCommandArgs** switch, followed by the required command-line arguments.

The **q** switch specifies quiet mode and is required to suppress the GUI. The **CompleteCommandArgs** switch must be followed by the command-line parameters required to configure and install the desired components.

The complete string of command-line parameters must be included in double quotes after the **CompleteCommandArgs** switch. If a parameter in the string also requires double quotes, those quotes must be escaped using ****. For example: **setup.exe /q /CompleteCommandArgs "INSTALL_PROPERTY=\"my value\" INSTALL_PROPERTY_2=\"my value 2\""**.

Note: You should check the return value of the setup.exe process. A return value of **0** (zero) indicates success. Any other value returned may indicate that an error was encountered and the installation failed.

Installation Overview

The Web Server requires the OnBase Application Server to communicate with OnBase. Perform the following actions to install the Application Server and configure the Web and Application Servers to communicate with each other.

1. Configure the data source connection string to the OnBase database on the server where you install the Application Server. If multiple applications will be accessing different data sources through the Application Server, the data source connection string to each data source must be configured on the Application Server. An application accessing a data source must specify the name of the data source connection string on the Application Server as the name of the data source.
2. Run the Application Server installer. Running this installer ensures registry settings, permissions, and the OnBase Event Log are configured correctly. See the **Application Server** module reference guide for installation information.
3. Install the Web Server. See [Running the Installer on page 34](#) for instructions.
4. Configure the Web Server to communicate with the Application Server. See [Configuring Service Client Settings on page 51](#).

Running the Installer

This section describes installing the OnBase Web Server using the graphical installer.

For complete details on running the installer from the command line, see [Controlling the Installer from the Command Line on page 45](#).

For complete details on installing the Web Server manually, see the [Web Server Manual Installation Checklist on page 94](#).

If you are modifying or removing a previous installation, see [Change, Repair, or Remove an Installation on page 44](#).

Note: Before installing the Web Server, ensure that the OnBase Application Server is installed and configured correctly. See the **Application Server** module reference guide for complete information.

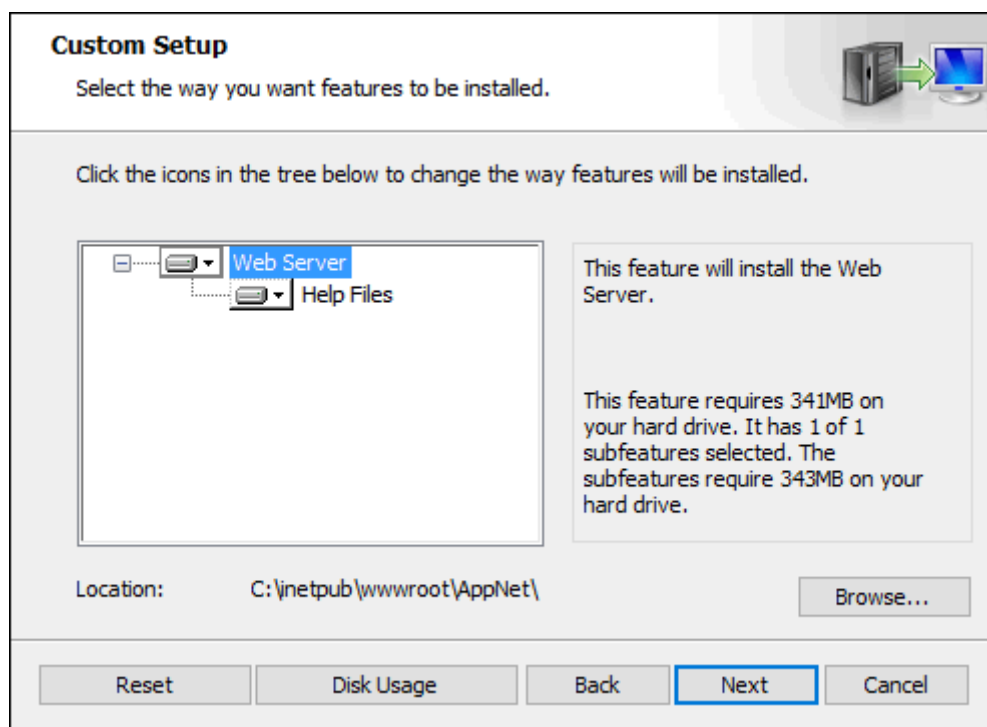
To install the Web Server:

1. Launch the Web Server installer by executing **setup.exe**. This executable is usually located in the **\install\Web Server** folder of your source installation files.

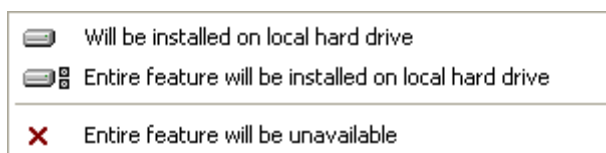
Note: If the installer is being copied from the source location to be run from a different location, the entire **Web Server** folder and its contents must be copied to the new location.

The welcome page is displayed. If you are modifying or removing a previous installation, the **Program Maintenance** dialog is displayed. See, [Change, Repair, or Remove an Installation on page 44](#).

2. Click **Next**. The **Custom Setup** page is displayed.



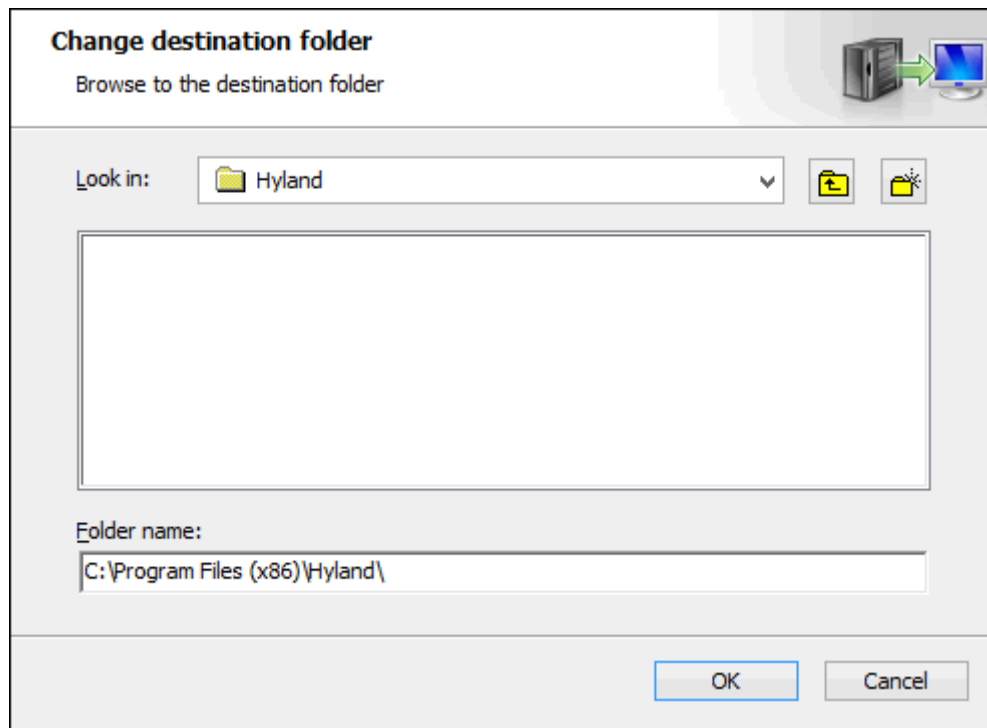
- Click the drop-down list beside the name of a component to display the installation options:



Option	Description
Will be installed on local hard drive	Installs the selected feature and does not install any dependent, optional functionality. To view optional functionality, click the + icon next to the feature to expand the sub feature list.
Entire feature will be installed on local hard drive	Installs the selected feature and any dependent functionality. To view the dependent functionality, click the + icon next to the feature to expand the sub feature list.
Entire feature will be unavailable	Select this option to remove a feature from the list of features to install.

- Select **This feature will be installed on local hard drive** for each component you want to install.
To install all components, select **Entire feature will be installed on local hard drive** from the drop-down list beside the top-level component.
- To determine the amount of space available for installation of the selected components, click **Disk Usage**. The **Disk Space Requirements** dialog box is displayed, with information on the space required for the selected components and the space available on the drives accessible by the installation machine.

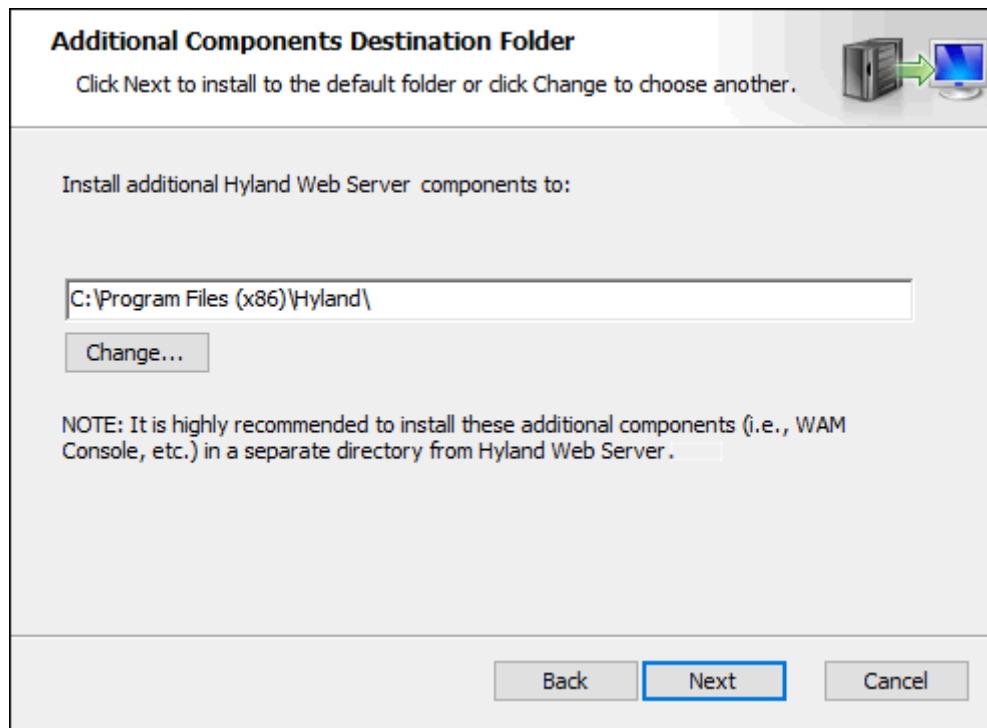
6. To change the installation location of a component, select it and click **Browse**. The **Change destination folder** dialog box is displayed.



Enter a **Folder name** in the field provided or select it from the **Look in** drop-down list. If the destination folder is not changed, components are installed to the default locations listed in the following table.

Component	Default Location
Web Server	<p>C:\Inetpub\wwwroot\AppNet\</p> <hr/> <p>Note: The installer only supports installation to a virtual directory. You cannot use the installer to install to a Web site root. The OnBase Web and Application Servers cannot be installed to the same virtual directory. The name of the virtual directory must match the configured Application Name for the server.</p> <hr/>
Help Files	<p>The Web-based help files are installed to the same location as the Web Server.</p> <hr/> <p>Note: If the help files are not installed users cannot search for help from the Web-based modules.</p> <hr/>

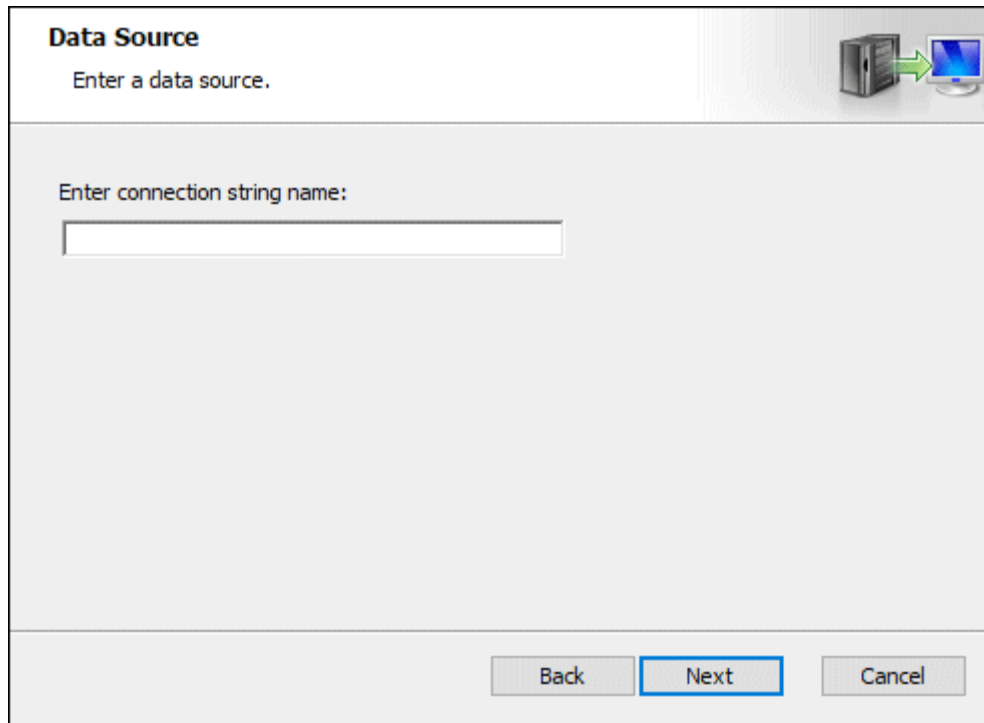
- Click **Next**. The **Additional Components Destination Folder** page is displayed.



To change the installation location of additional components being installed with the Web Server (such as the Web Application Management Console), enter a new folder location or click **Change** to navigate to the folder location.

Note: It is highly recommended to install additional components in a separate directory from the Web Server.

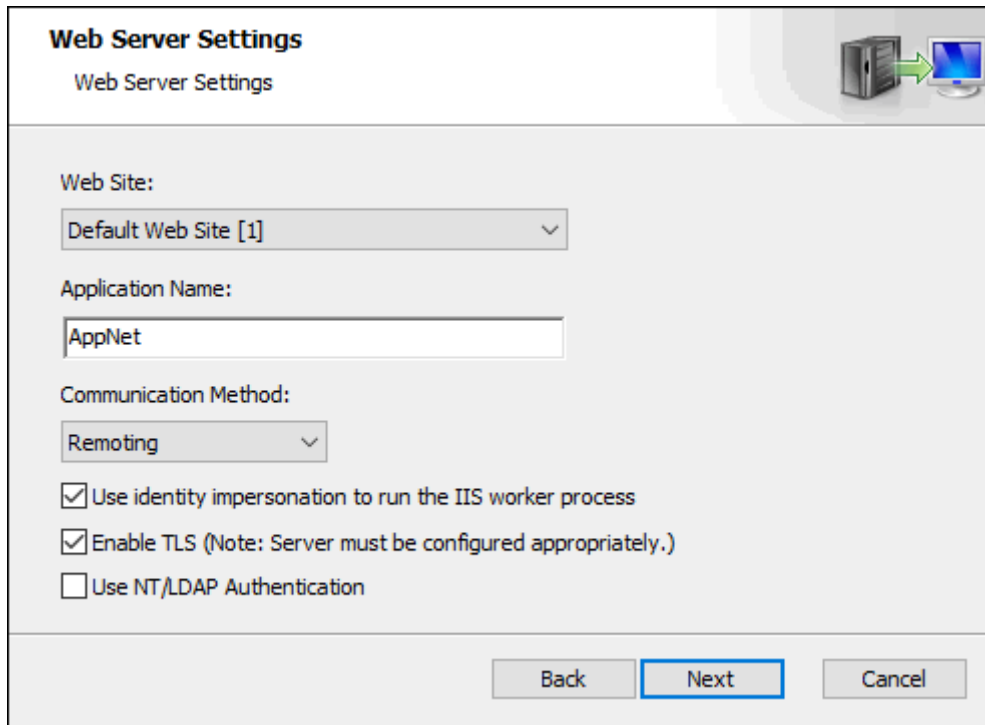
- Click **Next**. The **Data Source** page is displayed.



The image shows a 'Data Source' dialog box. At the top, it says 'Data Source' and 'Enter a data source.' To the right of this text is an icon of a server connected to a monitor by a green arrow. Below this, there is a label 'Enter connection string name:' followed by a text input field. At the bottom of the dialog, there are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a blue border.

- Enter the name of a valid connection string in the field.

10. Click **Next**. The **Web Server Settings** page is displayed.

The image shows a 'Web Server Settings' dialog box. At the top, it has the title 'Web Server Settings' and a subtitle 'Web Server Settings'. In the top right corner, there is an icon of a server rack connected to a computer monitor by a green arrow. The main area of the dialog contains three sections: 'Web Site:' with a drop-down menu showing 'Default Web Site [1]'; 'Application Name:' with a text box containing 'AppNet'; and 'Communication Method:' with a drop-down menu showing 'Remoting'. Below these are three checkboxes: 'Use identity impersonation to run the IIS worker process' (checked), 'Enable TLS (Note: Server must be configured appropriately.)' (checked), and 'Use NT/LDAP Authentication' (unchecked). At the bottom right, there are three buttons: 'Back', 'Next' (which is highlighted with a blue border), and 'Cancel'.

- Select a **Web Site** to install the OnBase Web Server to from the drop-down list. The **Web Site** list is populated with the Web servers configured in IIS and available to the target machine.
- Enter a name for the OnBase Web Server in the **Application Name** field.

Note: The OnBase Web and Application Servers cannot have the same Application Name. It is a best practice not to use parentheses in the Application Name.

- Under **Communication Method**, select the how the Web and Application Servers will communicate.

Remoting: .NET remoting allows the Web Server to use binary over HTTP to communicate with the Application Server. Remoting provides better performance than SOAP and is enabled by default. You may be unable to use remoting if a firewall needs to inspect the information passed between the Application Server and Web Server, such as when the two servers are hosted on different machines. In these situations, use SOAP.

SOAP: SOAP allows the Web Server to use XML SOAP over HTTP to communicate with the Application Server. This option is useful for load balancing or situations where a firewall needs to inspect the information passed between the Web Server and Application Server. If a load balancer is balancing traffic from the Web Server to the Application Server, then the Web Server must be configured to use SOAP.

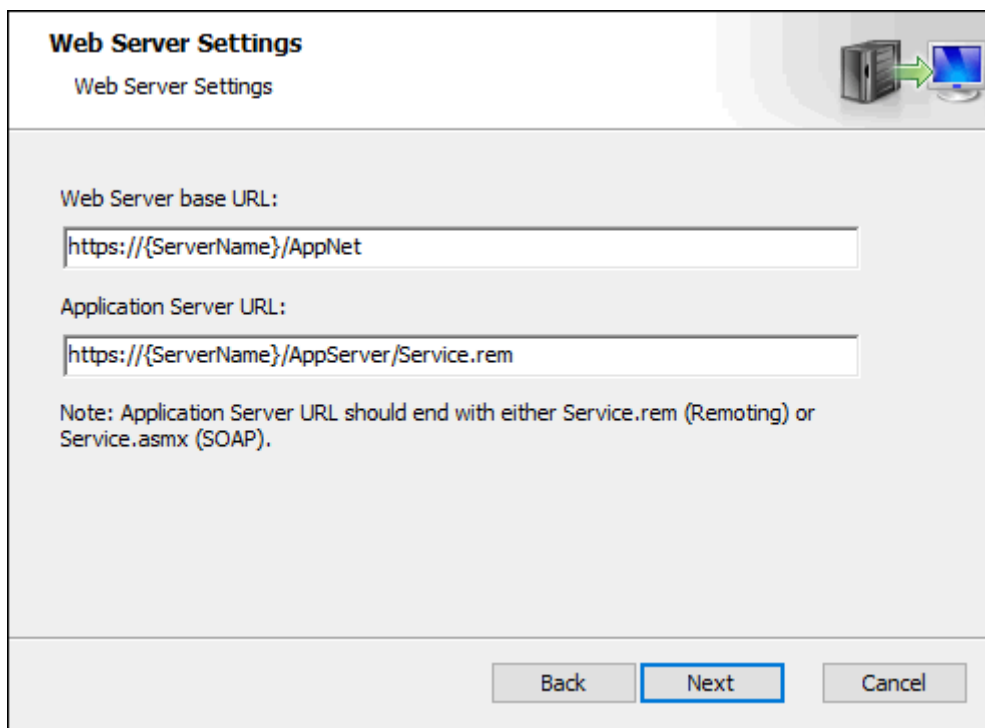
Tip: In most situations, select **Remoting** if the Web Server and Application Server are hosted on the same machine. If the Web Server and Application Server are hosted on different machines, select **SOAP**.

- Select **Use identity impersonation to run the IIS worker process** to use identity impersonation to run the installed OnBase Web server under the account specified. If this option is deselected then the server runs under the **Network Service** account. The impersonation account is granted modify rights to the directories and sub-directories of the Web Server. The installer does not add modify rights for any other groups.

Note: Ensure that the account the installed server is running under is granted modify rights to the server directories. If modify rights are not extended, you may experience permissions errors in modules attempting to modify files on the server.

- Select **Enable TLS** to run the Web Server with an HTTPS connection. If this option is selected, you must ensure that your server is correctly configured for HTTPS connections. If this option is deselected then an insecure network connection is used. You are prompted to acknowledge that you understand the risks associated with disabling this security layer before you can proceed with the installation.
- Select **Use NT/LDAP Authentication** to enable Active Directory or LDAP Authentication for the Web Server.

11. Click **Next**. The next **Web Server Settings** page is displayed.

The image shows a 'Web Server Settings' dialog box. At the top, it has the title 'Web Server Settings' and a subtitle 'Web Server Settings'. To the right of the title is an icon showing a server and a monitor connected by a green arrow. Below the title, there are two text input fields. The first is labeled 'Web Server base URL:' and contains the text 'https://{ServerName}/AppNet'. The second is labeled 'Application Server URL:' and contains the text 'https://{ServerName}/AppServer/Service.rem'. Below these fields is a note: 'Note: Application Server URL should end with either Service.rem (Remoting) or Service.asmx (SOAP)'. At the bottom of the dialog box are three buttons: 'Back', 'Next', and 'Cancel'. The 'Next' button is highlighted with a blue border.

- In the **Web Server base URL** field, enter the full URL to the OnBase Web Server you are installing. The default value populated in this field is based on previous installation selections and current user input. Ensure that the URL root entered is accurate. The URL must reflect the machine and virtual directory that will contain the OnBase Web Server.

Note: The installer only supports installation to a virtual directory. You cannot use the installer to install to a Web site root. If you selected **Enable TLS** earlier in the installation, the **Web Server base URL** must begin with **https://**. The name of the virtual directory must match the configured Application Name for the server.

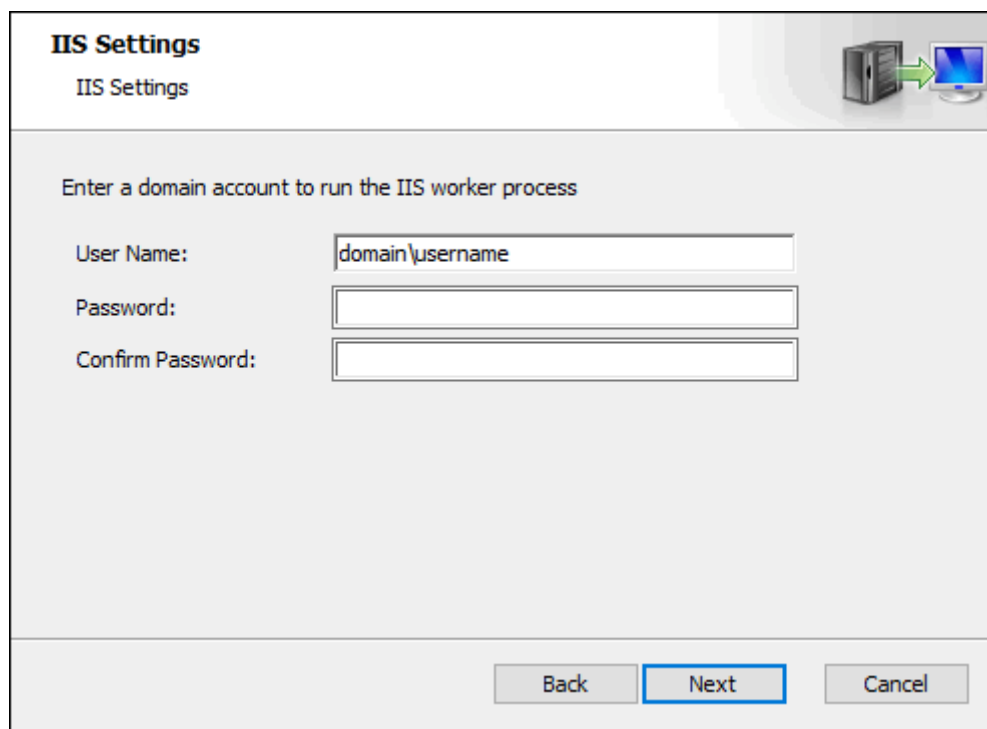
- In the **Application Server URL** field, enter the full URL to the **Service** page on the OnBase Application Server you are installing. The file extension of the service page depends on the **Communication Method** you selected for the Application Server. If you selected **Remoting**, the service page is **Service.rem**. If you selected **SOAP**, the service page is **Service.asmx**.

Tip: It is recommended to use **localhost** in the URL of the Application Server when it is being installed on the same machine as the OnBase Web Server. For example, **http://localhost/AppServer/Service.rem**.

The default value populated in this field is based on previous installation selections and current user input. Ensure that the URL entered is accurate. The URL must reflect the machine and virtual directory that will contain the OnBase Application Server.

Note: If you selected **Enable TLS** earlier in the installation, the **Application Server URL** must begin with **https://**. The name of the virtual directory must match the configured Application Name for the server.

12. If you selected **Use identity impersonation to run the IIS worker process** for the Web or Application Server settings, the **IIS Settings** page is displayed.



IIS Settings
IIS Settings

Enter a domain account to run the IIS worker process

User Name:

Password:

Confirm Password:

Back Next Cancel

- In the **User Name** field, enter the domain and user name to use to run the IIS worker process for your server. This must be entered in the **domain\username** format.
 - In the **Password** field, enter the password that corresponds to the user name provided.
 - In the **Confirm Password** field, re-enter the password that corresponds to the user name provided. This is used to ensure that the password is typed correctly.
13. Click **Next**. The **Ready to install...** page is displayed.
 14. Select **Create Desktop shortcut(s) when applicable** to create a shortcut to the Web Application Management Console on the Windows desktop.

15. Click **Install** to install the selected components.
Click **Back** to return to the previous dialog to change configuration options, or click **Cancel** to close the installer without installing any of the selected components.
16. When the **Completed the Hyland Web Server Setup Wizard** page is displayed, click **Finish** to complete the installation.

Note: In order to ensure that the required system settings take effect, it is a best practice to restart the installing machine once the installer has finished.

17. After the Web Server is installed it must be configured to communicate with the Application Server. See [Configuring Service Client Settings on page 51](#).

Change, Repair, or Remove an Installation

After initial installation, the setup program can be used to change, repair, or remove components from a previous installation. After launching **setup.exe** or the ***.msi** installation package, and clicking **Next** at the welcome dialog, the **Change, repair, or remove installation** dialog box is displayed.

Select the option for the actions you wish to perform:

Option	Description
Change	<p>Add or remove components using the Custom Setup dialog.</p> <hr/> <p>Note: This option is not available if the installer has no independently selectable features.</p> <hr/> <p>The steps for adding selected components are the same as those under the Component Selection section of the installation instructions, if applicable to the installer.</p> <hr/> <p>Note: Change does not allow you to alter configuration options originally set during a previous installation of components contained in the installer.</p> <hr/>
Repair	<p>Repair errors in the most recent installation of the component, such as missing and corrupt files, shortcuts, and registry entries.</p> <hr/> <p>Note: This option is not available from all installers. Repair does not include errors made in the configuration options set by the user during installation. For specific troubleshooting information regarding an installed component, see the module reference guide for that component.</p> <hr/>
Remove	<p>Removes all previously installed components.</p>

Controlling the Installer from the Command Line

The Hyland Web Server installer can be run from an installation CD or a local drive. If upgrading from a previous installation that used the Hyland Web Server installer, it is not necessary to uninstall the old components before running the installer.

Silent Installation Using setup.exe

If you are running setup.exe silently from the command line you must use the **/q** switch and the **/CompleteCommandArgs** switch, followed by the required command-line arguments.

The **/q** switch specifies quiet mode and is required to suppress the GUI. The **CompleteCommandArgs** switch must be followed by the command-line parameters required to configure and install the desired components.

The complete string of command-line parameters must be included in double quotes after the **CompleteCommandArgs** switch. If a parameter in the string also requires double quotes, those quotes must be escaped using ****. For example: **setup.exe /q /CompleteCommandArgs "INSTALL_PROPERTY=\"my value\" INSTALL_PROPERTY_2=\"my value 2\""**.

Note: You should check the return value of the setup.exe process. A return value of **0** (zero) indicates success. Any other value returned may indicate that an error was encountered and the installation failed.

Feature and Property Names

The following sections describe the feature and property names that can be applied to the command line to install and configure components contained in the Hyland Web Server installer.

Features define the components that are installed. Properties define the configuration settings for the components that are installed.

Feature Names

You can control the installation of components from the command line using the **ADDLOCAL** property. To install a component, pass its feature name to the installer using the **ADDLOCAL** property. The table below lists the feature names for each component in the Hyland Web Server installer.

The **ADDLOCAL** property is appended to the end of the install command line, as shown in this example:

```
msiexec /i "Hyland Web Server 16.msi" ADDLOCAL=Web_Server,Web_Server_Help
```

This example installs the OnBase Web Server and the help files. It also installs any components required by the features selected.

Note: Feature names are case sensitive and must be added to the command line exactly as they appear in this table. The associated properties listed may also have to be included on the command line in order to configure the installed component. For details on the associated properties see, [Property Names on page 46](#).

Component	Feature Name	Associated Properties
Web Server	Web_Server <hr/> Note: You must have IIS installed with at least one Web site in order to install the Web Server. Installing this component also installs the Web Applications Management Console . <hr/>	WEBSERVER_FILES APPSERVER_APPLICATION_NAME DATASOURCE IIS_ASPNET_USER IIS_ASPNET_PASS WEBSERVER_APPLICATION_NAME WEBSERVER_APPSERVER_URL WEBSERVER_IIS_ASPNET_IMPERSONATION WEBSERVER_IIS_NTAUTH WEBSERVER_IIS_TLS WEBSERVER_IIS_WEBSITE_ID WEBSERVER_SERVICECLIENTTYPE WEBSERVER_URL
Help Files	Web_Server_Help	<hr/> Note: There are no properties for this component. <hr/>

Property Names

When controlling the installation of components from the command line you must also configure the settings for each component you are installing by using the properties listed in the following sections. The sections below list the property names available and the corresponding features that use them.

Installation Locations

The following table lists the properties that control the installation locations for each feature.

Note: To set a specific installation location for a feature, enter the full path to the installation directory to use. If the installation location property for a feature is not included, the feature is installed to the default location listed in this table.

Component / Feature Name	Property Name / Default Location
Web Server Web_Server	WEBSERVER_FILES C:\Inetpub\wwwroot\AppNet\ <hr/> Note: The installer only supports installation to a virtual directory. You cannot use the installer to install to a Web site root. The OnBase Web and Application Servers cannot be installed to the same virtual directory. The name of the virtual directory must match the configured Application Name for the server.
Help Files Web_Server_Help	<Web Server location>\Help\ <hr/> Note: In order for the help files to function correctly, this location cannot be changed.

Configuration Options

Note: In order to make a property empty, set its value to an empty string on the command line. For example, **WEBSERVER_IIS_ASPNET_IMPERSONATION** accepts **1** to enable impersonation or no value to disable impersonation. In other words, to disable impersonation the property is set like this on the command line:

WEBSERVER_IIS_ASPNET_IMPERSONATION="".

APPSERVER_APPLICATION_NAME

The name for the OnBase Application Server in IIS. If this property is not included, the default value of **AppServer** is used.

For example: **APPSERVER_APPLICATION_NAME="AppServer"**

Required when adding:

- Web_Server

DATASOURCE

The name of the data source for OnBase that the installed components will use.

For example: **DATASOURCE="My Data Source Name"**

Required when adding:

- Web_Server

IIS_ASPNET_USER

The domain user account to use for identity impersonation. This must be entered in the **domain\username** format. If this property is not included, the default value of **domain\username** is used.

For example: **IIS_ASPNET_USER="domain\username"**

Required when the following property is set to **1**:

- WEBSERVER_IIS_ASPNET_IMPERSONATION

IIS_ASPNET_PASS

The password for the IIS_ASPNET_USER user name entered.

For example: **IIS_ASPNET_PASS="password"**

Required when the following property is set to **1**:

- WEBSERVER_IIS_ASPNET_IMPERSONATION

WEBSERVER_APPLICATION_NAME

The name for the OnBase Web Server in IIS. If this property is not included, the default value of **AppNet** is used.

For example: **WEBSERVER_APPLICATION_NAME="AppNet"**

Required when adding:

- Web_Server

WEBSERVER_APPSERVER_URL

The base URL of the OnBase Application Server's virtual directory. The name of the virtual directory must match the configured Application Name for the server.

Tip: It is recommended to use **localhost** in the URL of the Application Server when it is being installed on the same machine as the OnBase Web Server. For example, **http://localhost/AppServer**.

For example: **WEBSERVER_APPSERVER_URL="http://localhost/AppServer"**

Required when adding:

- Web_Server

WEBSERVER_IIS_ASPNET_IMPERSONATION

Enter **1** to enable IIS identity impersonation and run the OnBase Web Server under the account specified. The impersonation account is granted modify rights to the directories and sub-directories of the Web Server (in a default installation, **AppNet** is the Web Server directory). The installer does not add modify rights for any other groups.

To disable identity impersonation, this property must be included and the value left empty. If identity impersonation is disabled, the server runs under the **Network Service** account.

If this property is not included, the default value of **1** is used and IIS identity impersonation is enabled.

Note: Ensure that the account the installed Web Server is running under is granted modify rights to the server directories. If modify rights are not extended, you may experience permissions errors in modules attempting to modify files on the server.

For example: **WEBSERVER_IIS_ASPNET_IMPERSONATION="1"** or
WEBSERVER_IIS_ASPNET_IMPERSONATION=""

Required when adding:

- Web_Server

If set to **1**, the following properties are required:

- IIS_ASPNET_PASS
- IIS_ASPNET_USER

WEBSERVER_IIS_NTAUTH

Enter **1** to enable Active Directory or LDAP Authentication for the Web Server.

For example: **WEBSERVER_IIS_NTAUTH="1"**

Optional when adding:

- Web_Server

WEBSERVER_IIS_TLS

Enter **1** to run the Web Server using an HTTPS connection. If this option is enabled you must ensure that your server is correctly configured for HTTPS connections.

To disable this option, this property must be included and the value left empty. If HTTPS connections are disabled, an insecure network connection is used (HTTP).

If this property is not included, the default value of **1** is used and HTTPS connections are enabled.

For example: **WEBSERVER_IIS_TLS="1"**

Optional when adding:

- Web_Server

WEBSERVER_IIS_WEBSITE_ID

The identifier number of the Web site in IIS that the OnBase Web Server will be installed to. Web site identifiers are found in the **Internet Information Services (IIS) Manager**. If you have only one Web site under IIS (e.g., **Default Web Site**), its number is typically **1**.

For example: **WEBSERVER_IIS_WEBSITE_ID="1"**

Required when adding:

- Web_Server

WEBSERVER_SERVICECLIENTTYPE

Enter **Remoting** if the Web Server and Application Server are hosted on the same machine. If the Web Server and Application Server are hosted on different machines, enter **SOAP**. This corresponds to the **Communication Method** setting in the graphical interface. If this property is not included, the default value of **Remoting** is used.

For example: **WEBSERVER_SERVICECLIENTTYPE="Remoting"** or
WEBSERVER_SERVICECLIENTTYPE="SOAP"

Required when adding:

- Web_Server

WEBSERVER_URL

The base URL of the OnBase Web Server's virtual directory.

For example: **WEBSERVER_URL="http://web-server/AppNet"**

Note: The installer only supports installation to a virtual directory. You cannot use the installer to install to a Web site root. If you set **WEBSERVER_IIS_TLS="1"** the URL must begin with **https:**. The name of the virtual directory must match the configured Application Name for the server.

Required when adding:

- Web_Server

Post-Installation

After you have installed the Web Server, ensure that any antivirus software is properly configured. Read the [Impact of Running Antivirus Software on the OnBase Web Server](#) on page 56.

Configuring Service Client Settings

After installing the Web Server application, you must configure it to communicate with the Application Server for services. Determine whether the Web Server application will use .NET remoting or SOAP to communicate with the Application Server. For information about these communication methods, see [Remoting on page 51](#) and [SOAP on page 51](#).

Remoting

.NET remoting allows the Web Server application to use binary over HTTP to communicate with the Application Server. Remoting provides better performance than SOAP and is enabled by default.

You may be unable to use remoting if a firewall needs to inspect the information transmitted between the Application Server and Web Server application.

1. In the Application Server's Web.config file, ensure that the **useRemoting** attribute in the **Endpoint** element is set to **true**.
2. In the Web Server application's Web.config file, under **Hyland.Services.Client**, set the **ServiceClientType** attribute to **Remoting**.
3. In the same element, set the **URL** to the URL of the service page on the Application Server.

Ensure **.rem** is the extension on the service page. For example: **<ApplicationServer URL="https://server1/AppServer/service.rem" ServiceClientType="Remoting">**.

SOAP

SOAP allows the Web Server application to use XML SOAP over HTTP to communicate with the Application Server. This option is useful for load balancing or Internet situations where firewalls need to inspect the XML passed between the Web Server application and Application Server.

Note: If a load balancer is balancing traffic from the Web Server application to Application Server, then the Web Server application must be configured to use SOAP.

1. In the Web Server application's Web.config file, under **Hyland.Services.Client**, set the **ServiceClientType** attribute to **SOAP**.
2. In the same element, set **ApplicationServer URL** to the URL to the service page on the Application Server.

Ensure **.asmx** is the extension on the service page. For example: **<ApplicationServer URL="https://server1/AppServer/service.asmx" ServiceClientType="SOAP">**.

Enabling Impersonation

Both the Web Server and Application Server installers provide the option to enable identity impersonation for both the Web and Application Server.

Note: By default, the impersonation setting is set to **false**. The exception to this is if a previous Web Server install was done on your machine, the Impersonation option defaults to the last known setting.

If you enable impersonation for an application, the installer inserts a new identity element into that application's Web.config file and creates the encrypted credential values in the registry. If you did not select the impersonation option, you can configure impersonation manually.

Note: Full details on creating encrypted account registry keys are available in the Microsoft article: "How to use the ASP.NET utility to encrypt credentials and session state connection strings" available at: <http://support.microsoft.com/kb/329290/>

Tip: Impersonation can be configured using the Web Application Management Console. See the **Web Application Management Console** module reference guide for more information.

For best practices on using impersonation, see [IIS and ASP.NET Configuration for Web Server Autologin on page 333](#).

To manually configure impersonation, complete the following steps:

1. From a command line, change the directory to the location where the aspnet_setreg.exe tool resides. A copy of this tool is provided in the **..\utilities\misc** subdirectory in the build distribution package.
2. Enter the following command, where **YourApp** is the name of the directory where the Application Server or Web Server is installed, **DOMAIN** is the domain for the impersonation account, **name** is the user name of impersonation account, and **password** is the password for the impersonation account.

```
aspnet_setreg.exe -k:SOFTWARE\Hyland\YourApp\Identity -u:"DOMAIN\name"  
-p:"password"
```

3. Open a **Run** dialog box and enter **regedt32**.

4. Grant the application pool's identity account **Read** permissions to the appropriate registry key.

- In 32-bit environments, grant the **Read** permission on:
HKLM:SOFTWARE\Hyland\YourApp\Identity\ASPNET_SETREG
- In 64-bit environments, grant the **Read** permission on:
HKLM:SOFTWARE\Wow6432Node\Hyland\YourApp\Identity\ASPNET_SETREG

The aspnet_setreg utility automatically stores the encrypted credentials in these keys when impersonation is configured for the Web or Application Server in these environments.

Note: If the application pool is configured to use the built-in ApplicationPoolIdentity account, then the IIS_IUSRS group must be granted **Read** access to the registry key.

Caution: Modify the registry at your own risk. Incorrectly editing the Windows registry can cause serious problems that may require you to reinstall your operating system. Be sure to back up the registry before making any changes to it. For more registry information, see the following Microsoft articles: <http://support.microsoft.com/kb/256986> and <http://technet.microsoft.com/en-us/library/cc725612.aspx>

5. Open the application's web.config file from the directory where it was installed. By default, server applications are installed in the following locations:
 - Application Server (32-bit): **C:\inetpub\wwwroot\AppServer**
 - Application Server (64-bit): **C:\inetpub\wwwroot\AppServer64**
 - Web Server: **C:\inetpub\wwwroot\AppNet**
6. Uncomment the **<identity>** element by removing the **<!--** and **-->** located above and below it.

```
<!--
<identity impersonate="false"
  userName="registry:HKLM\SOFTWARE\Hyland\AppNet\Identity\ASPNET_SETREG,userName"
  password="registry:HKLM\SOFTWARE\Hyland\AppNet\Identity\ASPNET_SETREG,password"
/>
```

7. Ensure **impersonate** is set to **true**.
8. Save the web.config file.
9. If you are configuring impersonation for the Application Server, grant the impersonated identity account **Modify** permissions to the OnBase disk group storage locations and other domain locations where resources such as style sheets are stored.

Disabling Impersonation

To disable impersonation, comment out the **identity** element from the application's Web.config. If you only set **impersonate** to **false**, .NET Framework still causes the application to check the registry for the encrypted credentials, even though the credentials are not used for impersonation. This behavior can cause issues if the registry key doesn't exist or if the identity account is denied access to the key.

To comment out the **identity** element, add `<!--` above the element and `-->` below the element, as shown below.

```
<!--  
<identity impersonate="false"  
  userName="registry:HKLM\SOFTWARE\Hyland\AppNet\Identity\ASPNET_SETREG,userName"  
  password="registry:HKLM\SOFTWARE\Hyland\AppNet\Identity\ASPNET_SETREG,password"  
>
```

Active Directory Authentication

Additional configuration is required if OnBase is configured for Active Directory authentication. For comprehensive information about configuring the Web Server for Active Directory authentication, see the **Legacy Authentication Methods** module reference guide.

Key requirements include the following, which are explained in detail in the **Legacy Authentication Methods** module reference guide:

1. Set **enableAutoLogin** in the Web Server's Web.config to **true**.
2. Set **AllowNTAuthenticationOnForwarding** in the Web Server's Web.config to **true**.
3. Disable anonymous access on the Web Server's virtual directory.
4. If you are using **Active Directory - Enhanced** authentication and interactive autologon, if alternate binding credentials are specified, then check to make sure that the alternate binding credentials have Account Operators permissions. If you are using non-interactive autologon, ensure the alternate binding credentials have domain querying rights.

For information about configuring impersonation, see [Enabling Impersonation on page 52](#).

5. If you are using **Active Directory - Enhanced** authentication and non-interactive autologon, complete the additional requirements in [Required Configuration Settings for Non-Interactive Active Directory Authentication on page 58](#).

Note: These requirements are intended as a quick guide for configuring the Web Server for Active Directory authentication. To use Active Directory authentication, you must configure OnBase for Active Directory authentication as described in the **Legacy Authentication Methods** module reference guide. This guide also provides additional information about multiple site configurations and troubleshooting.

Additional Active Directory Authentication Steps for Firefox

If the Web Server is configured for autologon using Active Directory authentication, Firefox users who access the HTML Web Client will be prompted for their credentials by the browser. To allow Firefox users to access the Web Client without being prompted, use the following workaround.

Note: The following steps affect only the current workstation and the currently logged-on user. For enterprise deployments, the specified settings would need to be modified in the pref.js file found in each user's Firefox profile. Consider using the tools described at the following site: https://wiki.mozilla.org/Deployment:Deploying_Firefox#Deployment_Tools

1. Open Firefox.
2. Type **about:config** into the address bar.
3. Click **I'll be careful, I promise!** if prompted.
4. Locate the following settings by typing **trusted** in the **Search** field provided:
 - **network.automatic-ntlm-auth.trusted-uris** (for NTLM)
 - **network.negotiate-auth.trusted-uris** (for Kerberos)
5. Double-click each setting and enter a comma-delimited list of trusted Web servers. For example:
srv-web001,srv-web002,srv-web003
When a Firefox user accesses the HTML Web Client through any of these servers, the browser will not prompt the user for credentials.
6. Restart Firefox. If the user who logged on to the computer has permission to access the Web Server virtual directory, the browser will not prompt the user for credentials.

Note: If you encounter the error "HTTP Error 401.1 - Unauthorized: Access is denied due to invalid credentials," see the Microsoft KB article located at the following URL: <http://support.microsoft.com/kb/871179>

Note: To allow Mac users to log on using Active Directory authentication, you may need to perform additional steps.

Integration for Single Sign-On

Additional configuration is required if your solution includes the OnBase Integration for Single Sign-On. For comprehensive information about configuring the Web Server to use Single Sign-On, see the **Legacy Authentication Methods** module reference guide.

Configuring the Web Client for Two Authentication Types

Follow these steps to configure a single virtual directory with two login pages, where one page automatically logs users on to OnBase and the other page requires users to enter their credentials.

1. Configure the Web Server for autologon. See [Active Directory Authentication on page 54](#).
2. Create a copy of the **Login.aspx** page in the Web Server virtual directory.
3. Rename the copy appropriately, keeping the **aspx** extension. For example: **ManualLogin.aspx**
4. Open the Web Server's Web.config.
5. Above the **<appSettings>** node, add the following, where **ManualLogin.aspx** is the name of the copied login page.

```
<location path="ManualLogin.aspx">
  <appSettings>
    <add key="loginPage" value="ManualLogin.aspx" />
    <add key="EnableAutoLogin" value="false" />
  </appSettings>
</location>
```

With this configuration, users who access the Web Client through the ManualLogin.aspx page will have to log on manually, while users who access the Login.aspx page will be logged on automatically.

Impact of Running Antivirus Software on the OnBase Web Server

Modifying the contents of the Web Server or Application Server virtual directories will cause the applications to restart. When this occurs, connected users will lose their sessions and their applications will become unresponsive. This behavior occurs because the OnBase Web Server and Application Server are ASP.NET Web Applications. ASP.NET detects file changes, including changes to file system attributes and time stamps, and restarts the application if a change is detected.

Unintended application restarts can occur when virus scanning software, backup software, or indexing services access the contents of an application's virtual directory. These processes don't modify the contents of an application's files, but they can modify the files' attributes, which is enough for ASP.NET to restart the application. To properly configure virus scanning, backup software, or indexing service software, follow these guidelines:

- Exclude the virtual directories for the OnBase Web Server and Application Server and the ASP.NET Temporary Files directory from antivirus, backup, or indexing service scanning. The ASP.NET Temporary Files directory is below:

- 32-bit installations:

C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files

- 64-bit installations:

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files

If these files are scanned by antivirus, backup, or indexing software, IIS will restart the application pool for the OnBase application. When an application pool restarts, all existing OnBase sessions are reset, causing errors for connected users.

- Real-time scanning of script execution, which is available in some antivirus software, should only be engaged according to the software manufacturer's instructions. Some manufacturers do not intend this functionality to be used on servers.

Consult your antivirus software's documentation for other recommended settings for Web servers. Ensure that any virus scanning changes will not be overwritten by the automatic policy settings configured for your network.

Loss of Session Context

When antivirus software scans the virtual directory of a Web server application like the OnBase Web Server, this scanning may cause the application to restart. As a result, users currently logged on to the application lose their sessions, and the application becomes unresponsive. For OnBase applications, the OnBase Event Log records the **Application End** and **Application Start** events, which are followed by a series of errors. The Diagnostics Console logs the message: **Failed to get session for session id.**

The recommended solution is to disable antivirus software from scanning the server's virtual directories as well as the ASP.NET Temporary Files in the following locations:

- 32-bit installations:

C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files

- 64-bit installations:

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files

The Microsoft Knowledge Base describes this issue in greater detail. For more information, refer to the following articles:

- <http://support.microsoft.com/kb/821438>
- <http://support.microsoft.com/kb/312592/en-us?spid=8940&sid=global>
- <http://support.microsoft.com/kb/316148/EN-US/>

Decreased Performance and Scalability

Antivirus software running on a Web server or client workstation may have adverse effects on system performance. Two known issues regarding McAfee® VirusScan® with ScriptScan are described below.

If you have any questions, please contact your solution provider.

The following recommendation is for:

- Performance Issues on Servers Running McAfee VirusScan
- Performance Issues on Client Workstations Running McAfee VirusScan

Recommendation for Performance Issues on Servers and Client Workstations

Servers running any OnBase server application, and workstations running the OnBase Web Client or Medical Records Management Solution will exhibit decreased performance when running McAfee VirusScan with ScriptScan enabled.

The recommended solution from McAfee is to first test whether whitelisting solves any problems. If it does not, then you will need to disable ScriptScan.

The McAfee Knowledge Base describes this issue in greater detail. For more information, refer to the following article:

https://kc.mcafee.com/corporate/index?page=content&id=KB65382&actp=null&viewlocale=en_US&showDraft=false&platinum_status=false&locale=en_US

Required Configuration Settings for Non-Interactive Active Directory Authentication

Additional configuration is required to maintain the authentication credentials of web applications in OnBase when the following conditions are met:

- OnBase is configured to use **Active Directory - Enhanced** as the authentication method
- OnBase is configured to use non-interactive/autologons

Non-interactive authentication is configured in OnBase by de-selecting the **Interactive User Authentication** options in the **Directory Service Authentication** dialog box. When non-interactive authentication is used, the domain account currently logged in to the workstation is used to authenticate the user in OnBase.

Note: If **Active Directory - Enhanced** is not the authentication method configured, or **Interactive User Authentication** is enabled, additional configuration is not required.

This section describes the additional configuration required in order to use non-interactive/autologon Active Directory authentication with OnBase web applications, including the OnBase Application Server.

To complete the additional configuration you must configure the Microsoft Windows environment, configure the OnBase Application Server, and configure the web applications of your OnBase modules.

These processes are described in the following sections:

- To configure the Microsoft Windows environment, see [Registering a Service Principal Name \(SPN\) and Configuring Delegation in Microsoft Windows](#) on page 59.
- To configure the OnBase Application Server, see [Configuring the Application Server](#) on page 60.
- To configure OnBase web applications, see, [Configuring Web Applications](#) on page 62.

Tip: Additional information may be available in the **Directory Service Authentication** whitepaper, available from your first line of support.

Registering a Service Principal Name (SPN) and Configuring Delegation in Microsoft Windows

Before configuring any OnBase web applications, you must first:

- Register a Service Principal Name (SPN) to a domain account in Microsoft Windows
- Set the registered SPN account to trust delegation in Active Directory

Note: The SPN only needs to be registered once for the HTTP service on the server, even though a server may host one or more OnBase web applications.

The domain account that is registered as the SPN must be the same as the application pool identity that is running all of the application pools for OnBase web applications on the server.

The SPN is registered using the Microsoft Windows **Setspn** command-line tool. To successfully register the SPN, you must have domain administrative privileges on the server or be logged in under a user account with those privileges delegated to it.

Note: Setspn is a Microsoft tool. For complete details on registering SPNs and using the Setspn tool, see the documentation provided by Microsoft for Windows servers. The example included in this section is for illustration purposes only.

For example, to register the SPN for the HTTP service, for fully qualified domain name **myserver.mydomain.net**, to the application pool identity **jdoe**, type:

```
Setspn -s HTTP/myserver.mydomain.net mydomain\jdoe
```

After registering the SPN you must also set that user account to trust delegation. This is configured in Microsoft Windows by launching the **Active Directory Users and Computers** toolkit with elevated administrator privileges.

Note: Active Directory is a Microsoft product. Complete details on using and configuring Active Directory can be found in the documentation provided by Microsoft.

In the **Active Directory Users and Computers** toolkit:

1. Navigate to the **Users** dialog.
2. Search for the domain account you registered the SPN to.
3. Open the properties for that account and select the **Delegation** tab.
4. Configure that account to trust delegation for services.

Note: It is considered a best practice to use constrained delegation by selecting **Trust the user for delegation to specified service only** and selecting **Use Kerberos only**. However, if other services are using the same account, this configuration may not always be possible. For more information on constrained delegation, see the **Kerberos Constrained Delegation** information available from Microsoft.

Configuring the Application Server

The OnBase Application Server can be optimized for non-interactive Active Directory authentication using the **Optimize for Windows Authentication** tool in the Web Application Management Console.

Note: Before configuring any OnBase web applications, ensure that the identity running the application pool for the module is registered as the SPN. See [Registering a Service Principal Name \(SPN\) and Configuring Delegation in Microsoft Windows on page 59](#).

To use the **Optimize for Windows Authentication** tool and configure the Application Server:

1. Launch the Web Application Management Console.

Tip: For complete details on installing and using the Web Application Management Console, see the **Web Application Management Console** module reference guide.

2. Click **Open Web Application** in the upper left of the window.
3. Select the Application Server from the **Select the web application to configure** list.
4. Select **Tools | Optimize for Windows Authentication**.
5. Click **Yes** in the confirmation dialog that is displayed.
6. Save the configuration and close the Web Application Management Console.

7. In Microsoft Windows, launch the **Internet Information Services (IIS) Manager** with elevated administrator privileges.

Note: IIS is a Microsoft product. Complete details on using IIS and the IIS Manager can be found in the documentation available from Microsoft.

8. In the **Sites** area, configure the following settings for the web application of the OnBase Application Server.

Setting	Configuration
IIS Authentication Anonymous Authentication	Set to Enabled .
IIS Authentication ASP.NET Impersonation	Set to Disabled .
IIS Authentication Windows Authentication	Set to Disabled . <hr/> Note: Additionally, Negotiate must be at the top of the list of providers. To access the providers list, right click Windows Authentication and select Providers . <hr/>

9. If the OnBase Application Server is hosted on a different server from the other OnBase web applications, you must also complete the following configuration:
 - a. Under **Management**, launch the **Configuration Editor** for the web application of the OnBase module.
 - b. From the **Section** drop-down list, navigate to the **system.webServer/security/authentication/windowsAuthentication** path.
 - c. Set the value of **useAppPoolCredentials** to **False**.
10. Under the **Default Web Site**, expand the pages under the OnBase Application Server and select the **AuthService.asmx** page.
11. Configure the following settings for the **AuthService.asmx** page.

Setting	Configuration
IIS Authentication Anonymous Authentication	Set to Disabled .
IIS Authentication ASP.NET Impersonation	Set to Disabled .
IIS Authentication Windows Authentication	Set to Enabled . <hr/> Note: Additionally, Negotiate must be at the top of the list of providers. To access the providers list, right click Windows Authentication and select Providers . <hr/>

12. In the **Application Pools** area, configure the following setting for the application pool of the OnBase Application Server.

Setting	Configuration
Process Model Identity	The domain account you registered the SPN to (see Registering a Service Principal Name (SPN) and Configuring Delegation in Microsoft Windows on page 59).

13. Recycle the application pool of the OnBase Application Server for the changes to take effect.

Tip: To configure the OnBase web applications that use the Application Server, see [Configuring Web Applications on page 62](#).

Configuring Web Applications

A web application is any OnBase module installed to IIS that presents a web-based interface to the user. This includes, but is not limited to, modules such as the OnBase Web Server, DeficiencyPop, and the OnBase Patient Window.

If a module requires the OnBase Application Server to connect to OnBase but is not installed to IIS, that module does not require additional configuration as long as the Application Server is configured correctly (see [Configuring the Application Server on page 60](#)). This includes modules like the OnBase Unity Client.

Several OnBase modules can be optimized for non-interactive Active Directory authentication using the **Optimize for Windows Authentication** tool in the Web Application Management Console.

Note: Before configuring any OnBase web applications, ensure that the identity running the application pool for the module is registered as the SPN. See [Registering a Service Principal Name \(SPN\) and Configuring Delegation in Microsoft Windows on page 59](#).

To use the **Optimize for Windows Authentication** tool and configure a web application:

1. Launch the Web Application Management Console.

Tip: For complete details on installing and using the Web Application Management Console, see the **Web Application Management Console** module reference guide.

2. Click **Open Web Application** in the upper left of the window.

3. Select the module from the **Select the web application to configure** list. The configuration for that module is loaded into the Web Application Management Console.

Note: If the OnBase module you are configuring is not in the list, it cannot be optimized using the Web Application Management Console. You may need to manually change the settings described in the remainder of this procedure.

- a. Click **Tools | Optimize for Windows Authentication**.
 - b. Click **Yes** in the confirmation dialog that is displayed.
4. Save the configuration and close the Web Application Management Console.
 5. In Microsoft Windows, launch the **Internet Information Services (IIS) Manager** with elevated administrator privileges.

Note: IIS is a Microsoft product. Complete details on using IIS and the IIS Manager can be found in the documentation available from Microsoft.

6. In the **Sites** area, confirm that the following settings for the web application of the OnBase module are configured correctly.

Setting	Configuration
IIS Authentication Anonymous Authentication	Set to Enabled . <hr/> Note: For some OnBase modules this setting may need to be set to Disabled . However, this is not the preferred configuration because setting it to Disabled may cause performance issues.
IIS Authentication ASP.NET Impersonation	Set to Enabled . <hr/> Note: Additionally, the Impersonation setting must be set to Authenticated User .
IIS Authentication Windows Authentication	Set to Enabled . <hr/> Note: Additionally, Negotiate must be at the top of the list of providers. To access the providers list, right click Windows Authentication and select Providers .

7. Under **Management**, launch the **Configuration Editor** for the web application of the OnBase module.
8. From the **Section** drop-down list, navigate to the **system.webServer/security/authentication/windowsAuthentication** path.
9. Set the value of **useAppPoolCredentials** to **True**.

10. In the **Application Pools** area, confirm that the following setting for the application pool of the web application is configured correctly.

Setting	Configuration
Process Model Identity	The domain account you registered the SPN to (see Registering a Service Principal Name (SPN) and Configuring Delegation in Microsoft Windows on page 59).

11. Recycle the application pool of the OnBase module for the changes to take effect.
12. Repeat this process for each OnBase web application in your environment.

Tip: To configure the OnBase Application Server, see [Configuring the Application Server on page 60](#).

Java API

Installing the Java API Interface

Please contact your first line of support for legacy Java API information.

Updating an Existing Hyland.jar JAVA API Installation

Please contact your first line of support for legacy Java API information.

Automatic Query Execution Upon Logon

Automatic query execution provides users instant access to search results as soon as they log on to the Web Client. Similar to DocPop queries, these searches can be based on a Custom Query, Document Type Group, Document Type, Keyword value, or document handle (docID). Search results are displayed using the Web Client interface, allowing users to perform additional searches and navigate to other areas of the Web Client as their privileges allow.

To use this feature, modify the URL to the Web Client's login page to include a query string containing the necessary search parameters.

URL Creation Methods

Because Web Client query strings are similar in construction to DocPop query strings, you can use the DocPop URL creator to build the necessary query structure for the login URL. Then, modify the resulting URL as needed for submission to the Web Client's login.aspx page.

Queries also can be built manually; however, you must use the correct syntax to ensure the queries execute properly.

See the following topics for more information:

- [Modifying DocPop URLs for Web Client Use on page 65](#)
- [Creating Web Client URLs Manually on page 66](#)

Modifying DocPop URLs for Web Client Use

The DocPop URL Creator page allows you to create a DocPop URL querying for the desired documents. You can then modify the URL for submission to the login page.

Note: Although Web Client query strings and DocPop query strings are similar in construction, there are some differences between them. See [Differences Between DocPop & Web Client URLs on page 70](#) for an overview.

The following steps describe how to modify a DocPop URL for use with the Web Client:

1. Create a DocPop URL for the documents you want to retrieve. See the DocPop module reference guide for DocPop URL Creator steps and more DocPop query information.

The following is an example of a properly configured DocPop URL:

```
http://<machine>/AppNet/docpop/docpop.aspx?clienttype=activex&docid=5375
```

Note: To use the DocPop URL Creator, you must configure the **datasource** setting in the **Hyland.Web.DocPop** element in the Web Server's Web.config. However, the DocPop configuration settings do not affect queries submitted to the login.aspx page. Configuring the DocPop settings is not necessary for automatic query execution in the Web Client.

2. Replace **docpop/docpop.aspx** with **login.aspx**.

`http://<machine>/AppNet/login.aspx?clienttype=activex&docid=5375`

3. Replace the **clienttype=activex** or **clienttype=html** parameter (if present) with the **query=true** parameter

`http://<machine>/AppNet/login.aspx?query=true&docid=5375`

If the **clienttype** parameter is not present in the DocPop query string, then append **&query=true** to the end of the query string.

Creating Web Client URLs Manually

1. Begin with a URL to the Web Client login page, as shown in the following example:

`http://serverweb1/AppNet/Login.aspx`

2. Append **?query=true** to the login URL.

`http://serverweb1/AppNet/Login.aspx?query=true`

Note: Each additional parameter you append to the query string must be preceded by an ampersand (&).

3. Append one of the parameters from the following table to the login URL. For example, to execute a Custom Query with an ID number of 152, you would append **&cqid=152**.

`http://serverweb1/AppNet/Login.aspx?query=true&cqid=152`

Query String Parameter	Query String Value
cqid	The number of the Custom Query to be executed, if a Custom Query is being performed.
docid	The document handle of the document to retrieve, if a document number query is being performed. To retrieve multiple documents, enter multiple document handles. Separate each handle with a comma (no spaces). For example: docid=5820,6112,6904
doctypegroupid	The number of the Document Type Group to search by, if a Document Type Group query is being performed.
doctypeid	The number of the Document Type to search by, if a Document Type query is being performed.

Query String Parameter	Query String Value
keytype	The name of the Keyword Type to search by, if the query is restricted by Keyword values. See the following topic, Keyword Parameters , to apply Keyword parameters to your search.

4. If applicable, append the necessary Keyword parameters to the query string. See [Keyword Parameters on page 67](#).

`http://serverweb1/AppNet/Login.aspx?query=true&cqid=152&KT102_0_2_0=500.00`

5. Append any additional parameters as needed. See [Optional Parameters on page 69](#).

`http://serverweb1/AppNet/
Login.aspx?query=true&cqid=152&KT102_0_2_0=500.00&FromDate=08%2f31%2f2012`

Note: Keyword or date parameters containing special characters must conform to URL encoding rules. For example, in date values, slashes (/) must be replaced with %2f. Consult an HTML reference guide for more information.

Keyword Parameters

Keyword parameters specify the Keyword Types and values used for retrieval and how the values relate to each other. The format for Keyword parameters is displayed below. The bracketed items represent variables, which are described in the table at the end of this section.

KT[Keyword Type Number]_[Instance Number]_[Comparative Operator Number]_[Logical Operator Number]=[Keyword Value]

For an example of how parameters look in a query string, see the [Keyword Parameters Example on page 68](#).

If a Keyword value uses a specific currency format, add the following parameter for each value:

KTCF[Keyword Type Number]_[Instance Number]=[Currency Format Number]

The variables required in the Keyword parameter are described in the following table:

Variable	Description
Keyword Type Number	The Keyword Type's internal number as defined in OnBase. This is the number displayed in the upper-right corner of the Keyword Type Configuration dialog box when the Keyword Type is selected in OnBase Configuration.

Variable	Description
Instance Number	The Keyword value's position relative to other values provided for the same Keyword Type. The number for the first instance of the Keyword Type is 0 . If there are two values for a single Keyword Type, the second value would have an instance number of 1 .
Comparative Operator Number	The numeric value that specifies which comparative operator to use with the Keyword value. Possible values are listed below: <ul style="list-style-type: none"> • 0 for = (equal to) • 1 for < (less than) • 2 for > (greater than) • 3 for <= (less than or equal to) • 4 for >= (greater than or equal to) • 5 for <> (does not equal) • 6 for " " (exactly matches)
Logical Operator Number	The numeric value that specifies which logical (boolean) operator to use when multiple Keyword values are provided for a single Keyword Type. Possible values are listed below: <ul style="list-style-type: none"> • 0 for AND • 1 for OR • 2 for TO
Keyword Value	The Keyword value you want to use to limit your search.
Currency Format Number	The currency format ID for Keyword values that require a specific currency format. This is the number displayed in the upper-right corner of the Currency Format Configuration dialog box when the currency format is selected in OnBase Configuration.

Keyword Parameters Example

Suppose you are searching within a range of account numbers, and you want to limit your search to account numbers from 1500 to 2000. On the URL Creator page, you could enter these values in the Keyword Type fields, as shown below.

The screenshot shows a dialog box with two input fields. The first field is labeled 'Account #' with a '>=' operator to its right, and contains the value '1500'. To the right of this field is a button labeled 'TO'. The second field is also labeled 'Account #' with a '<=' operator to its right, and contains the value '2000'.

In the query string on the URL, these parameters are formatted as shown below:

KT51_0_4_2=1500&KT51_1_3_0=2000

Notice that each numeral represents a variable as described in the table above:

- The Keyword Type number for Account # is **51**. You can determine the number of any Keyword Type using the OnBase Configuration module.
- The first Keyword value has an instance number of **0**. The second Keyword value has an instance number of **1**.
- Because you are searching for values from 1500 to 2000, the comparative operator on the first Keyword value is \geq , which is represented by the number **4**. The comparative operator on the second Keyword value is \leq , which is represented by the number **3**.
- The Boolean operator, TO, is represented by the number **2**. Because there are only two values for the Keyword Type, only the operator from the first Keyword value is needed to describe the relationship between the values. The operator on the second Keyword value, 0, is ignored because there are no additional Keyword values for the Keyword Type.
- The Keyword value follows the equal sign. The first Keyword value is **1500**; the second is **2000**.

Optional Parameters

You can append the following additional parameters to the login query string:

Query String Variable Name	Query String Value
datasource	The name of the data source to use for the query.
FromDate	Used when searching for a document by date or within a particular range: FromDate is the beginning search date (mm-dd-yyyy format). This parameter is often used in conjunction with ToDate .
ToDate	Used when searching for a document by date or within a particular range: ToDate is the ending search date (mm-dd-yyyy format). This parameter is often used in conjunction with FromDate .
pageID	Used only with the Document # query type, pageID indicates the page number the specified document should open to.

Query String Variable Name	Query String Value
sessionID	<p>Passes the session ID on the query string. This parameter is useful if a custom application uses the Web Client to retrieve documents, and the session needs to be controlled by the application.</p> <hr/> <p>Note: When the session ID is created through a custom application, the session will not automatically be disconnected by OnBase, and the license will remain in use. It is the responsibility of the application that creates the session ID to disconnect the session when it is done, which will release the license.</p> <hr/> <p>For information about creating session IDs, see the Hyland SDK.</p> <hr/>

Differences Between DocPop & Web Client URLs

Although DocPop and Web Client URLs are constructed similarly, there are some basic differences, including the following:

- Web Client query strings are passed to the login.aspx page in the Web Server's virtual root. DocPop query strings are passed to the docpop.aspx page in the DocPop directory.
- Web Client query strings must include the **query=true** parameter.
- You do not need to configure DocPop's Web.config settings for Web Client query strings to work.
- The document select list is always displayed for Web Client queries.
- The Web Client's login page ignores the **username** and **password** query string parameters used by DocPop and FolderPop.
- The Web Client's login page ignores the **ClientType** query string parameter used by DocPop. To change the client type used by the Web Client, see [Configuring the Web Client Type on page 258](#)
- The Web Client's login page ignores the **viewerOnlyForSingle** and **displaySingle** parameters used by DocPop.

Backup and Recovery

The following sections describe how to backup and recover the OnBase Application Server or Web Server using IIS on Windows Server. For database backup and recovery procedures, see the **System Administration** module reference guide.

Note: Backup and recovery on IIS requires that all IIS configuration settings be backed up and restored. For information about backing up and restoring IIS configuration, see the IIS documentation from Microsoft.

Backup

Server recovery requires a backup of the following files:

File(s)	Default Location
Web.config for the Application Server or Web Server	C:\<Virtual Root>\<OnBase Directory>\
Hyland Services configuration files	C:\inetpub\wwwroot\
Machine.config for ASP	OnBase 6.4 or earlier: %windir%\Microsoft.NET\Framework\v1.1.4322\CONFIG\ OnBase 7.2 through OnBase 9.2: %windir%\Microsoft.NET\Framework\v2.0.50727\CONFIG\ OnBase 10.0 or later: %windir%\Microsoft.NET\Framework\v4.0.30319\CONFIG\
Application pool settings	See Exporting Application Pool and Virtual Directory Settings on page 71 .
Virtual directory settings	See Exporting Application Pool and Virtual Directory Settings on page 71 .

Backup these files and settings whenever they are modified.

Exporting Application Pool and Virtual Directory Settings

Backup your IIS configuration settings according to Microsoft's instructions, found in the following Microsoft KB article:

<http://support.microsoft.com/kb/954872>

Recovery

You can recover the OnBase Application Server or Web Server from backed up files. Before you begin, ensure no instances of the OnBase Client and Configuration modules are open on the server machine.

1. Stop IIS. From a command prompt, type **iisreset -stop** and press **Enter**.
2. Remove the OnBase installation on the server.
 - a. If the OnBase server was installed using the installer, you can remove the installation using Add or Remove Programs from the Control Panel.
 - b. If the OnBase server was installed manually, you must manually unregister and remove all OnBase files.
3. Ensure all OnBase files in **%windir%\system32** (or **%windir%\SysWow64**, on a 64-bit system) have been removed. These files may create conflicts with the new installation.
4. Run the installer for the latest version of the OnBase Application Server. Use the installer for the version you are recovering to restore that version.
5. From backup, copy or restore the following files to their appropriate locations:

File(s)	Default Location
Web.config for the Application Server or Web Server	C:\<Virtual Root>\<OnBase Directory>\
Hyland Services configuration files	C:\inetpub\wwwroot\
Machine.config for ASP.NET	OnBase 6.4 or earlier: %windir%\Microsoft.NET\Framework\v1.1.4322\CONFIG\ OnBase 7.2 through OnBase 9.2: %windir%\Microsoft.NET\Framework\v2.0.50727\CONFIG\ OnBase 10.0 or later: %windir%\Microsoft.NET\Framework\v4.0.30319\CONFIG\
Application pool settings	See Restoring the Application Pool and Virtual Directory Settings on page 72 .
Virtual directory settings	See Restoring the Application Pool and Virtual Directory Settings on page 72 .

6. Start IIS after all files and settings are restored. From a command prompt, type **iisreset -start** and press **Enter**.

The OnBase server has been restored.

Restoring the Application Pool and Virtual Directory Settings

Restore your IIS configuration settings according to Microsoft's instructions, found in the following Microsoft KB article:

<http://support.microsoft.com/kb/954872>

Start IIS after all files and settings are restored. From a command prompt, type **iisreset -start** and press **Enter**.

The Web Server has been restored.

Desktop Host is a component that enables cross-platform desktop capabilities in web applications and module-specific functionality in the OnBase HTML Web Client. To determine if a web application or module requires Desktop Host, see the installation or requirements documentation for that product. If an application or module requires it, Desktop Host should be installed on workstations used to access the web application or Web Client.

Note: Desktop Host is supported only in a single-user environment scenario. It is not supported for shared or virtualized environments.

This chapter contains information on installing, configuring, and troubleshooting Desktop Host.

Installing Desktop Host

This section describes installing Desktop Host using the graphical installer.

See the following sections for specific instructions on these topics:

- [Microsoft Windows Requirements on page 74](#)
- [Upgrade Considerations on page 75](#)
- [Running the Windows Installer on page 75](#)
- [Change, Repair, or Remove an Installation for Windows on page 80](#)
- [Installing Silently from the Command Line on page 80](#)
- [Running the macOS Installer on page 81](#)
- [Removing an Installation for macOS on page 86](#)

Note: Before you run the Desktop Host installer, it is recommended that you configure a whitelist. See [Whitelisting a Domain on page 86](#) for complete information.

Microsoft Windows Requirements

General Visual C++ Requirements

Both 32-bit and 64-bit versions of the Desktop Host require the Microsoft Visual C++ Redistributable Packages listed below. If not already present on your system, these packages are installed when the installer is executed to install Desktop Host.

If you are using a 32-bit system, the following Microsoft Visual C++ Redistributable Package is required:

- Microsoft Visual C++ 2019 Redistributable Package (x86)

If you are using a 64-bit system, the following Microsoft Visual C++ Redistributable Package is required:

- Microsoft Visual C++ 2019 Redistributable Package (x64)

Upgrade Considerations

This section describes upgrading an installation of Desktop Host using the graphical installer.

Upgrading an Installation on Windows

To upgrade Desktop Host, launch the latest Desktop Host installer by executing the installer. Before proceeding with an upgrade, it is recommended that you back up your existing configurations.

Upgrading an Installation on macOS

To upgrade Desktop Host, launch the latest Desktop Host installer by executing the installer **Hyland Desktop Host.pkg**. Before proceeding with an upgrade, it is recommended that you back up your existing configurations.

Running the Windows Installer

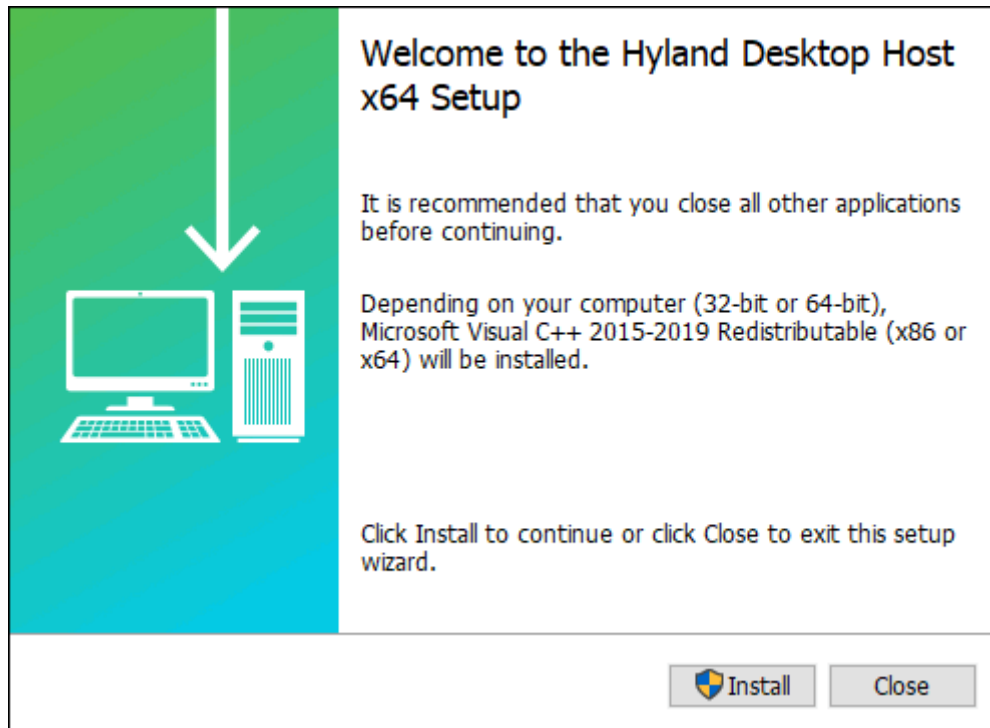
This section describes installing Desktop Host using the graphical installer for Windows. For illustration purposes, the screenshots below reference the 64-bit installer.

Note: If you are using Firefox and installing Desktop Host for the first time or reinstalling it, it is recommended that you configure Firefox. See [Firefox Restricts Desktop Host on page 91](#) for complete information.

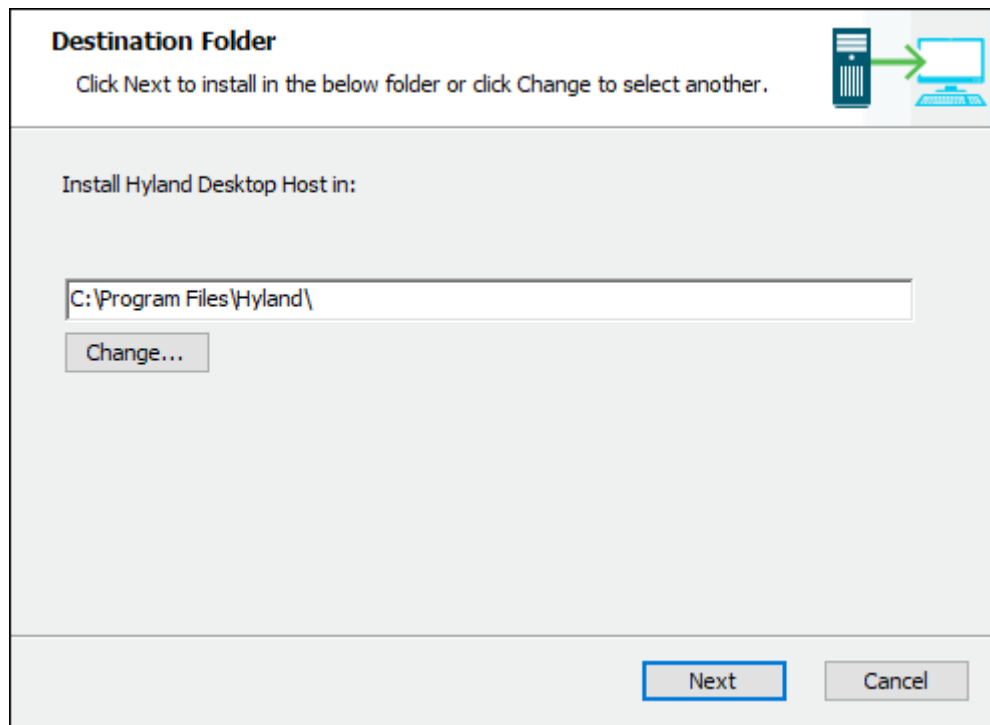
Caution: Ensure that you use the 32-bit and 64-bit installers to install the application on 32-bit and 64-bit computers, respectively.

To install Desktop Host:

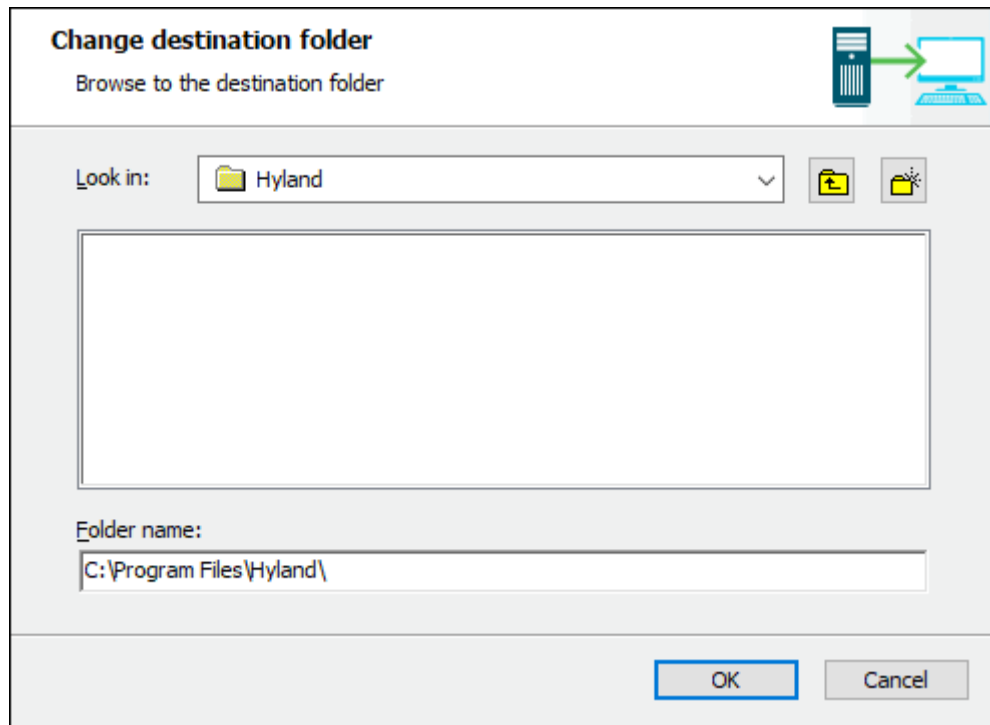
1. Launch the Desktop Host installer by executing the installer (**HylandDesktopHostSetup.x86.exe** or **HylandDesktopHostSetup.x64.exe**). The **Welcome to Hyland Desktop Host Setup** page is displayed.



2. Click **Install**. If Microsoft Visual C++ 2015-2019 Redistributable (x86 or x64) is not present, depending on your computer (32-bit or 64-bit), it is installed.
The **Destination Folder** page is displayed.



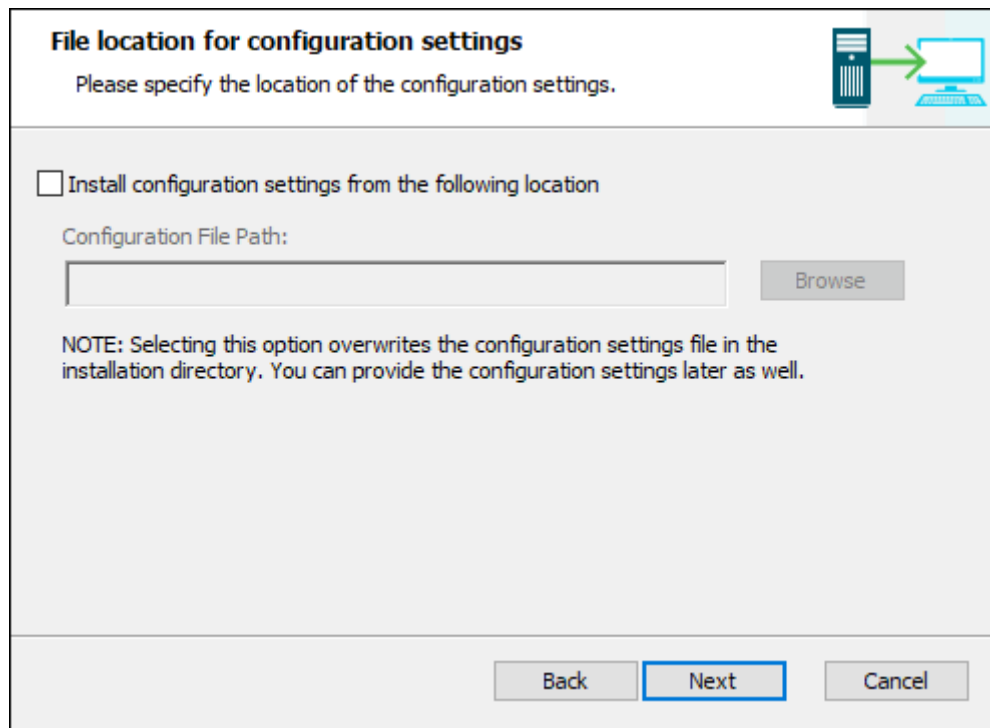
3. To change the installation location, enter a new folder location in the field provided or click **Change** to navigate to the folder location. The **Change destination folder** dialog box is displayed.



Note: If the destination folder is not changed, the application is installed to **C:\Program Files\Hyland\DesktopHost** by default.

4. Enter the full path for the destination folder in the **Folder name** field provided or select the folder from the **Look in** drop-down list.

5. Click **Next**. The **File location for configuration settings** page is displayed.



6. To specify the folder where the **config.json** file is present, select the **Install configuration settings from the following location** check box.

Note: Selecting this option overwrites the **config.json** file in the installation directory. You can skip this step and provide the configuration settings after installation is complete.

7. Enter the full path for the folder in the **Configuration File Path** field provided or click **Browse**.
8. Click **Next**. The **Ready to install** page is displayed.
Click **Back** to return to the previous page to change configuration options, or click **Cancel** to close the installer without installing.

Note: You may need to enter the Administrator password to continue installation.

9. After the **Installation completed** page is displayed, click **Close** to complete the installation and exit the installer.

Change, Repair, or Remove an Installation for Windows

After initial installation, the installer can be used to repair or remove components from a previous installation. Launch the installer and select the option for the action you want to perform:

Option	Description
Change	This option is unavailable for Desktop Host.
Repair	Repair errors in the most recent installation of the application, such as missing and corrupt files, shortcuts, and registry entries.
Uninstall	Removes all previously installed components.

Installing Silently from the Command Line

This section describes installing Desktop Host silently and optionally specifying the location of the custom **config.json** file during installation.

This procedure installs the application to the default installation location at **C:\Program Files\Hyland\DesktopHost**.

If you are running the installer silently from the command line you must use the **/silent** switch. The **/silent** switch specifies the quiet mode and is required to suppress the GUI.

Caution: Ensure that you use the 32-bit and 64-bit installers to install the application on 32-bit and 64-bit computers, respectively.

To install Desktop Host silently:

1. Launch a command prompt with elevated privileges.
2. Navigate to the directory on your computer where the Desktop Host installer is located.
3. Enter the complete name of the installer executable (**HylandDesktopHostSetup.x86.exe** or **HylandDesktopHostSetup.x64.exe**) within double quotes, followed by a space.

For example:

"HylandDesktopHostSetup.x64.exe"

4. To specify the location of the custom config.json file, enter **DH_CUSTOM_CONFIG_PATH="[path]"** where **[path]** is the full path to the custom **config.json** file. The path must be a full absolute path (including the file name), within double quotes, and followed by a space.

For example:

```
"HylandDesktopHostSetup.x64.exe"
```

```
DH_CUSTOM_CONFIG_PATH="C:\DesktopHostInstaller\bin\config.json"
```

Note: If you specify the **DH_CUSTOM_CONFIG_PATH** parameter, the **config.json** file in the installation directory is overwritten. You can also skip this step and provide the configuration settings after installation is complete.

5. Enter **/silent** and press **Enter** to execute the command.

For example:

```
"HylandDesktopHostSetup.x64.exe"
```

```
DH_CUSTOM_CONFIG_PATH="C:\DesktopHostInstaller\bin\config.json" /silent
```

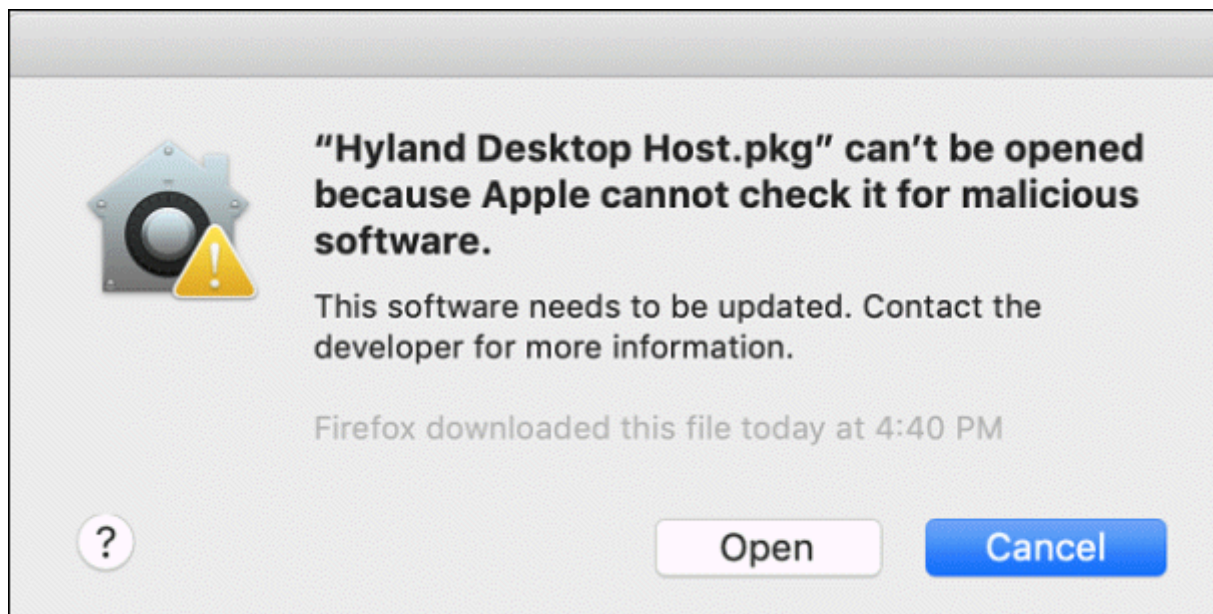
Running the macOS Installer

This section describes installing Desktop Host using the graphical installer for macOS.

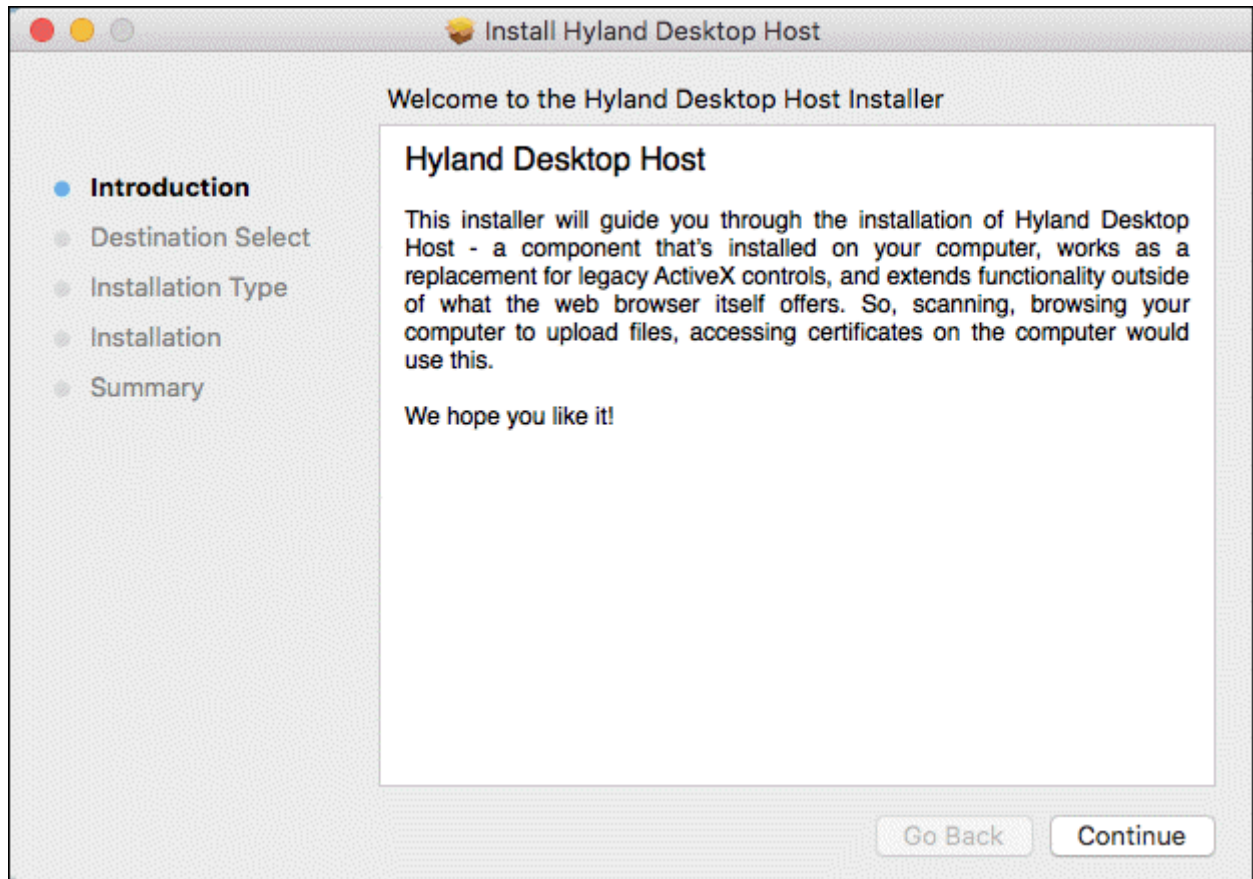
Note: If you are using Firefox and installing Desktop Host for the first time or reinstalling it, it is recommended that you configure Firefox. See [Firefox Restricts Desktop Host on page 91](#) for complete information.

To install Desktop Host:

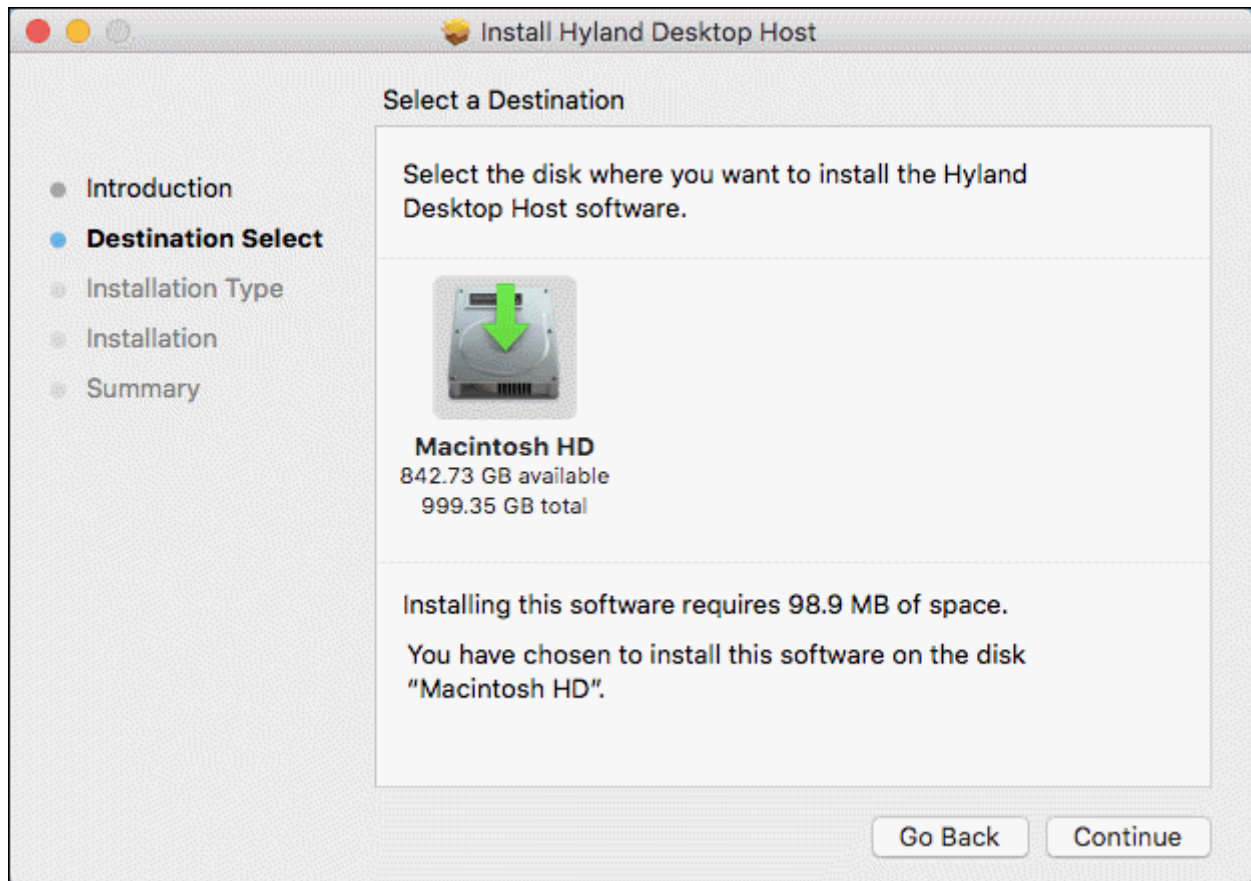
1. Right-click on **Hyland Desktop Host.pkg**, select **Open With**, and then select **Installer (default)**. The following dialog box is displayed.



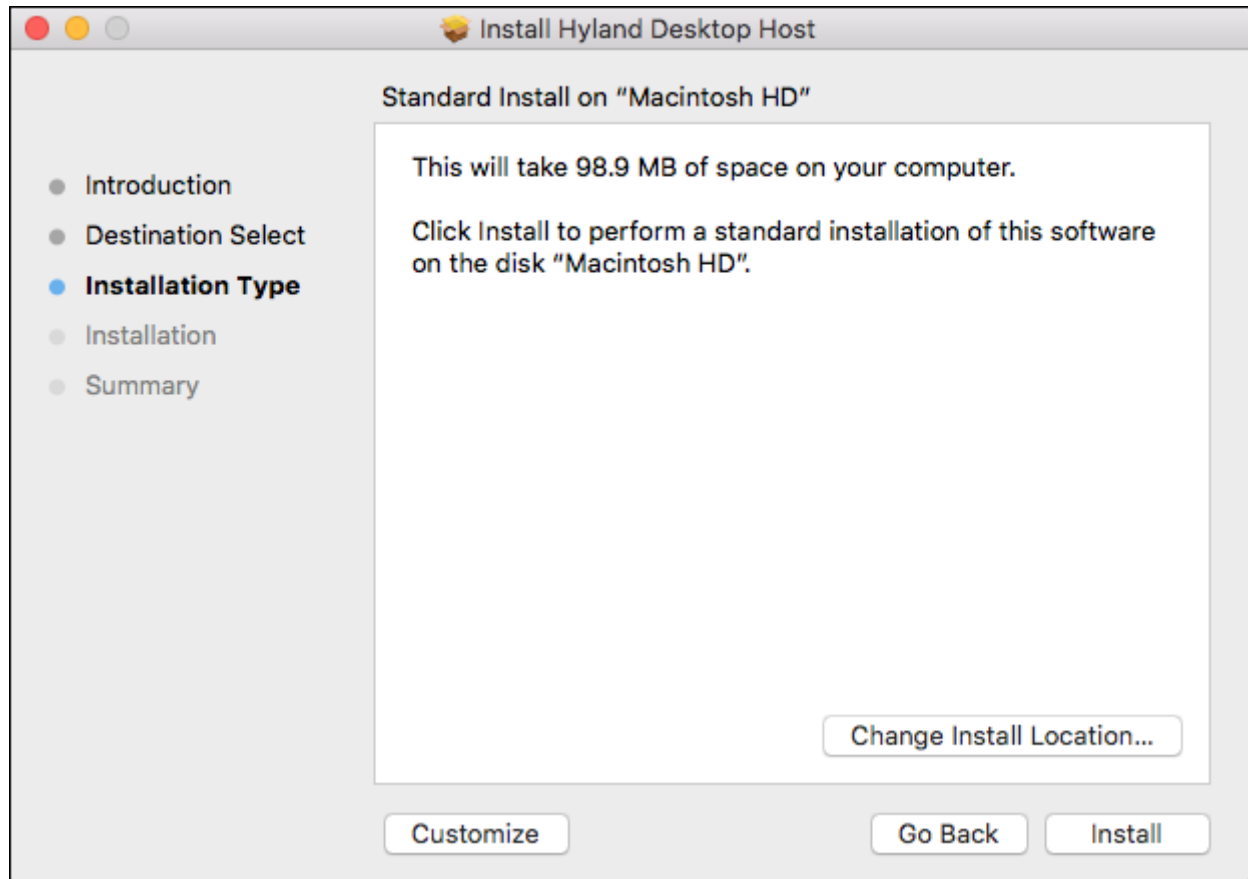
2. On the dialog box, click **Open**. The **Welcome to Hyland Desktop Host Installer** page is displayed.



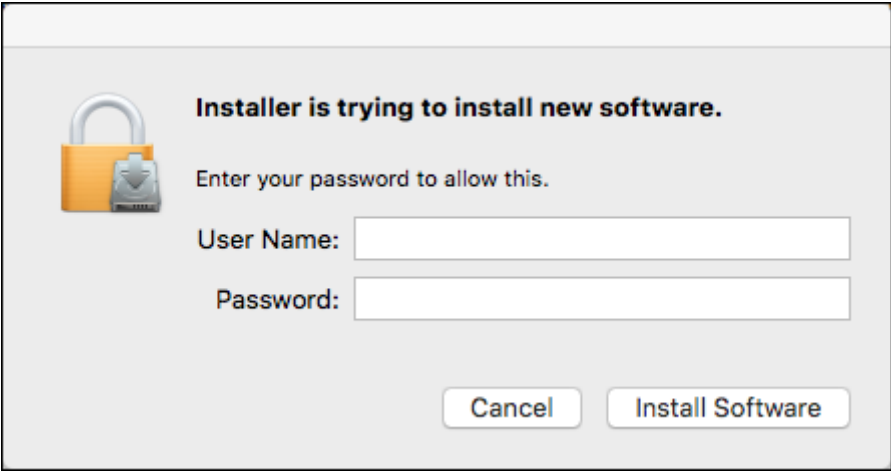
3. Click **Continue**. The **Select a Destination** page is displayed.



4. To install Desktop Host in this destination, click **Continue**. The **Standard Install** page is displayed.



5. Click **Install**. A dialog box prompting for your user name and password is displayed.



Installer is trying to install new software.

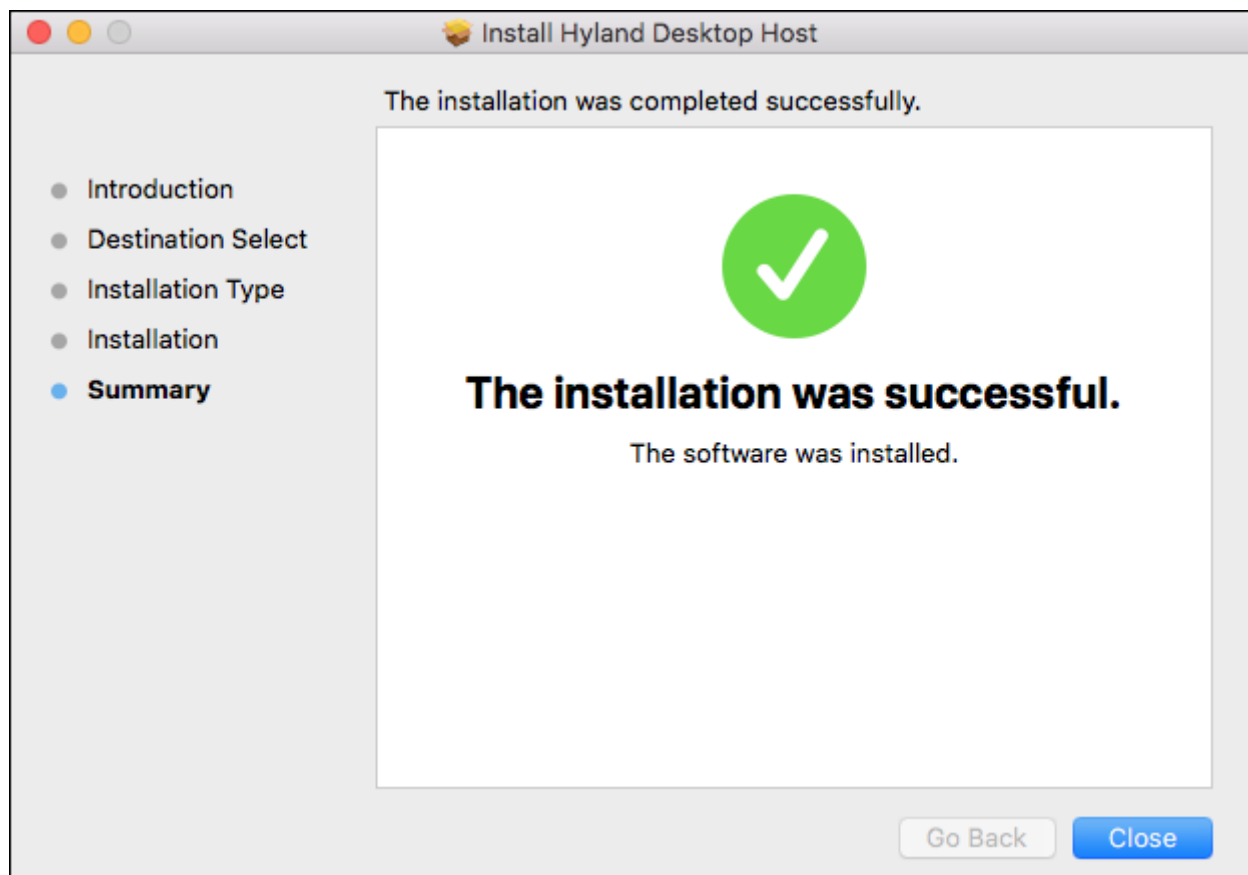
Enter your password to allow this.

User Name:

Password:

To continue installing, enter your credentials and click **Install Software**. A screen confirming successful installation is displayed.

Click **Cancel** to return to the previous page.



Removing an Installation for macOS

After installation, you can remove Desktop Host by performing the following steps:

1. Navigate to the **Library/Hyland** folder.
2. Double-click the **uninstall.command** file.

Note: If the **uninstall.command** file is unavailable, delete the **Hyland** folder by right-clicking on it and selecting **Move to Bin** or **Move to Trash**, or by dragging the folder to the Trash in the Dock. Then, restart the computer.

Whitelisting a Domain

Desktop Host can communicate only with domains that are included in a preconfigured whitelist. You can edit the **config.json** file included in the Desktop Host installation. This file is delivered with the installer for Desktop Host. When you run the installer, the file is copied to the **..\bin** directory of the installed application. You can edit the file before or after installation. If you edit the file after installation, you must restart Desktop Host to honor the new list of domains.

To add or modify domains to a whitelist:

1. Open the **config.json** file in a plain-text editor. In a typical installation, this file is in one of the following locations:
 - Before installation, the file is in the same directory as the installer.
 - After Windows installation, the file is in **C:\Program Files\Hyland\DesktopHost\bin**.
 - After macOS installation, the file is in **/Library/Hyland/DesktopHost/bin**.
2. In the **WhitelistedAddress** section, enter the domains that you want to whitelist. Each domain must be in double quotation marks, and multiple domains must be separated with commas. For example:

```
{
  "WhitelistedAddress": [
    "https://www.example.com",
    "https://www.example2.com"
  ]
}
```

Only include the domains for addresses that you want to whitelist; do not include full URL addresses. For example, to communicate with **https://www.example.com/public/**, include only **https://example.com** on the whitelist.

Note: By default, the whitelist contains the domain **127.0.0.1:8080**. You may remove or modify this domain if you do not want to allow communication at that address.

3. Save the **config.json** file.

4. Do one of the following:

- If you have not yet installed Desktop Host, place the **config.json** file in either the same folder as the Desktop Host installer (for Windows) or in the **Home** folder (for macOS).
- If you have already installed Desktop Host, restart the computer.

Configuring Desktop Host for Identity Providers

This section provides information on how to configure Desktop Host to work with an IdP (Identity Provider) service, such as the Hyland Identity Provider (Hyland IdP) or the Hyland Experience Platform Identity Provider (HxP IdP).

Note: You need to make the following configuration changes to Desktop Host only if it utilizes services that need to be authenticated using an IdP.

Desktop Host requests an access token from both the Hyland IdP and HxP IdP servers. This token is used by services using Desktop Host to authenticate users and allow access to protected resources or actions.

To configure Desktop Host to use an IdP service:

1. Open the **config.json** file in a plain-text editor. In a typical installation, this file is in one of the following locations:
 - Before installation, the file is in the same directory as the installer.
 - After Windows installation, the file is in **C:\Program Files\Hyland\DesktopHost\bin**.
 - After macOS installation, the file is in **/Library/Hyland/DesktopHost/bin**.
2. Locate the end of the **WhitelistedAddress** section and insert the following text after it to create a new **IdP** section:

```
"IdP": [  
  {  
    "ServiceName": "IdP Service Name",  
    "Issuer": "https://my.domain/identityprovider",  
    "ClientID": "Client ID",  
    "Scope": "openid offline_access"  
  }  
]
```

Note: Each key and value must be in double quotation marks, and pairs of key and value elements must be separated with commas.

3. For the key **"ServiceName"**, edit the value to specify the name of the IdP service. For example, **IdP Service Name**.

4. For the key "**Issuer**", edit the value to specify the URL of the IdP server issuer endpoint. For example, if the domain is **my.domain**, the IdP application name is **identityprovider**, and the environment is configured for secure connections, then the value is: **https://my.domain/identityprovider**.
5. For the key "**ClientID**", edit the value to specify the unique identifier of the IdP service that works with Desktop Host.
6. For the key "**Scope**", edit the value to specify a list of access privileges requested by the client. Each scope name must be separated with a space. For example, **openid offline_access**.
7. Save the **config.json** file.
8. Do one of the following:
 - If you have not yet installed Desktop Host, place the **config.json** file in either the same folder as the Desktop Host installer (for Windows) or in the **Home** folder (for macOS).
 - If you have already installed Desktop Host, restart the computer.

Creating Log Files for Troubleshooting

This section provides information on how to configure Desktop Host to send diagnostics logging messages to log files that can be used by Technical Support to diagnose and troubleshoot issues.

To configure Desktop Host to create log files:

1. Open the **config.json** file in a plain-text editor with elevated privileges. In a typical installation, this file is in one of the following locations:
 - On Windows, the file is in **C:\Program Files\Hyland\DesktopHost\bin**.
 - On macOS, this file is in **/Library/Hyland/DesktopHost/bin**.
2. In the file, locate the **DesktopHost_Log** diagnostics route, within the **Hyland.Logging** element. By default, the route includes the following key and value elements, which you can edit as needed:

```
"DesktopHost_Log":{
  "File": "../logs/Log.json",
  "minimum-level": "Information",
  "FileRollInterval": "Day",
  "FileByteLimit": "10000000",
  "FileCountLimit": "30",
  "FileRollOnSize": "true",
  "OutputFormat": "Json"
}
```

- For the key **"File"**, replace **"../logs/Log.json"** with the file path for the log file, including the name of the file you want the log to be saved as. This file must be a .json file.
For example, **"../logs/Log.json"** would write the logs to a file called **Log<date-stamp>.json** in the logs directory within the directory where Desktop Host is installed.

Note: Ensure that the Windows user account running Desktop Host has write permission for the path specified in the **"File"** key.

For the key **"minimum-level"**, edit the value to the lowest level of severity you want to be reported in the log. The following log levels are available, listed from most severe to least severe:

Note: Log level names are case sensitive.

Log Level	Description
Critical	Logs that describe an unrecoverable application, system crash, or catastrophic failure that requires immediate attention.
Error	Logs that highlight when the current flow of execution is stopped due to a failure. These logs indicate a failure in the current activity, but not an application-wide failure.
Warning	Logs that highlight an abnormal or unexpected event in the application flow but do not otherwise cause the application to stop.
Information	Logs that track the general flow of the application.
Debug	Logs that are used for interactive investigation during development.
Trace	Logs that contain the most detailed messages and may include sensitive data. These logs should never be enabled in a production environment.
None	A logging category that does not write any logging messages.

For example, the route could be edited to include the following attribute:

```
"minimum-level": "Information",
```

This example specifies that the logging route only receives logging messages with a severity level of Information or above.

Note: The default severity level of a route is a minimum of Information and a maximum of Critical. The route uses these severity levels if it does not include a **minimum-level** line specified in the **config.json** file.

- For the key **"FileRollInterval"**, edit the value to specify the interval after which you want a new log created. The following intervals are available for use:

Interval	Description
Minute	A new log file will be created every minute.
Hour	A new log file will be created every hour.
Day	A new log file will be created every day.
Month	A new log file will be created every month.
Year	A new log file will be created every year.
Infinite	A new log file will never be created.

- For the key **"FileByteLimit"**, you can edit the value to specify the maximum size in bytes for a log file before a new file is created. This attribute is only active if the value for the key **"FileRollOnSize"** is set to **"true"**.
- For the key **"FileCountLimit"**, you can edit the value to specify the number of log files that are created before the oldest file is deleted. If you do not want to delete older files, you can set the value to **"null"**.
- For the key **"FileRollOnSize"**, you can edit the value to **"true"** if you want a new log file to be created when the current log file reaches the maximum size in bytes. If you do not want create new files based on file size, you can set the value to **"false"**.

Note: If **"FileRollOnSize"** is set to **"true"**, the attribute **"FileByteLimit"** is active.

- For the key **"OutputFormat"**, you can specify the structure of each message that would be written in the log file. The following formats are available for use:

Format	Description
Minimal	Message that contains only the time, log level, exception, and the message field.
Text	Message that contains all possible fields as a list of key-value pairs.
Json	Message that contains fields in a compact JSON format on a single line. This format is ideal for further processing into a SIEM (Security Information and Event Management) or for reading with the Diagnostics Console.

- Save the file and close the text editor.
- Restart Desktop Host.

Troubleshooting Desktop Host

This section describes common issues you may encounter with Desktop Host and how to resolve them.

See the following sections:

- [Whitelisted URL Does Not Open](#) on page 91
- [Firefox Restricts Desktop Host](#) on page 91
- [Firefox Does Not Connect in Windows 8.1 or Windows Server 2012 R2](#) on page 92
- [Certificate Issues on macOS](#) on page 93

Whitelisted URL Does Not Open

Issue: While trying to open a whitelisted URL using Internet Explorer or Microsoft Edge, the URL does not open.

Solution: The whitelisted URL may be blocked by network isolation, an application security feature in Windows that restricts certain types of network communication. You can disable this restriction by enabling loopback for network access, allowing you to open the URL in the browser.

Caution: Enabling loopback is intended only for development or debugging purposes. Consult Microsoft's documentation on enabling loopback and troubleshooting network isolation before performing any commands that disable security features in your environment.

To enable loopback, perform the following command using PowerShell and with elevated privileges or Administrator rights:

```
CheckNetIsolation LoopbackExempt -a -n="Microsoft.Microsoft-Edge_8wekyb3d8bbwe"
```

Firefox Restricts Desktop Host

Issue: While using Firefox, Desktop Host does not function as expected.

Solution: Desktop Host needs a valid CA (Certificate Authority) certificate to enable communication with a web application. Although a self-signed certificate is used as a CA certificate, Firefox does not recognize this CA certificate if the browser is not configured adequately. You can configure Firefox to search CAs that are trusted to issue certificates for TLS (Transport Layer Security) web server authentication by changing the **security.enterprise_roots.enabled** preference.

To configure Firefox, perform the following steps after opening a new tab in Firefox:

1. In the address bar, enter **about:config** and click **I accept the risk**.
2. In the **Search** box, enter **enterprise** and double-click the **security.enterprise_roots.enabled** preference to change its value to **True**.

Note: If you have uninstalled Desktop Host and reinstalled it, you need to change the **security.enterprise_roots.enabled** preference to **False** and then change it again to **True**.

3. Restart Firefox.

Firefox Does Not Connect in Windows 8.1 or Windows Server 2012 R2

Issue: While using Firefox with older versions of Windows, Desktop Host fails to connect as expected.

Solution: Desktop Host needs adequate encryption rules such as a cipher suite to secure the communication with a web application. Firefox uses the HTTP/2 protocol that does not work with the default cipher suites available on Windows 8.1 and Windows Server 2012 R2. You can configure the **config.json** file to enable only the HTTP/1 protocol for Desktop Host:

1. Open the **config.json** file in a plain-text editor. In a typical installation, this file is in one of the following locations:
 - Before installation, the file is in the same directory as the installer.
 - After installation, the file is in **C:\Program Files\Hyland\DesktopHost\bin**.
2. Insert the following text:

```
"Kestrel": {  
    "EndpointDefaults": {  
        "Protocols": "Http1"  
    }  
}
```
3. Save the **config.json** file and close the text editor.
4. Do one of the following:
 - If you have not yet installed Desktop Host, place the **config.json** file in the same folder as the Desktop Host installer.
 - If you have already installed Desktop Host, restart it.

Alternately, you can also configure Firefox to disable HTTP/2 by changing the **network.http.spdy.enabled.http2** preference.

To configure Firefox, perform the following steps after opening a new tab in Firefox:

1. In the address bar, enter **about:config** and click **I accept the risk**.
2. In the **Search** box, enter **http2** and double-click the **network.http.spdy.enabled.http2** preference to change its value to **False**.

Note: If you have uninstalled Desktop Host and reinstalled it, you need to change the **network.http.spdy.enabled.http2** preference to **True** and then change it again to **False**.

3. Restart Firefox.

Certificate Issues on macOS

Issue: Self-signed certificates may not be added and removed automatically during a reinstallation on macOS.

Solution: By using HylandDesktopHostCertificateProducer on macOS, self-signed certificates can be added as trusted certificates to a keychain.

To install a self-signed certificate, perform the following commands after opening Terminal:

```
sudo /Library/Hyland/DesktopHost/bin/HylandDesktopHostCertificateProducer install  
  
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/  
System.keychain /Library/Hyland/DesktopHost/bin/hyland.desktophost.local.cer
```

To uninstall a self-signed certificate, perform the following commands after opening Terminal:

```
sudo security delete-certificate -c "Hyland-Desktop-Host" /Library/Keychains/  
System.keychain
```

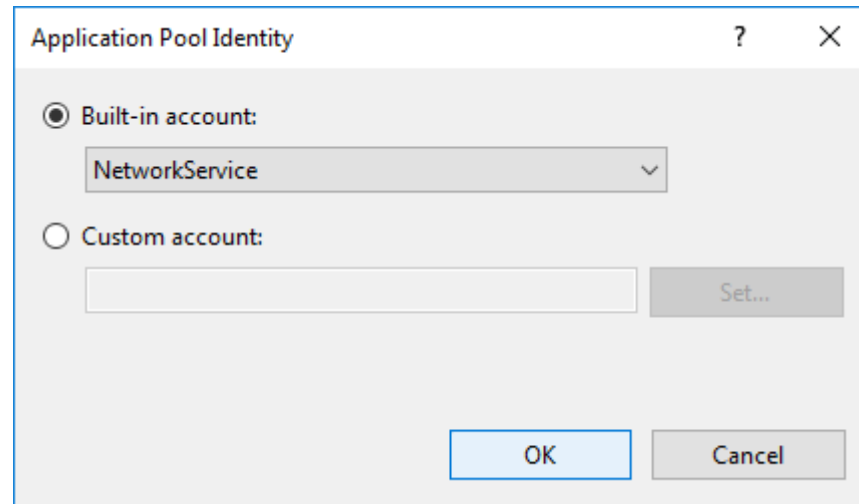
WEB SERVER MANUAL INSTALLATION CHECKLIST

The Web Server installation checklist guides you through the steps required to manually install the OnBase Web Server on supported versions of Windows Server.

Complete each item in the following checklist to ensure your OnBase Web Server is successfully installed.

Web Server Installation Steps Checklist

In the following steps, the term "application pool identity account" refers to the user account configured to run the application pool worker process. In IIS, this account is specified in the **Application Pool Identity** dialog box. You can select a built-in service account or set the credentials for a custom account.





The term "impersonated identity account" refers to the custom service account that ASP.NET uses to access domain resources in high-security deployments. This account's credentials are encrypted in the registry, and the registry location is specified in the Web Server's web.config file.

Complete each item in this checklist to ensure the OnBase Web Server is successfully installed. This checklist is applicable for supported versions of Windows Server and the versions of IIS included with Windows Server.








Web Server Installation Steps				Notes
1	<input type="checkbox"/>	Follow Microsoft best practices for securing Windows Servers, IIS, and ASP.NET Web applications throughout the install.		<p>Additional information is available on securing different versions of Windows Server:</p> <p>Windows Server 2012:</p> <ul style="list-style-type: none"> See the Microsoft TechNet guide to securing Windows Server 2012 R2: http://technet.microsoft.com/en-us/library/hh831360.aspx See the Microsoft Security Compliance Manager: http://www.microsoft.com/en-us/download/details.aspx?id=16776 <p>Windows Server 2016 and Windows 2019:</p> <ul style="list-style-type: none"> See the Microsoft Security and Assurance guide: https://docs.microsoft.com/en-us/windows-server/security/security-and-assurance
2	<input type="checkbox"/>	Verify that the Web Server machine meets OnBase Web Server Requirements.		See Requirements on page 22 .
			<input type="checkbox"/> CPU	2.4GHz dual-core / dual processor (Intel® XEON™ processor with multiple cores or processors recommended)
			<input type="checkbox"/> System Memory	4 GB (8 GB recommended)
			<input type="checkbox"/> Internet Browser	Internet Explorer 11, with all related security patches, must be installed on the server.

Web Server Installation Steps				Notes
			<input type="checkbox"/> Server Deployment Notes	<p>OnBase Web Servers must be dedicated purpose servers; NOT USED as a domain controller, DNS server, non-OnBase Web server, email server, print/database/file server, index server, proxy server, network backup server, jukebox manager, network performance monitor, Client processing workstations or Workflow/API Client brokers.</p> <p>Network and disk I/O hardware should be optimized for performance and redundancy. Two network cards can reduce server bottlenecks by using a segmented network for external and internal requests, where external requests are sent to the Web clients and internal requests are sent to the file and database servers.</p> <p>It is strongly recommended that you complete these installation procedures on a clean operating system.</p>

Web Server Installation Steps				Notes
			 Virtual Machine Deployment Notes	<p>Hyland Software develops, tests, and supports the OnBase suite of products on specific Operating Systems, not specific hardware configurations. When OnBase is operated in a virtual environment (such as Citrix, VMware, Hyper-V, or Windows Remote Desktop) there may be limitations or subtle differences imposed by the environment. The customer and the virtual environment vendor are responsible for any interactions or issues that arise at the Hardware or Operating System layer as a result of their use of a virtual environment.</p> <p>When it appears that a performance-related issue in OnBase is either caused by (or is unique to) the virtual environment, organizations may be asked to validate that the issue occurs in a non-virtual environment. Hyland Software will make this request if there is reason to believe that the virtual environment is a contributing factor to the issue.</p> <p>Each OnBase site is unique. Hyland Software depends on the customers who deploy OnBase in virtual environments to do so only after careful design and adequate planning (that takes into account the workloads of your organization), and in accordance with recommendations provided by the virtual environment's vendor. As with any implementation, Hyland Software strongly recommends that any customer deploying the OnBase solution in a virtual environment thoroughly test the solution before putting it into production.</p> <p>For information about using OnBase in a Citrix and Microsoft Windows Remote Desktop environment, please see the Citrix and Microsoft Windows Remote Desktop Environment Deployment Guide, available from your solution provider.</p>
			 Supported Database Versions	<p>For specific database version support, see the database requirements section in the OnBase Installation Requirements manual.</p>

Web Server Installation Steps				Notes
			<input type="checkbox"/> OnBase Database Version	Version 3.5-409 or greater
			<input type="checkbox"/> Client Notes	<p>For operating system and web browser support, see the operating system requirements and web browser requirements sections in the OnBase Installation Requirements manual.</p> <p>Browser toolbars and pop-up blockers are not supported.</p> <p>It is strongly recommended that you use a separate client workstation during installation for all Web Client testing of the installed Web Server.</p> <p>Mismatched versions or multiple registered copies of these .OCX/.DLL files are the most common source of failed Web Server installations, requiring further troubleshooting.</p>
3	<input type="checkbox"/>	Install or verify installation of Windows Server.		
4	<input type="checkbox"/>	Install or verify installation of IIS.		

Web Server Installation Steps				Notes
			<input type="checkbox"/> Install only the necessary IIS components.	<p>Use the Add Roles and Features Wizard in Windows Server Manager to install IIS and ASP.NET.</p> <ol style="list-style-type: none"> 1. When prompted to assign a role, choose Web Server (IIS). 2. When prompted to select role services, select the following: <ul style="list-style-type: none"> • Static Content • Default Document • ASP.NET • .NET Extensibility • ISAPI Extensions • ISAPI Filters • Request Filtering • IIS Management Console • Windows Authentication (if you plan to use Active Directory authentication) <hr/> <p>Caution: Do not add the Dynamic Content Compression feature. This feature interferes with the XML sent between the Web Server and other servers or applications, and it should not be installed or enabled on the Web Server.</p> <hr/> <p>Other roles may be needed depending on network security and other functionality needed for your solution. Add these required roles when prompted.</p>
			<input type="checkbox"/> Restart the IIS service.	<p>Recommended: Use the Microsoft iisreset.exe utility located in C:\WINDOWS\system32.</p>
5	<input type="checkbox"/>	Apply any required Windows Server service packs and updates.		

Web Server Installation Steps				Notes
6		Install or verify installation of Microsoft .NET Framework.		
			 Verify that .NET Framework has been successfully installed.	OnBase requires Microsoft .NET Framework 4.7.2 or later. The .NET Framework can be obtained from the Microsoft Download Center at http://www.microsoft.com/downloads . .NET Framework is installed when selecting the Web Server (IIS) role.
			 Verify all updates to .NET Framework have been successfully installed.	
7		Uninstall OnBase Core Services.	 Search the entire server system path for older versions of the Web Server files that may have been installed in a previous installation.	Unregister any registered Core Services files from previous versions using REGSVR32 /U . Then, delete the unregistered files. It is critical that multiple copies of the Core Services DLL files not be registered on the server. The Web Server will not function correctly with multiple or mismatched versions of the Core Services DLLs.
8		Install OnBase Core Services.		OnBase Core Services is required for the execution of Workflow VBScripts. Other modules, such as Disconnected Scanning and Front Office Scanning, also require OnBase Core Services. Check the reference guides for modules in your solution to determine additional installation requirements.
			 Copy the file contents of the ..\BIN directory from the build distribution package to a system path location.	If necessary, edit the computer's PATH environment variable to include the local directory containing the copied OnBase Core Services DLL files.

Web Server Installation Steps				Notes
			<input type="checkbox"/> Install the OnBase Diagnostics Service.	<p>The Diagnostics Service monitors low-level Web Server error and informational messages. It is available in the ..\apps\NTServices\Hyland.Diagnostics directory in the build distribution package. See the Diagnostics Service & Diagnostics Console module reference guide for information about installing and configuring the service and using the Diagnostics Console.</p> <hr/> <p>Note: If you are upgrading your Core Services installation, uninstall previous versions of the Diagnostics Service and Diagnostics Console before installing the latest version.</p> <hr/>
9	<input type="checkbox"/>	Create a Web site. For high-security deployments, follow Microsoft best practices.	<input type="checkbox"/> Create a new Web site in the IIS Manager.	A Web site root directory must be designated.





Web Server Installation Steps				Notes
			<input type="checkbox"/> Configure IIS logging as needed.	<p>Use the IIS Logging feature to configure logging at either the site or server level. The following W3C Logging Fields are recommended:</p> <ul style="list-style-type: none"> • Date • Time • Client IP Address • User Name • Method • URI Stem • URI Query • Protocol Status • Win32 Status • Bytes Sent • Time Taken • User Agent • Referrer <p>To access these logging fields, open the Logging feature for the server or site, ensure W3C is the selected format, and click Select Fields.</p>
10	<input type="checkbox"/>	Install the current OnBase Web Server build.	<input type="checkbox"/> Create a Web content sub-directory within the Web site root directory:	<p>It is recommended that you name the new subdirectory whatever you plan to name your Web application/virtual directory.</p> <p>..\YourWebSiteRoot\YourWebApp</p>

Web Server Installation Steps				Notes
			<input type="checkbox"/> Copy the standard OnBase Web Server and Web Client files, including subdirectories, from the ..\WEB\appnet build directory into the virtual directory file location as configured for the virtual directory in IIS Manager.	The copied files include test files in the appnet\Diagnostics directory: test.gif – for testing access to static non-ASP.NET content aspnetcheck.aspx – for verifying non-OnBase ASP.NET functionality
11	<input type="checkbox"/>	Create an application pool.	<input type="checkbox"/> In IIS Manager, create a unique application pool for each Web application/virtual directory you plan on creating.	For high security deployments, the default, well-known Default application pool should NOT be used.
12	<input type="checkbox"/>	Configure the Web site properties.	<input type="checkbox"/> Convert the directory you created in step 10 to an application.	In IIS Manager, right-click the directory you created in step 10 and select Convert to Application . When prompted, select the application pool you created in step 11. If you did not install the OnBase Web Server files in the Web site content directory, right-click the Web site in IIS Manager and select Add Application . Follow the prompts to create the Web Server application.
			<input type="checkbox"/> Set login.aspx as the default document.	Login.aspx is already specified in the defaultDocument element in the Web Server's web.config file.
			<input type="checkbox"/> In the Authentication feature for the Web Server application, enable Anonymous Authentication and configure the specific local machine user account.	The anonymous account is normally named IUSR by default and should not need to be changed.

Web Server Installation Steps				Notes
			<input type="checkbox"/> Assign your newly created application pool to the virtual directory.	A unique application pool should be assigned to each separate Web application/virtual directory you plan on operating.
13	<input type="checkbox"/>	Configure the application pool.		For recommended settings, see Application Pool Configuration on page 237 . To access all configuration settings, select the application pool in IIS Manager, and click Advanced Settings from the Actions pane.
			<input type="checkbox"/> Set .NET CLR Version to v4.0 .	This setting is under (General) in the Advanced Settings dialog box.
			<input type="checkbox"/> Set Enable 32-Bit Applications to False .	The OnBase Web Server is a 64-bit application, so 32-bit execution must be disabled.
			<input type="checkbox"/> Ensure Integrated is selected for the Managed Pipeline Mode .	
			<input type="checkbox"/> Set the Queue Length to 65535 .	Setting this value is the same as clearing the Limit the kernel request queue (number of requests) option in IIS.
			<input type="checkbox"/> Set the Limit Interval to 0 .	This setting is under CPU in the Advanced Settings dialog box.





Web Server Installation Steps				Notes
			<input type="checkbox"/> Set the Identity to NetworkService .	<p>This setting is under Process Model in the Advanced Settings dialog box.</p> <p>You can also select another built-in service account, or you can enter a user name and password for a custom service account to run the application pool worker process and potentially access domain resources.</p> <ul style="list-style-type: none"> For steps on creating a custom service account, see the Microsoft article: "How To: Create a Service Account for an ASP.NET 2.0 Application" (this article is applicable to .NET 2.0 and later versions): http://msdn2.microsoft.com/en-us/library/ms998297.aspx For file and folder permissions required with .NET 4.x, see the ACL Technology Overview: http://msdn.microsoft.com/en-us/library/ms229742.aspx <p>See also the article on ASP.NET Required Access Control Lists (ACLs): http://msdn.microsoft.com/en-us/library/kwzs111e.aspx </p> <hr/> <p>Caution: Use of the LOCAL SYSTEM account is a significant security vulnerability that must be avoided in any production or customer data environment.</p> <hr/>
			<input type="checkbox"/> Set the Idle Time-out to 0 .	
			<input type="checkbox"/> Ensure the Maximum Worker Processes is set to 1 .	<p>The OnBase Web Server requires that this value be set to the default value of 1.</p>
			<input type="checkbox"/> Set Ping Enabled to False .	




Web Server Installation Steps				Notes
			<input type="checkbox"/> Under Rapid-Fail Protection , set Enabled to False .	
			<input type="checkbox"/> Set Regular Time Interval to 0 .	This setting is under Recycling in the Advanced Settings dialog box.
14	<input type="checkbox"/>	Configure the Web.config application settings for the Web application pool.	<input type="checkbox"/> Specify the data source.	In the <appSettings> section of the Web Server's Web.config file located within the virtual directory content directory, set <dmsDataSource> to your data source.
			<input type="checkbox"/> Specify the server address.	<p>The server address must match the address accessed by end users. In the <appSettings> section of the Web Server's Web.config file located within the virtual directory content directory, set <dmsVirtualRoot> to the URL that users will access your Web application. (e.g., http://hostname/virtualdirectory)</p> <hr/> <p>Note: The server address used in the <dmsVirtualRoot> element can be a UNC server name, an IP address, or a fully qualified domain name. The host name cannot contain an underscore character (_). If the server's machine name contains an underscore character, use its IP address instead.</p> <hr/> <p>Examples: http://localhost/YourWebApp for local testing/demo Web apps http://127.0.0.1/YourWebApp for local testing/demo Web apps http://srv-99223344/YourWebApp for intranet Web apps http://192.101.101.44/YourWebApp for IP addressed Web apps http://www.yoursite.com/YourWebApp for DNS addressed Web apps http://demo1.yoursite.com/YourWebApp for DNS addressed Web apps</p>

Web Server Installation Steps				Notes
15		Assign NTFS permissions for the IUSR Anonymous Account to access the Web content directory.	 Web content directory and sub-directories: C:\inetpub\wwwroot\YourWebApp (or the path that the virtual directory points to)	Anonymous access account: Read and Execute Read
16		For high-security deployments, create a custom, least-privileged service account for identity impersonation. The built-in ASP.NET process accounts are well-known least-privileged accounts and are suitable for most environments.		<ul style="list-style-type: none"> For full details on custom service account configuration, see the Microsoft article: "How To: Create a Service Account for an ASP.NET 2.0 Application" (this article is applicable to .NET 2.0 and later versions): http://msdn2.microsoft.com/en-us/library/ms998297.aspx For file and folder permissions required with .NET 4.x, see the ACL Technology Overview: http://msdn.microsoft.com/en-us/library/ms229742.aspx See also the article on ASP.NET Required Access Control Lists (ACLs): http://msdn.microsoft.com/en-us/library/kwzs111e.aspx <hr/> <p>Caution: Do not use IIS Manager to configure impersonation. IIS Manager enters the account's credentials into Web.config in plain text. Use the following steps to configure the account, enable impersonation in web.config, and encrypt the account's credentials in the registry.</p> <hr/>
			 Create a new local user account.	

Web Server Installation Steps				Notes
			<input type="checkbox"/> Assign ASP.NET permissions to the new account.	At a Command Prompt, change the directory to: C:\Windows\Microsoft.NET\Framework Enter the following command: aspnet_regiis -ga MachineName\AccountName This command grants access to IIS resources and permissions to write to the ASP.NET Temporary files folder.
			<input type="checkbox"/> Assign permissions to the Web content directory and subdirectories: C:\inetpub\wwwroot\YourWebApp (or the path that the virtual directory points to)	New account permissions: Modify
			<input type="checkbox"/> Assign permissions to the OnBase Core Services installation directory (from step 8).	Application pool identity account and impersonated identity account: Read and Execute List Folder Contents
17	<input type="checkbox"/>	Assign local security policy user rights for the account you created in step 16, using secpol.msc.		If you created a new account in step 16, you must change the local security policy user rights for the new account. If you are using a built-in process account (e.g., ASPNET), skip this step.
			<input type="checkbox"/> Access this computer from the network.	
			<input type="checkbox"/> Log on as a batch job.	

Web Server Installation Steps				Notes
			<input type="checkbox"/> Log on as a service.	
			<input type="checkbox"/> Deny logon locally.	
			<input type="checkbox"/> Deny logon through Remote Desktop Services.	
18	<input type="checkbox"/>	Create registry keys containing encrypted username and password values to use in production Web Server installations.		<p>A copy of the aspnet_setreg tool is located in the ..\utilities\misc subdirectory in the build distribution package.</p> <p>Full details on creating Encrypted account registry keys are available in the Microsoft article: "How To Use the ASP.NET Utility to Encrypt Credentials and Session State Connection Strings" available at: http://support.microsoft.com/kb/329290</p>
			<input type="checkbox"/> Create registry keys containing encrypted username and password values for the impersonated identity account.	<p>Use the Microsoft ASPNET_SETREG.EXE tool:</p> <p>aspnet_setreg.exe -k:SOFTWARE\Hyland\YourApp\identity -u:"DOMAIN\name" -p:"password"</p>
			<input type="checkbox"/> Assign NTFS permissions for the registry keys.	<p>ASP.NET application pool identity account: Read</p> <hr/> <p>Note: If the application pool is configured to use the built-in ApplicationPoolIdentity account, then the IIS_IUSRS group must be granted Read access to the registry key.</p> <hr/>

Web Server Installation Steps				Notes
19		Encrypt the ASP.NET impersonated identity account.	 Assign a registry reference pointing to the encrypted user name and password created in step 18, for the user name and password values.	Within the application pool's virtual directory's web.config file <identity> element: <identity impersonate="true" userName="registry:HKLM\SOFTWARE\Wow6432Node\Hyland\YourApp\identity\ASPNET_SETREG,userName" password="registry:HKLM\SOFTWARE\Wow6432Node\Hyland\YourApp\identity\ASPNET_SETREG,password" />
20		Install the OnBase Log.	The OnBase Log is installed by running the Event Log Creator in the Web Application Management Console.	See the Web Application Management Console module reference guide for instructions on installing the OnBase Log.
21		Configure the OnBase Log in Event Viewer.	The default log file sizes in Event Viewer need to be increased to avoid error messages.	In the Event Viewer, right click on the OnBase Log and select properties. The maximum log size should be set to 16384 KB. Overwrite events as needed should be selected.

Web Server Installation Steps				Notes
22		Configure your antivirus, backup, or indexing service software to exclude OnBase application files.		<p>Modifying the contents of the Web Server or Application Server's virtual directory will cause the application to restart. When this occurs, connected users will lose their sessions and their applications will become unresponsive. This behavior occurs because the OnBase Web Server and Application Server are ASP.NET Web Applications. ASP.NET detects file changes, including changes to file system attributes and time stamps, and restarts the application if a change is detected.</p> <p>Unintended application restarts can occur when virus scanning software, backup software, or indexing services access the contents of an application's virtual directory. These processes don't modify the contents of an application's files, but they can modify the files' attributes, which is enough for ASP.NET to restart the application. To properly configure virus scanning, backup software, or indexing service software, follow the guidelines below.</p>
			 Exclude both the OnBase Web Server's and Application Server's virtual directories from antivirus, backup, or indexing service scanning.	If these files are scanned by antivirus, backup, or indexing software, IIS will restart the application pool for the OnBase application. When an application pool restarts, all existing OnBase sessions are reset, causing errors for connected users.
			 Exclude the ASP.NET Temporary Files directory from antivirus, backup, or indexing service scanning.	The ASP.NET Temporary Files directory is C:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files.

Web Server Installation Steps				Notes
			<input type="checkbox"/> Real-time scanning of script execution, which is available in some antivirus software, should only be engaged according to the software manufacturer's instructions. Some manufacturers do not intend this functionality to be used on servers.	Consult your antivirus, backup, or indexing software documentation for other recommended settings for Web servers.
			<input type="checkbox"/> Ensure that any antivirus, backup, or indexing service changes will not be overwritten by the automatic policy settings configured for your network.	
23	<input type="checkbox"/>	The OnBase Web Server is installed. Perform testing as necessary.		To troubleshoot account permissions, see the appendix, Troubleshooting Permissions on page 115 .
			<input type="checkbox"/> Configure the Web Server to refer to the Application Server for services. See Configuring Service Client Settings on page 51 .	

Notes

1.	
2	
3	
4	
5	
6	
7.	
8	
9	
10	

Troubleshooting Permissions

In a production environment, the ASP.NET process and impersonated identity accounts should be assigned the minimum privileges and permissions required. To troubleshoot permissions errors, test your configuration using existing accounts that have additional privileges and permissions.

Local System Account Testing

Use the Local System account to run the worker process to establish the correct registry entries and event viewer logs.

Caution: Use of the Local System account is a significant security vulnerability that must be avoided in any production or customer data environment.

On the Application Pool's **Identity** tab, select the Local System account.

After testing, change this account to the permanent username and password that will be used to run the application pool worker process and potentially access domain resources.

Domain User Account Testing

Configure the ASP.NET impersonated identity account using the following steps for secondary testing only:

1. Inside the **<system.web>** element tags within the worker process web.config file, create an **<identity>** element.

```
<identity impersonate="true"
  userName="yourUserName"
  password="yourPassword"
/>
```

2. Temporarily assign a known-good domain user account as the user name to use within the worker process web.config file **<identity>** element.
3. Temporarily assign the known-good domain user account password as the password to use within the worker process web.config file **<identity>** element.

Caution: This MUST later be reconfigured on any production Web Server installation (or test/development Web Server attached to a production database or production network domain). Use of clear text passwords in an XML web.config file is a significant security vulnerability that must be avoided in any production or customer data environment.

After Testing

After testing, reconfigure the ASP.NET identity account using the steps in the Web Server installation checklist.

If you are using impersonated identity, encrypt the ASP.NET impersonated identity account as described in the Web Server installation checklist.

W3wp.exe could not be started

If the worker process account does not have sufficient rights to system files, you may encounter the following error when accessing a Web page:

- **Server Application Unavailable**
The web application you are attempting to access on this web server is currently unavailable. Please hit the "Refresh" button in your web browser to retry your request.
Administrator Note: An error message detailing the cause of this specific request failure can be found in the system event log of the web server. Please review this log entry to discover what caused this error to occur.

The following error message is displayed in the Application event log:

- W3wp.exe could not be started. HRESULT for the failure: 80070005

For information on addressing this issue, see the Microsoft support article available at the following location: <http://support.microsoft.com/kb/833444>



Web Server

Administration Guide

General Usage

The Web Server allows users at remote client stations to search for, access, and change documents stored in a central database that is accessed by the Web Server.

If you have administrative privileges, you can use the Web Client to perform administrative tasks, such as viewing document and folder history and managing other OnBase users.

The following topics describe how to perform these tasks.

- [Viewing a Document's History on page 127](#)
- [Viewing a Folder's History on page 132](#)
- [User Administration on page 136](#)

The following topics describe how to log on to the Web Client and change your password:

- [Logging On on page 119](#)
- [Changing Your Password on page 124](#)

Logging On

To access documents through the Web Client, you must first log on to OnBase.

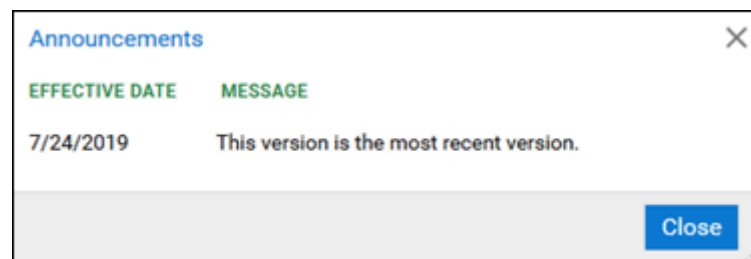
Note: If the **Selectable** option is enabled in the Web Application Management Console, the Web Server detects which browser is being used, and then configures the client type accordingly (to either ActiveX or HTML). Only Internet Explorer defaults to ActiveX, allowing you to choose HTML if necessary.

1. From the login screen, type your user name in the **User name** field.
2. Type your password in the **Password** field.
3. If the **Language** field is enabled, select the language you want from the drop-down list.
4. Click **Login**. The Web interface is displayed.

Note: If you have a 64-bit browser, the Web Client logs on in HTML mode.

Login Banner

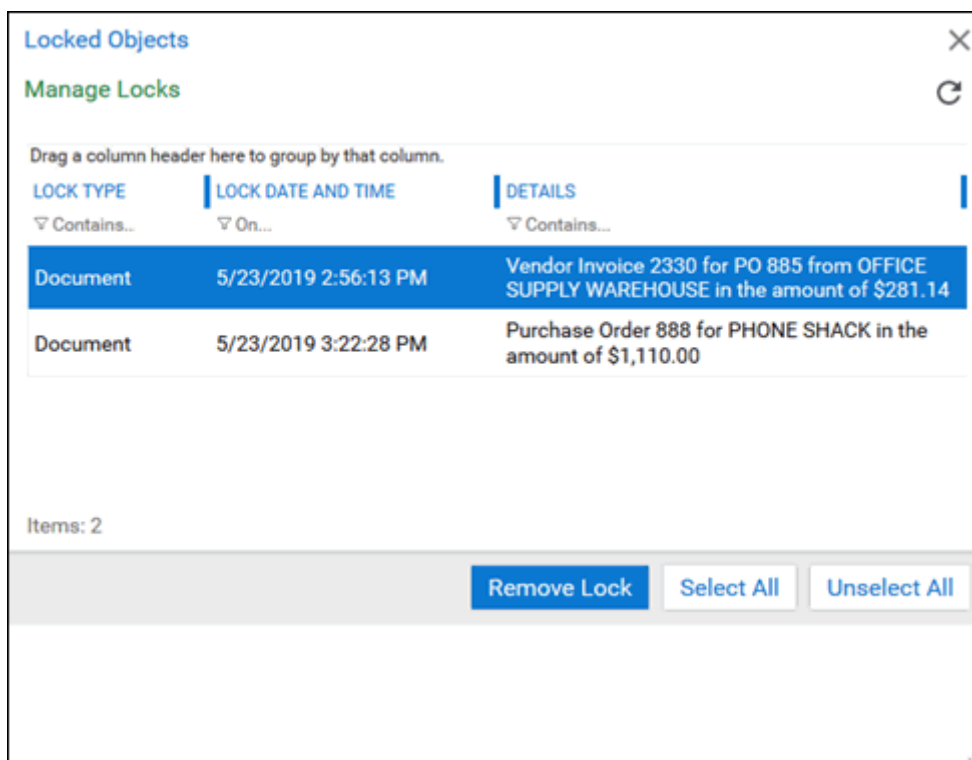
A login banner may be displayed after you log on. Login banners are system notifications containing important announcements. The system administrator configures the content of login banners and the number of days they are displayed.



Click **Close** to continue to the Web Client.

Locked Objects Notification

If there are any objects locked by your user account, the **Locked Objects** dialog box is displayed after you log on.



Locks can occur if you have documents open when OnBase closes unexpectedly. If you do not clear the locks, other users will only be able to open read-only copies of the locked document.

To clear locked objects:

- From the list of locked objects, select the documents you want to unlock.
 - To select multiple documents, hold **Shift** or **Ctrl** while clicking the documents in the list.
 - To select all documents in the list, click **Select All**.
 - To deselect all documents in the list, click **Unselect All**.
- Click **Remove Lock** to remove the locks from the selected documents.
- Click the X in the upper right to close the **Locked Objects** dialog box.

Database Mismatch Message

If there is a mismatch of the database, this message is displayed:

The server encountered an error when connecting to the database. If this problem persists, you should contact your administrator for resolution.

You will need to contact your system administrator who can fix the mismatch so you can log in to the Web Client.

ActiveX Control Message

If ActiveX controls fail to load, this message is displayed:

Failed to load Popup Blocker Assistant ActiveX control.

This message typically displays when you need to have new ActiveX controls installed on your machine. Click **OK** and then contact your system administrator to install the most recent controls.

Concurrent Client Licenses Message

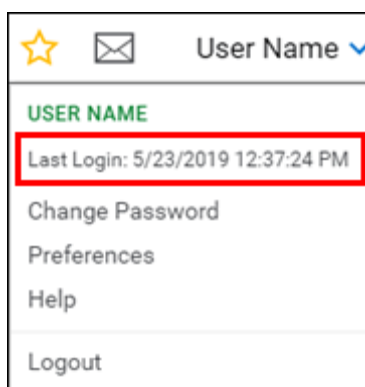
If there are not enough concurrent licenses for Web Client, this message is displayed:

**You have exceeded the concurrent licensing for product: Concurrent Client
A temporary license has been granted. Please report this licensing overage to your system administrator.**

Contact your system administrator so they can procure enough licenses for future use.

Last Login

Once in the Web Client, you can view the date and time you last logged in. Select the drop-down arrow next to your user name.



The information from your last login is shown below your user name. If this is your first time logging in, the word **Now** is displayed.

Session Interruption

Your Web Client session may be interrupted under certain circumstances. See the following sections for more information:

- [Session Timeout on page 122](#)
- [Authentication Required on page 122](#)

Session Timeout

Depending on your configuration, you may be prompted with the following message after a period of inactivity:

Your session appears to be inactive. You will be logged out in 30 seconds.

In order to stay logged on, you must either click **Stay Logged In** or press the **Enter** key. If the **Stay Logged In** button is not activated within the allotted time, you are logged off of the Web Client.

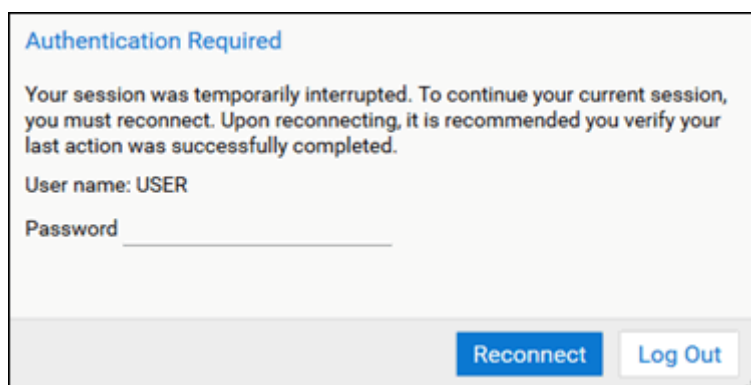
Caution: In Firefox, the message may not be displayed if the Web Client is minimized behind another application that is maximized. In this case, you may be silently logged off when the timeout threshold is reached. Ensure that there are no maximized applications in front of the Web Client.

Authentication Required

Your Web Client session may be interrupted and you may be required to re-authenticate your connection to OnBase. This can happen for several reasons, such as if you are required to reset your password, or if the network connection is interrupted.

Depending on your solution, you may be able to reconnect to OnBase and resume your session, or you may be required to log in again and begin a new session.

If you are allowed to resume your session, the **Authentication Required** dialog box is displayed:

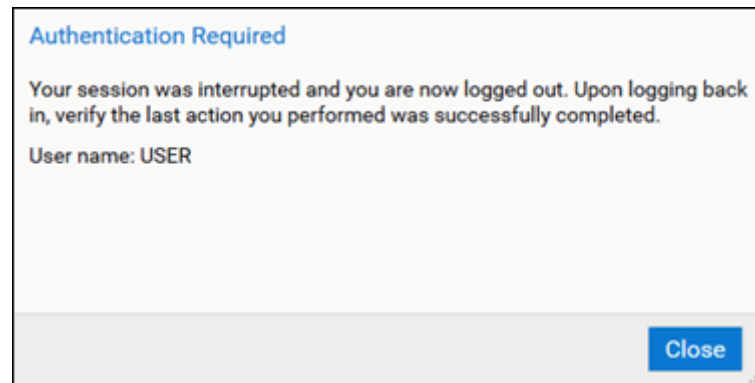
A screenshot of the 'Authentication Required' dialog box. The title bar is blue with the text 'Authentication Required' in white. The main area has a light gray background. It contains the text: 'Your session was temporarily interrupted. To continue your current session, you must reconnect. Upon reconnecting, it is recommended you verify your last action was successfully completed.' Below this, it says 'User name: USER' and 'Password' followed by a text input field. At the bottom right, there are two buttons: 'Reconnect' (blue with white text) and 'Log Out' (light gray with blue text).

Note: If your solution allows you to automatically log in to the Web Client, the **Password** field is not included.

Do one of the following:

- Enter your OnBase password (if required) and click **Reconnect** to resume your current session. You are returned to the Web Client context in which you were previously working. It is recommended that you verify that your last action before the interruption was successfully completed.
- Click **Log Out** to end your current session and return to the Web Client login page.

If you are required to begin a new session, the following **Authentication Required** dialog box is displayed:



Click **Close** to return to the Web Client login page, and re-enter your user name and password if required. It is recommended that you verify that your last action before the interruption was successfully completed.

Changing Your Password

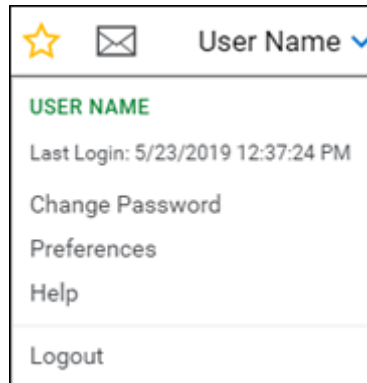
If you have appropriate privileges, you can change your OnBase password. When you change your password, the new password is saved throughout the entire OnBase system.

Note the following considerations when changing your password:

- Depending on your user account configuration and system setup, the **Change Password** option may not be available to you. See your system administrator for more information.
- The **Change Password** option is displayed in the user menu only if Standard Authentication is being used and if the property for the **Password** control bar setting in the Web Server web.config has been enabled.
- If password expiration is enabled in the OnBase system and your password has expired, the **Change Password** dialog box is displayed when attempting to log in. In this situation, you are required to change your password before entering the system.

To change your password:

1. Select **Change Password** from the user menu.



The **Change Password** dialog box is displayed.

A screenshot of the 'Change Password' dialog box. It has a title bar with 'Change Password' and a close button (X). The dialog contains the following fields: 'User name: MANAGER', 'OLD PASSWORD' (with a text input field), 'NEW PASSWORD' (with a text input field), and 'VERIFY NEW PASSWORD' (with a text input field). At the bottom right, there are two buttons: 'Save' (blue) and 'Cancel' (white).

2. In the **Old Password** field, type your current password.
3. In the **New Password** field, type the new password that you want to use in the future. Your new password can include any combination of printable characters, including those in the international character set.

Note: The minimum length and maximum length for a password are set by your system administrator.

4. In the **Verify New Password** field, type the new password again. It must be exactly the same as what you typed into the **New Password** field.
5. Click **Save**. A confirmation message is displayed.

6. Click **OK**.

Viewing a Document's History

A document's history is a log maintained by OnBase of all the actions performed on the selected document. If you have the appropriate administrative rights, you can view a history of the document that is currently open in the Document Viewer or displayed in the Document Search Results list. You cannot change any of the information in a document's history.

To view the history of an open document or a document in the Document Search Results list, right-click and select **History**. Additionally, in the HTML Web Client, you can also perform the **CTRL + H** keyboard shortcut to view a document's history.

Note: To view the document history for an open OLE or PDF document in the OnBase Web Client, select **Document | History**.

The **Document History** window lists the past actions performed on the document. By default, the entries are sorted in descending order, with recent actions listed first.

Resolution for - ()

DOCUMENT HISTORY			
DATE	USER	ACTION	MESSAGE
▽ Contains...	▽ Contains...	▽ Contains...	▽ Contains...
4/8/2017	MANAGER	Viewed Document	Viewed (619) 'Resolution for - ()'
4/6/2017	MANAGER	Viewed Document	Viewed (619) 'Resolution for - ()'
4/5/2017	MANAGER	Viewed Document	Viewed (619) 'Resolution for - ()'
4/5/2017	MANAGER	Viewed Document Keywords	Viewed keywords on document 619 (Resolution for - ())
4/5/2017	MANAGER	Viewed Document Keywords	Viewed keywords on document 619 (Resolution for - ())
4/5/2017	MANAGER	Viewed Document	Viewed (619) 'Resolution for - ()'
4/5/2017	MANAGER	Viewed Document Keywords	Viewed keywords on document 619 (Resolution for - ())
4/5/2017	MANAGER	Viewed Document	Viewed (619) 'Resolution for - ()'
4/5/2017	MANAGER	Viewed Document Keywords	Viewed keywords on document 619 (Resolution for - ())

Items: 13

Close

The **Document History** window displays actions in the following columns:

- **Date**
Lists the date when the action was performed. The date is formatted to correspond with the Windows **Short Date** format. This configuration can be found in **Start | Control Panel | Regional and Language Options | Regional Options** tab.
- **User**
Lists the person logged on when the action was performed

- **Action**

Lists the action performed. Actions that can be logged depend on the modules your solution is licensed for.

Actions include, but are not limited to:

- Viewing/creating/deleting a document
- Creating a document from an existing document
- Creating a revision/redaction
- Checking out/in a document
- Undoing a check out
- Printing a document
- Exporting/saving a document externally
- Sending a document through internal mail or external mail
- Saving a document's rotation
- Adding/deleting a page
- Reordering pages
- Copying pages to a new document
- Marking/unmarking a page for rescanning or scanning additional pages
- Copying content from text/image documents to the clipboard
- Creating/modifying/viewing/deleting a note
- Viewing document Keyword Values
- Adding/modifying/deleting a Keyword Value
- Adding a signature to a document
- Data mining a document
- Viewing or printing the first page of a document as a thumbnail using the OnBase Web Client's thumbnail viewer

Note: The **Replace Keywords** action in the Configuration module is not logged in a document's history log.

- **Message**

Lists the Document Handle and the Auto-Name of the document

Printing OLE Documents

Depending on the printing method, OnBase may not log a print action when OLE or PDF documents are printed. This behavior occurs when printing is handled by an application other than OnBase.

In the OnBase Web Client, the print action is not logged under these circumstances:

- The user clicks the OLE or PDF application's **Print** toolbar button.
- The user presses **Ctrl + P** in the OLE or PDF application.

The print action is logged when printing is initiated using the **Print** right-click option from the Document Search Results list or the **Document | Print** menu option. These options are available from the ActiveX Web Client.

In the HTML Web Client, users can still send OLE and PDF documents to a server print queue by selecting **Send To | Server Print Queue** from the right-click menu of the Document Search Results list. In this case, OnBase logs a print action when the document is printed through the server print queue.

Printing in the OnBase HTML Web Client

When documents are printed in the HTML Web Client, the following action is logged: **Document [docid] printed to Local Printer. All page(s) printed.** This action is also logged when E-Forms and HTML documents are printed using the **Print** right-click option in either the ActiveX or HTML Web Client.

Printing Thumbnails

If a user prints document thumbnails using the Web Client's thumbnail hit list viewer, the print action is logged when the user presses **Ctrl + P** to open the print dialog box, not when the thumbnails are printed. As a result, the print action is logged even if the user cancels out of the print dialog box.

The print dialog box launched with **Ctrl + P** is external to the Web Client and does not tell the Web Client whether a document has been printed. To ensure print events are logged, the Web Client logs the print action as soon as the dialog box is accessed from the thumbnail hit list viewer.

Filtering a Document History

To filter the actions displayed in the **Document History** window, right-click on the window and select **Filter Items**. The **Select Items to View** dialog box is displayed.

Note: The ability to filter items is available only in the ActiveX Web Client.

This dialog box allows you to filter by action type, user, and date range. These options are described in the following table:

Option	Description
View	Viewing of the document.
Print	Printing of the document.

Option	Description
Mail Document	Mailing of the document to a person who is either an internal user of the system or an external recipient.
Export	Exporting the document.
Modify Keywords	Modification of Keyword Values.
Add Keywords	Addition of Keyword Values.
Send to/from document	Creation and copying of pages to the document from an existing document.
Document Retention	Use of Document Retention process.
Redactions	Creation of Redactions.
Delete Keyword	Deleting Keyword Values.
Delete Page	Removal of a page from the document.
Add page	Addition of a page to the document.
Re-index	Re-indexing of the document.
Verity and Full Text	Document used by legacy Full-Text retrieval or indexing.
Rotation saved	Saving a rotation of an image document.
EDM Status Change	When selected, the transaction log entries corresponding to the following actions are displayed: Check Out, Check In, Undo Checkout
Notes	Application of Notes.
User name	<p>Allows you to display only actions performed by a specific user.</p> <hr/> <p>Tip: To further filter a long list of user names, type in the first few letters of a user name. The list will filter based on user names beginning with the letters you type.</p> <hr/>
Log Date	Allows you to display only actions occurring within a specific date range.

When you are finished, click **OK** to display the filtered results. When a filter is applied, the **Document History** window's title bar displays **(Filtered)** next to its name. To remove the filter, open the dialog box again, click **Clear**, and then click **OK**.

Note: If your system is licensed for Workflow, the **Document History** window contains multiple tabs. When a filter is applied, **(Filtered)** is displayed on the **Document History** tab rather than the window's title bar.

Viewing a Folder's History

A folder's history is a log of all the actions performed on the folder in OnBase. If you have sufficient administrative rights, you can view a history of a folder. A folder's history allows you to:

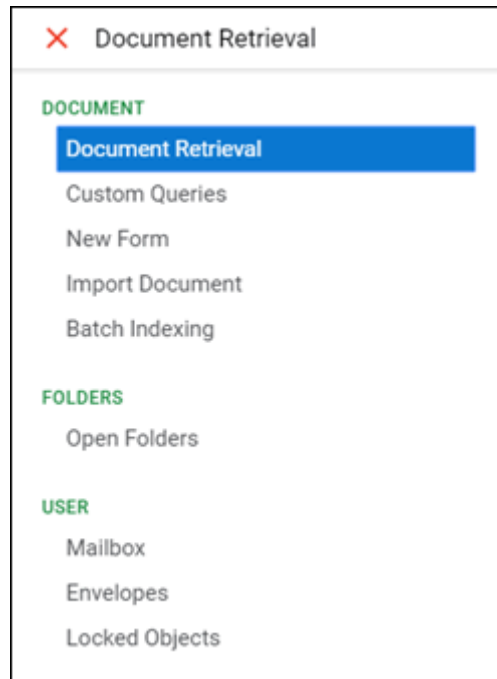
- See who has viewed a folder and ensure only authorized users are accessing it.
- See how a folder has changed over time, including who changed it and when.
- Evaluate which folders are being used and how frequently. For example, you can use this information to determine whether it's safe to remove a folder and whom to contact before deleting it.

Note: If documents were added to or removed from a folder prior to OnBase 5.0, these actions are not displayed in the folder's history. Other actions performed prior to OnBase 5.0 are displayed.

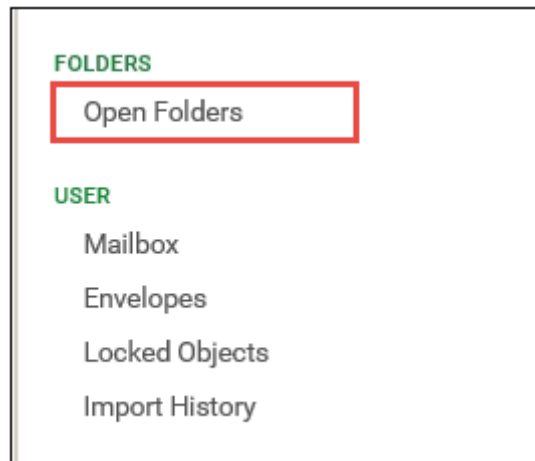
Note: Changes made to folder Keyword Values and folder dates in OnBase 8.2 and earlier are logged under the **Modify Folder Keywords** action. In OnBase 9.0 and later, changes to folder Keyword Values are logged under **Added Folder Keyword** and **Deleted Folder Keyword**, and changes to folder dates are logged under **Modified Folder Date**.

To view a folder's history, complete the following steps.

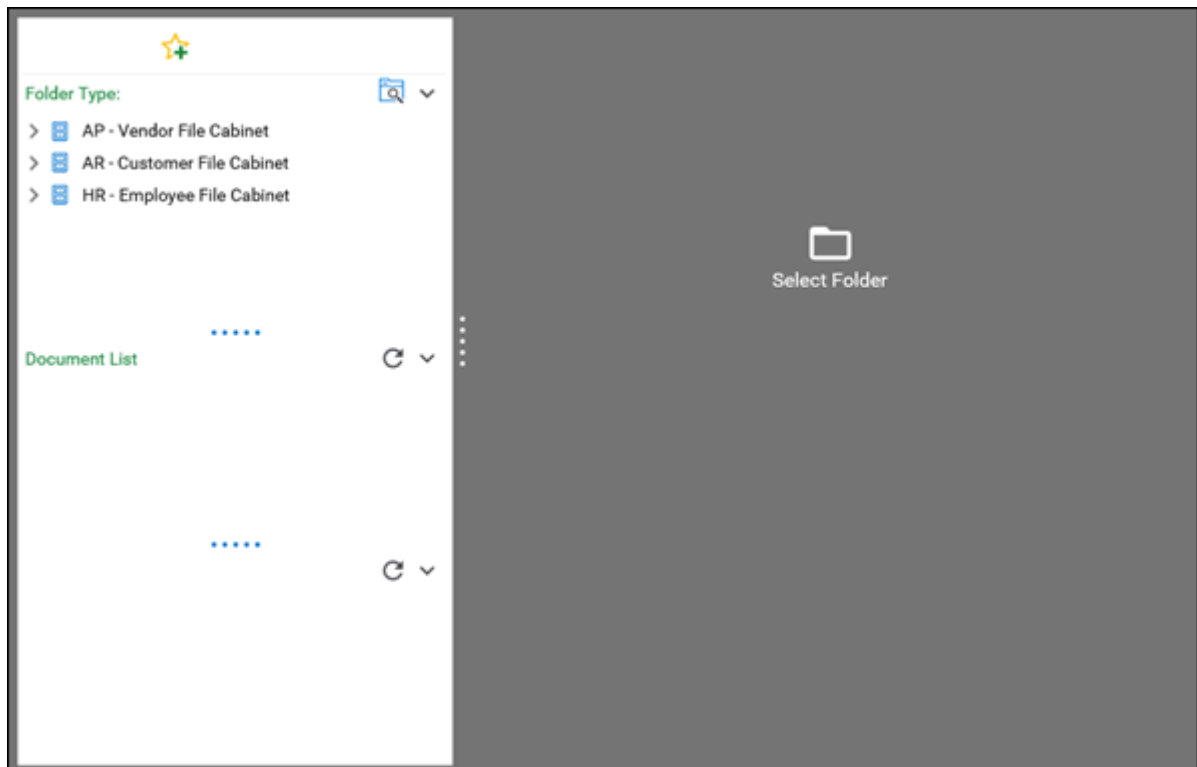
1. Log on to the OnBase Web Client.
2. Select the Main Menu button. The Menu List is displayed.



3. Scroll down to the Folders section, and then select **Open Folders**.



The folders screen opens in a separate window.



4. Open the parent of the folder whose history you want to view.
5. Select the folder whose history you want to view.

6. Right-click and select **History**. The **Folder History** window is displayed.

Minutes Documents - 3/1/2017			
DATE	USER	ACTION	DETAIL
Contains...	Contains...	Contains...	Contains...
4/12/2017 11:16 AM	MANAGER	Viewed Folder and Children	Viewed Folder 'Minutes Documents - 3/1/2017' and Children
4/5/2017 3:46 PM	MANAGER	Added Folder Keyword	Added Keyword (Meeting Date) '4/6/2017' to (116) 'Minutes Documents - 3/1/2017'
4/5/2017 3:44 PM	MANAGER	Viewed Folder Keywords	Viewed keywords on folder 116 (Minutes Documents - 3/1/2017)
4/5/2017 3:39 PM	MANAGER	Viewed Folder Keywords	Viewed keywords on folder 116 (Minutes Documents - 3/1/2017)
4/5/2017 3:38 PM	MANAGER	Viewed Folder Keywords	Viewed keywords on folder 116 (Minutes Documents - 3/1/2017)
Items: 26			
			Close

- The **Date** column displays the date and time the action occurred.
- The **User** column displays the OnBase user who performed the action.
- The **Action** column displays the type of action that occurred.
- The **Detail** column displays a brief description of the action.

User Administration

Web Client users with administrative rights can perform user administration from the **Administration** layout.

To view the rights required for this layout, see [Required Administrative Rights on page 136](#).

For information about available actions in the **Administration** layout, see the following topics:

- [Accessing Administration on page 138](#)
- [Navigation on page 139](#)
- [Creating a New User on page 142](#)
- [Configuring an Existing User on page 143](#)
- [Configuring User Settings on page 144](#)
- [Locking & Unlocking Users on page 152](#)
- [Disconnecting a User on page 154](#)
- [Deleting a User on page 155](#)
- [Sending a System Message to Active Users on page 155](#)

Required Administrative Rights

To configure users using the Web Client's **Administration** layout, you must have the **Web Client** product right and one of the following configuration rights:

- **User Account Admin**
- **User Update Admin**
- **Password Admin**

Each right provides access to different options in the Administration layout, as shown in the following table:

User Account Admin	User Update Admin	Password Admin
Lock/Unlock Account Configure User <ul style="list-style-type: none">• All Settings Delete User Create User Web Diagnostics	Lock/Unlock Account Configure User <ul style="list-style-type: none">• All Settings Web Diagnostics	Unlock Account Configure User <ul style="list-style-type: none">• Password Web Diagnostics

For more information about these rights, see the **System Administration** documentation.

For information about Web Diagnostics, see [Web Diagnostics Page on page 198](#).

Managing User Connections

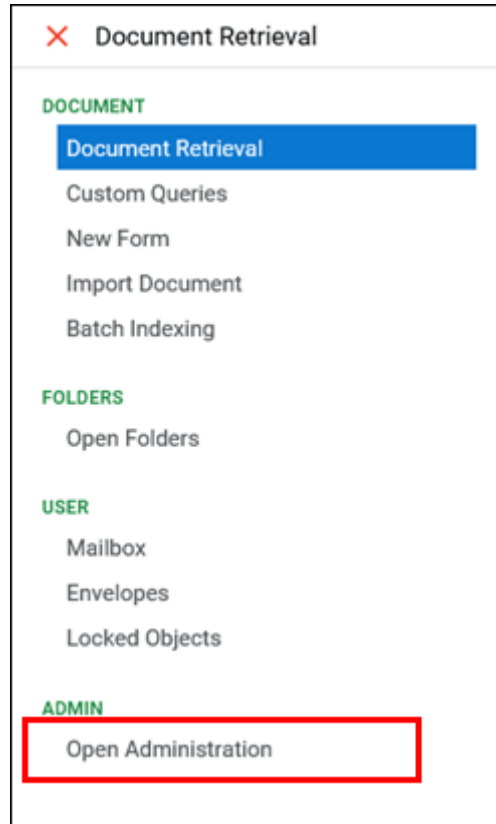
To view and administer user connections using the Web Client's **Administration** layout, you must have the **Web Client** product right and the **User Management** product right. This product right provides access to the following features:

- Show Active Users
- Show Users Consuming Licenses
- Disconnect User

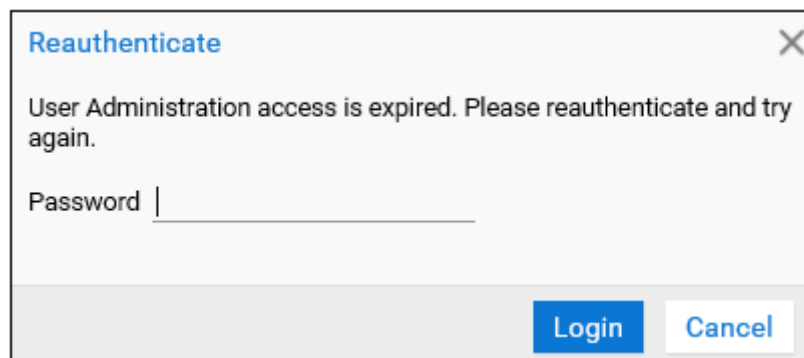
Accessing Administration

To access the **Administration** layout:

1. In the OnBase Web Client, click the Main Menu button and select **Open Administration** from the menu list:



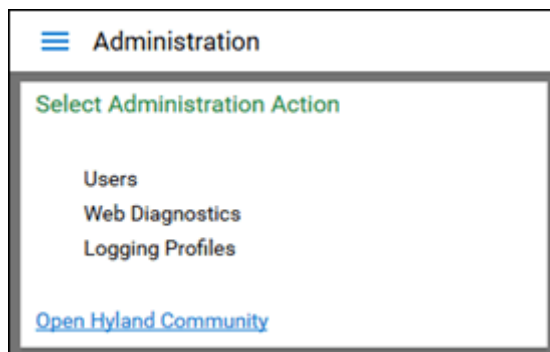
Depending on how the Global Client User is set up in the OnBase Configuration module, the **Reauthenticate** dialog box may be displayed.



This provides an extra layer of security when changing administrative options. Enter your password, and click **Login**.

Note: The reauthenticate option is only supported for the OnBase Client and Web Client. If the incorrect password is entered seven times, the user is returned to the Web Client login screen.

The **Administration** layout is displayed, with administration options listed.



Tip: When you access the **Administration** layout, the **Open Hyland Community** link is available in the Navigation Panel. Click this link to access the latest information from the Hyland Community website. This link is also available in the Help window for users who have the **Usergroup Security** or **User Configuration** configuration right.

2. Select **Users**. Any users for which you have administration rights are displayed.



Navigation

The following topics describe how to navigate the **Administration** layout:

- [Finding a User on page 140](#)
- [Viewing All Users on page 140](#)

- Viewing Active Users on page 140
- Viewing Users Consuming Licenses on page 141
- Refreshing the User List on page 141

Finding a User

Use the **Search** field to find a specific user. This field filters the user list by the following:

- user name
- real name

In the **Search** field, enter part of a user's account name or real name. The user list is automatically filtered to show only users matching the entered characters.

To remove the filter, delete the characters from the **Search** field.

Viewing All Users

To view all users you have rights to administer, select the **Show All Users** option from the drop-down list.

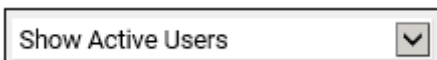
A screenshot of a web interface showing a dropdown menu with the text "Show All Users" and a downward-pointing arrow icon on the right.

To view users in this list, you must have one of the **User Configuration** configuration rights.

Note: Selecting this option does not clear the **Search** field. Any filters applied using this field remain applied when you click **Show All Users**. To remove the filter, clear the **Search** field.

Viewing Active Users

To view users who have an active OnBase session, select the **Show Active Users** option from the drop-down list. The list displays all users considered active by the specific Application Server you are using. This list is sorted in ascending order numerically and alphabetically.

A screenshot of a web interface showing a dropdown menu with the text "Show Active Users" and a downward-pointing arrow icon on the right.

For each user session, the list displays the user name, session ID, time of last access, idle time, consumed licenses and the current Web Browser.

```
MANAGER
Session ID : ce79e87b-30af-4f65-bd10-bd5c0d5d1d09
Last Time Accessed : 3/30/2017 10:41:01 AM - 0 minutes 1 seconds ago
Consumed Licenses : Concurrent Client
Web Browser : IE 11
```

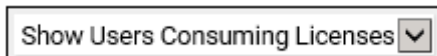
To use this feature, you must have the **User Management** product right in OnBase Configuration. Otherwise, this list is empty.

Note: Selecting **Show Active Users** does not clear filters applied using the **Search** field. To remove the filter, clear the **Search** field.

To close a session, see [Disconnecting a User on page 154](#).

Viewing Users Consuming Licenses

To view all users who are currently consuming licenses, select the **Show Users Consuming Licenses** option from the drop-down list. This list is sorted in ascending order numerically and alphabetically.



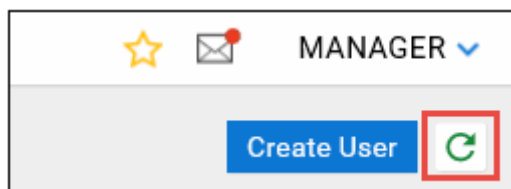
This option displays users currently logged on to OnBase and the type of licenses they are using. Users connected to OnBase using API connections are not displayed.

To use this feature, you must have the **User Management** product right in OnBase Configuration. Otherwise, this list is empty.

Note: Selecting **Show Users Consuming Licenses** does not clear filters applied using the **Search** field. To remove the filter, clear the **Search** field.

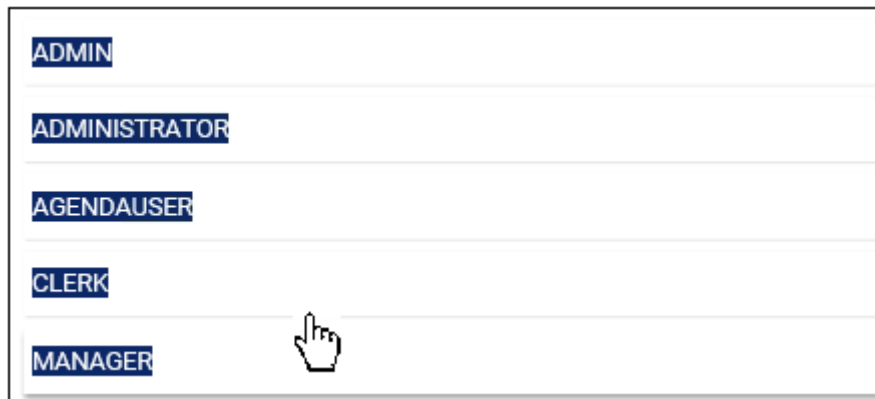
Refreshing the User List

To refresh the user list at any time, click the **Refresh** button.



Selecting Multiple Users

To select multiple users in the user list, click and drag your mouse over the users you want to select.



When multiple users are selected, you can lock/unlock the users' accounts, disconnect the users (provided all are connected), or you can delete the users from OnBase.

See the following topics for more information:

- [Locking & Unlocking Users on page 152](#)
- [Disconnecting a User on page 154](#)
- [Deleting a User on page 155](#)

Creating a New User

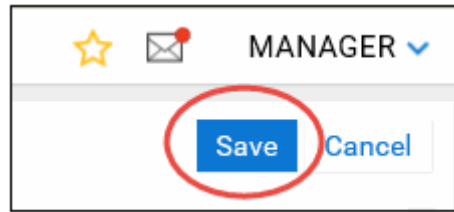
To create a new user:

1. Click the **Create User** button above the user list.



2. Configure the user's settings, which are described under [Configuring User Settings on page 144](#).

- When you are finished configuring the new user, click **Save**.

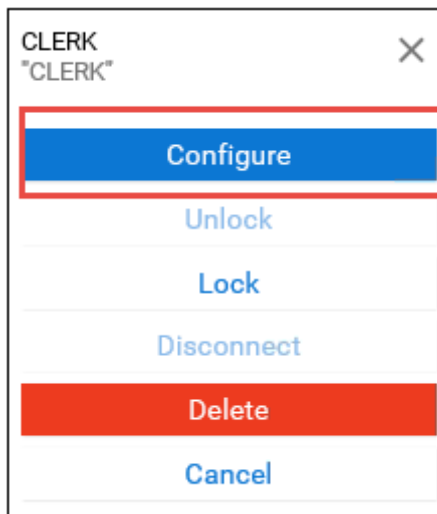


To cancel your changes without saving, click **Cancel**.

Configuring an Existing User

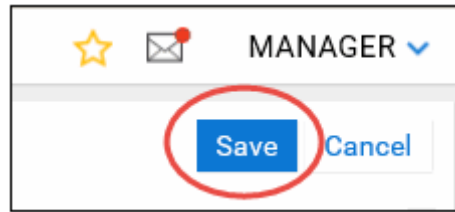
To change an existing user's settings, user groups, or security keywords:

- Click the name of the user you want to configure.
- Click **Configure** from the pop-up menu.



- Configure the user's settings, which are described under [Configuring User Settings on page 144](#).

4. When you are finished configuring the user, click **Save**.



To cancel your changes without saving, click **Cancel**.

Note: If you change a user's name, the change is not reflected in the user list until you click **Refresh**.

Configuring User Settings

When you create or configure a user, you can modify the several types of user settings. Continue to the following topics to configure each group of settings:

- [Accessing User Settings on page 144](#)
- [General Settings on page 145](#)
- [User Assigned License on page 146](#)
- [User Groups on page 148](#)
- [Security Keywords on page 148](#)

Accessing User Settings

To access the user configuration screen, do one of the following:

- To create a new user, click the **Create User** button above the user list.
- To configure an existing user, click the name of the user you want to configure, and then click **Configure**.

General Settings

General settings include the user's name, email address, and password, among others.

1. Modify the general user settings listed under **General Settings**:

GENERAL SETTINGS

User Name	CLERK
Real Name	CLERK
Email Address	
<input type="checkbox"/> Named Web User	
Password	
Verify Password	
<input type="checkbox"/> Require Password Change on Next Login	

Available settings are described in the following table:

Setting	Description
User Name	Enter the user name to be used to log on to OnBase. Up to 74 characters are permitted. If you are configuring an existing user, you can also change the user's user name.
Real Name	Enter the real name of the new user (or any other text string you want to use for identification). Up to 40 characters are permitted.
Email Address	(Optional) Enter the user's email address. Up to 255 characters are permitted.
Named Web User	<p>(Optional) This option is only available if your OnBase solution uses legacy licensing (instead of simplified licensing).</p> <p>Select this option to assign a Named Web User license to the new user. A Named license (as opposed to a Concurrent license) guarantees the specified user a login connection to the database.</p> <p>Note the following:</p> <ul style="list-style-type: none"> • A Named Web User can not simultaneously log on as part of a concurrent license pool. • If your OnBase solution uses a user template to create new users and that user template has a Named User license assigned to it, any user created from that template is also assigned a Named User license, regardless of whether you select the Named Web User option when creating the user from Web Client Administration.

Setting	Description
Password	Enter the user's password. The maximum number of characters allowed may vary depending on any applicable password policies. Note: Fill out the password field only when creating a new user or changing an existing user's password. If you are modifying other settings for an existing user, this field can be left blank.
Verify Password	Enter the user's password again. The Password and Verify Password values must match exactly.
Require Password Change on Next Login	Select this option to require the user to change their password the next time they log in.

2. Do one of the following:
 - Continue to [User Assigned License on page 146](#) to assign licenses (if using simplified licensing).
 - Continue to [User Groups on page 148](#) to assign user groups.
 - Click **Save** to save your changes and return to the user list.

User Assigned License

The **User-Assigned License** section is only available if your OnBase solution uses simplified licensing. Beginning in OnBase Foundation EP5, OnBase supports a simplified licensing model that automatically bundles legacy product licenses into base packages of related functionalities.

For more information on simplified licensing support in OnBase Foundation EP5, see the **Technical Requirements Overview for New Installations and Upgrades** document. For more information on the license packages available to you, contact your account manager.

To assign a license to the user:

1. Modify the user licensing setting listed under User-Assigned License:

USER-ASSIGNED LICENSE

☒ Unassigned
☐ Essential User
☐ Standard User
☐ Premier User

Available settings are described in the following table:

Setting	Description
Unassigned	Do not assign a license to the user.
Essential User	Assign the Essential User license to the user. This license includes basic functionalities in OnBase.
Standard User	Assign the Standard User license to the user. This license includes all Essential User functionalities, as well as additional functionalities.
Premier User	Assign the Premier User license to the user. This license includes all Essential User and Standard User functionalities, as well as additional advanced functionalities.

2. Do one of the following:
 - Continue to [User Groups on page 148](#) to assign user groups.
 - Click **Save** to save your changes and return to the user list.

User Groups

User group assignment determines the user groups a user belongs to.

- Do one of the following to assign a user to a user group:
 - Click the user group's name under **Unassigned Groups**. The group moves to the **Assigned Groups** list.
 - Type the Unassigned group name in the **Filter** field. The group name moves to the top in the list. Click the group name to move it to the **Assigned Groups** list.

The screenshot shows a web interface titled "USER GROUPS". It is divided into two main sections: "Unassigned Groups" on the left and "Assigned Groups" on the right. The "Unassigned Groups" section has a search bar with a magnifying glass icon and the text "Type to filter". Below the search bar is a list of group names: ADMIN CONFIG, ADMINISTRATOR, AgendaGroup, GroupA, GroupB, Meditech User, and MedPubUser. The "Assigned Groups" section shows a list with two items: CLERK USERS and MANAGER. Both lists have a vertical scrollbar on the right side.

- To remove a user from a user group, click the user group's name under **Assigned Groups**. The group moves to the **Unassigned Groups** list.
- Do one of the following:
 - Continue to [Security Keywords on page 148](#) to assign Security Keywords.
 - To save your changes and return to the user list, click **Save**.

Security Keywords

Depending on the **AllowSecurityKeywordsAdmin** setting in the Web Server's Web.config, you may be able to add and edit Security Keywords for each user. Security Keywords are unavailable if **AllowSecurityKeywordsAdmin** is set to **false**.

Security Keywords allow you to define specific limitations on an individual's document retrieval rights by restricting retrieval based on Keyword Value. For example, a shipping clerk could be limited to retrieving documents only from the Manufacturing and Distribution Divisions. The same clerk could also be prevented from retrieving documents related to a specific customer who receives products through another channel.

When assigning a Security Keyword, you must specify whether the document Keyword Value should be **Equal To** or **Not Equal To** the Security Keyword Value.

- **Equal To** means that the user can retrieve only documents with the specified Keyword Value.
- **Not Equal To** means that the user can retrieve all documents except those with the specified Keyword Value.

Note: Security Keywords do not enable users to retrieve documents that they lack rights to retrieve. For example, if the user lacks retrieval rights to Accounts Receivable documents from the Distribution Division, then that user cannot retrieve these documents regardless of his assigned Security Keywords.

The system administrator determines which Keyword Types can be used for Security Keywords and may also establish other validation rules.

You can add, edit, and delete Security Keywords for a user at any time. Changes are applied the next time the user logs on.

Assigning Security Keywords

To assign Security Keywords to a user during user configuration or creation:

1. Do one of the following to select the Keyword Type to be used for security.
 - Click the a keyword name under **Available Keywords**. The group moves to the **Assigned Keywords** list.
 - Type a keyword name in the **Filter** field. The keyword name moves to the top of the list. Click the keyword name to move it to the **Assigned Keywords** list.

The screenshot displays the 'SECURITY KEYWORDS' interface. On the left, under 'Available Keywords', there is a search bar with a magnifying glass icon and the text 'Type to filter'. Below the search bar is a list of keywords: ABA, Account #, Account Number, Agenda Item Caption, Agenda Item Key, Batch #, and Batch Number. The list has a vertical scrollbar on the right. On the right side, under 'Assigned Keywords', there is an empty rectangular box.

2. Click the operator to change it to **Equal To** or **Not Equal To**.
 - **Equal To** allows the user to retrieve documents whose Keywords match the specified value.
 - **Not Equal To** prevents the user from retrieving documents whose Keywords match the specified value.

Assigned Keywords	
Account #	<u>Equal To</u> _____

3. In the field provided, enter the Keyword Value.

Assigned Keywords	
Account #	<u>Equal To</u> <u>153268</u>

- Repeat steps 1-3 for each additional Security Keyword to be assigned to the user.

Note: Each configured Security Keyword must be unique. If you try to save user settings with duplicate Security Keywords, the duplicates will be highlighted and you cannot save the settings until you resolve the duplicates.

The following example illustrates the **Assigned Keywords** list after several Security Keywords have been configured:

Assigned Keywords	
Account #	<u>Equal To</u> 153268
File Name	<u>Equal To</u> In Progress
Site ID	<u>Not Equal To</u> SP1

To remove a Security Keyword, select it from the **Assigned Keywords** list. The Security Keyword is removed.

- When finished, click **Save**. The Security Keywords take effect the next time the user logs on to OnBase.

Enabling and Disabling Workflow Trace

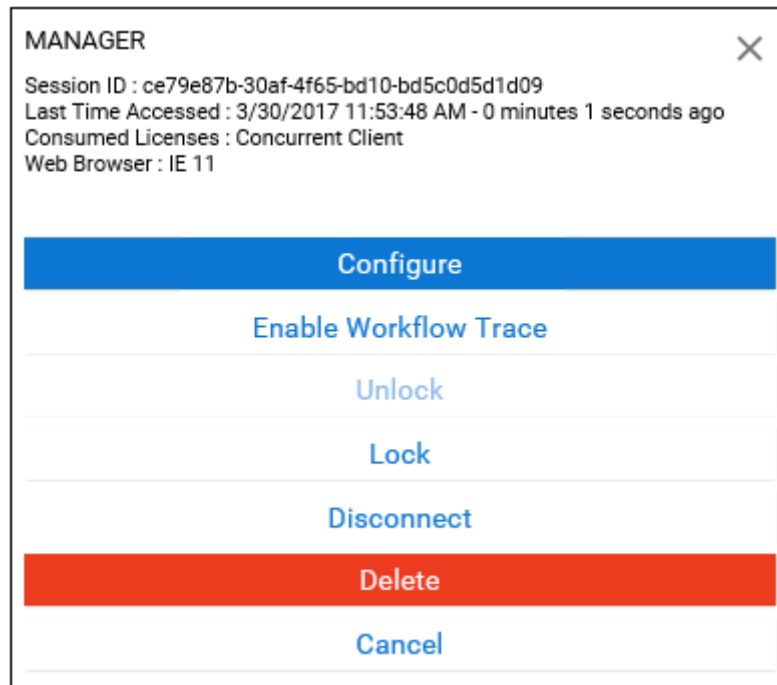
The **Administration** layout allows you to enable Workflow trace on a user as needed. Workflow trace information for that user is logged on the Workflow Trace tab in the Diagnostics Console and can be used for troubleshooting.

To enable Workflow Trace:

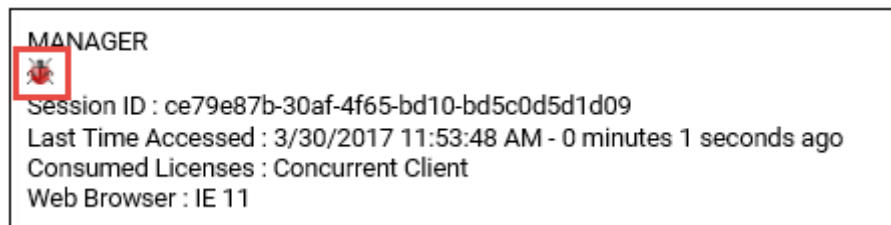
- Select the **Show Active Users** option from the drop-down list.

Show Active Users	▼
-------------------	---

- Click the user box to display the user configuration options.



- Click the **Enable Workflow Trace** option. The Workflow Trace is enabled and an icon is displayed under the User name indicating that Workflow Trace is enabled for this user.



- Disable the Workflow Trace by clicking the User box, and then selecting the **Disable Workflow Trace** option.

Locking & Unlocking Users

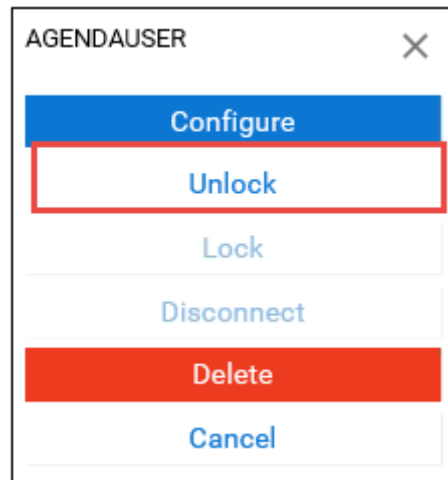
The **Administration** layout allows you to lock and unlock user accounts. When an account is locked, no one can use the account to log on to OnBase. User accounts may be locked automatically for various reasons, such as when a user has multiple failed logon attempts.

See the following topics:

- [Unlocking a User Account on page 153](#)
- [Locking a User Account on page 153](#)

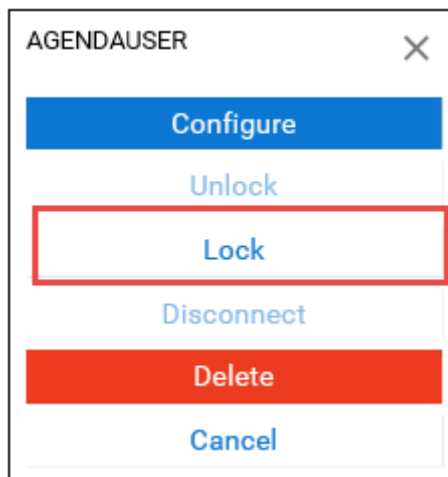
Unlocking a User Account

1. Select the locked user from the user list.
2. Click **Unlock** from the pop-up menu. OnBase unlocks the selected account.



Locking a User Account

1. Select the user from the user list.
2. Click **Lock** from the pop-up menu. OnBase locks the selected account.



Disconnecting a User

From the **Administration** layout, you can disconnect an active Web Client user.

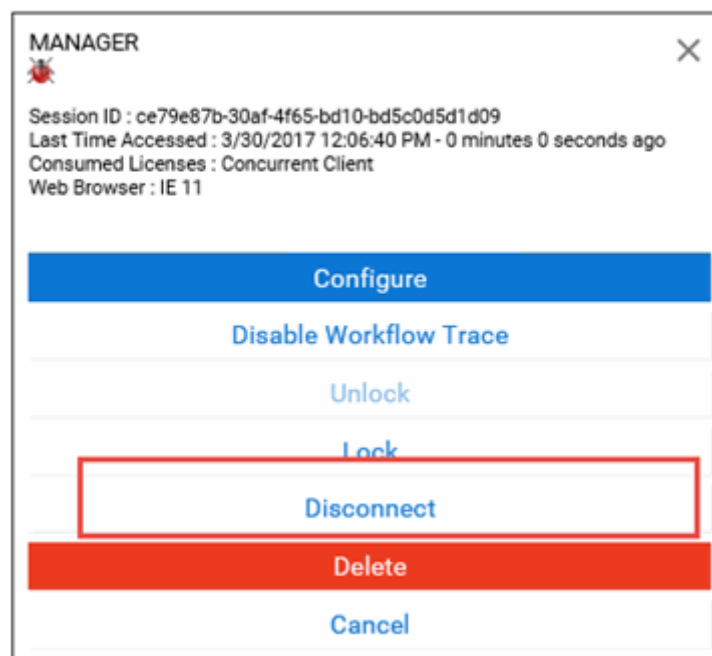
Caution: Disconnecting an active user can end the user's session in OnBase. Depending on your solution's authentication method and the user's context at the time of disconnection, the user may be fully logged out of OnBase without warning, and any unsaved changes made by the user may be lost. Always ensure the user is not actively working in OnBase when you disconnect an active session.

To disconnect an active Web Client user:

1. Select the **Show Active Users** option from the drop-down list.



2. Select the user you want to disconnect.
3. Click **Disconnect** from the pop-up menu. This button is available only if the user is currently connected.

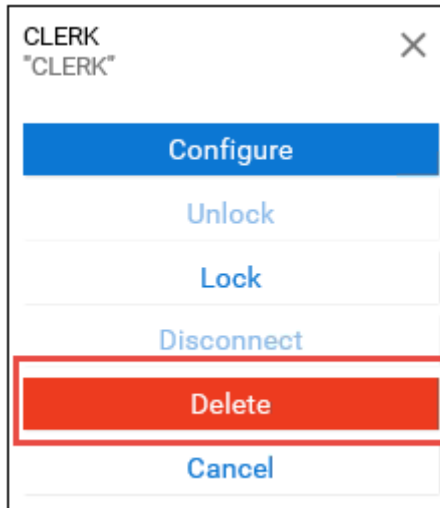


The user's session is disconnected.

Deleting a User

You can delete existing users from the Web Client at any time. Once deleted, a user can no longer log on to OnBase.

1. Select a user from the user list.
2. Click **Delete** from the pop-up menu.



3. Click **OK** to confirm. The user account is deleted from OnBase.

Sending a System Message to Active Users

Administrators can send a system message to users who are currently logged into the Web Client. The message can be sent to a single user or all active users. The message is displayed to the user as a pop-up notification in the Web Client window. The user must close the message to resume their session.

Sending system messages requires additional configuration in the Web Server web.config file. Locate the **owin:AutomaticAppStartup** key in the **appSettings** section and set it to **true**:

```
<add key="owin:AutomaticAppStartup" value="true" />
```

Additionally, it is recommended that the **WebSocket Protocol** Windows Server feature is enabled for IIS for optimal performance. The WebSocket Protocol feature can be enabled in the **Turn Windows features on or off** dialog box or in the Server Manager. See Microsoft documentation for more information on Windows Server features and roles.

Once configuration is complete, follow these steps to send a system message to all active users:

1. In the Web Client, click the Main Menu button and select **Open Administration** from the menu list. The **Administration** layout is displayed.
2. Select **Send Message**. The system message form is displayed.

Send a message to all users currently logged in.

SUBJECT 50

☒ All
☐ Select a User

SELECT A USER

ANDREW LINCOLN
JANE HARPER
MANAGER

MESSAGE 250

Send

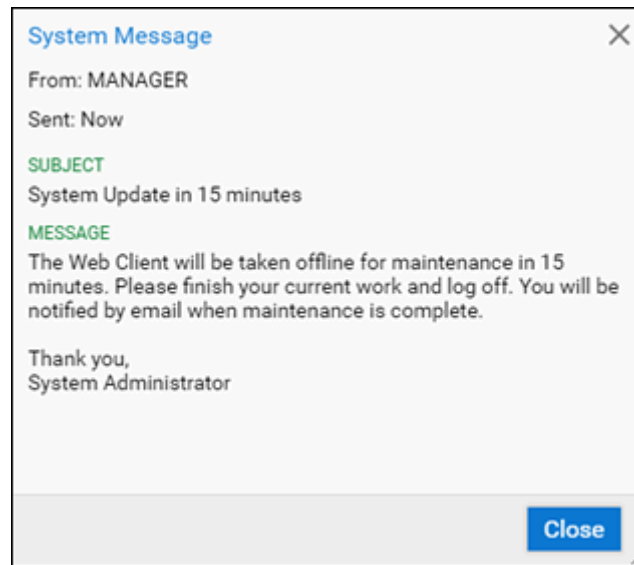
3. Enter a subject for the message in the **Subject** field. The character counter displays the remaining characters allowed in the field.

Note: The **Subject** field is required.

4. Select the **All** option to send the message to all users currently logged into the Web Client, or select **Select a User** to send the message to a single active user.
5. If you are sending the message to a single user, select the user name from the **Select a User** list.
6. Enter a message body for the system message. The character counter displays the remaining characters allowed in the field.

Note: The **Message** field is required.

7. Click **Send**. The system message is sent to all users currently logged into the Web Client.



Additional Web Server Documentation

Several modules are included with the OnBase Web Server. Additional documentation is available for these modules in separate module reference guides and help files.

ActiveX Web Client

See the **Web Client** module reference guide or help file for information about using the ActiveX Web Client.

HTML Web Client

For HTML Web Client considerations, see the [Feature Matrix on page 340](#).

See also the **Web Client** module reference guide or help file, which provides detailed information about Web Client features and behavior.

DocPop

See the **DocPop** documentation for detailed information regarding DocPop.

FolderPop

See the **FolderPop** documentation for detailed information regarding FolderPop.

FormPop

For information about FormPop, see [FormPop on page 306](#).

LoginFormProc

For information about LoginFormProc, see [LoginFormProc on page 302](#).

PDFPop

See the **PDFPop** documentation for detailed information regarding PDFPop.

StatusView

See the **StatusView** documentation for detailed information about StatusView.

Troubleshooting

This section describes potential errors or issues you may encounter and their possible causes. OnBase also offers the following diagnostic tools:

- The Diagnostics Console logs events and errors generated by OnBase modules. You can use the Diagnostics Console to monitor performance and troubleshoot issues. See [Diagnostics Console on page 195](#).
- The Web Diagnostics page, `diagnostics.aspx`, displays installation and configuration information for the Web Server and for the client workstation you are working on. See [Web Diagnostics Page on page 198](#).
- The OnBase Log, which is available in the Windows Event Viewer on the server, logs events and errors from the OnBase Web Server or Application Server.

For Web Server events, **ASP.NET Web Client** is listed as the source. For Application Server events, **Hyland Application Server** is listed as the source.

Users Cannot Log On Using Active Directory Authentication

Before troubleshooting this issue, ensure that you have set up OnBase and the Web Server for Active Directory authentication as described on page 54 of this manual and also as described in the **Legacy Authentication Methods** module reference guide.

If your solution is configured to use Active Directory authentication, users may be presented with a Windows logon dialog box when they attempt to connect to the Web Server.



This dialog box is usually displayed if the Web Server's NTLM settings are not configured properly.

To check your NTLM settings, see the following topics:

- [Checking NTLM settings in IIS 8.x](#)
- [Checking NTLM settings in IIS 10.x](#)

Checking NTLM settings in IIS 8.x

To check NTLM settings in IIS 8.x, see the following Microsoft article:

[http://technet.microsoft.com/en-gb/library/cc754628\(WS.10\).aspx](http://technet.microsoft.com/en-gb/library/cc754628(WS.10).aspx)

To force the use of NTLM, execute the following command in the Command Prompt:

appcmd set config /section:windowsAuthentication -providers.[value='Negotiate'].value

If the issue persists, see [Additional Steps on page 160](#).

Checking NTLM settings in IIS 10.x

To check NTLM settings in IIS 10.x, see the following Microsoft article:

[http://technet.microsoft.com/en-gb/library/cc754628\(WS.10\).aspx](http://technet.microsoft.com/en-gb/library/cc754628(WS.10).aspx)

To force the use of NTLM, execute the following command in the Command Prompt:

appcmd set config /section:windowsAuthentication -providers.[value='Negotiate'].value

If the issue persists, see [Additional Steps on page 160](#).

Additional Steps

If the Windows logon dialog box is still displayed when users attempt to log on, ensure the Web Server is listed as a trusted site in Internet Explorer on the client workstations.

1. From an Internet Explorer window, select **Tools | Internet Options**.
2. Click the **Security** tab.
3. Click **Local intranet**.
4. Click **Apply**, and then click **OK**.
5. From the **Security** tab, click **Custom level**.
6. Scroll to the **User Authentication** settings, which are located at the bottom of the list.
7. Under **Logon**, select **Automatic logon with current user name and password**.
8. Click **OK** to close **Security Settings**.
9. Click **OK** to close **Internet Options**.
10. If users are still unable to log on from client workstations, verify that the **Authenticated Users** Windows user group has the **Read** permission for the Web Server's virtual directory.

The Screen is Empty Upon Login

If a user has the **Retrieve Dialog** and **Retrieve/View** Privileges and the **Client** and **Web Client** Product Rights, but has no rights to Document Types, then the screen is empty.



Assign the user to the appropriate Document Types to allow the user to retrieve documents.

ActiveX Controls Fail to Load

ActiveX Controls may fail to load due to various causes. See the following topics for more information:

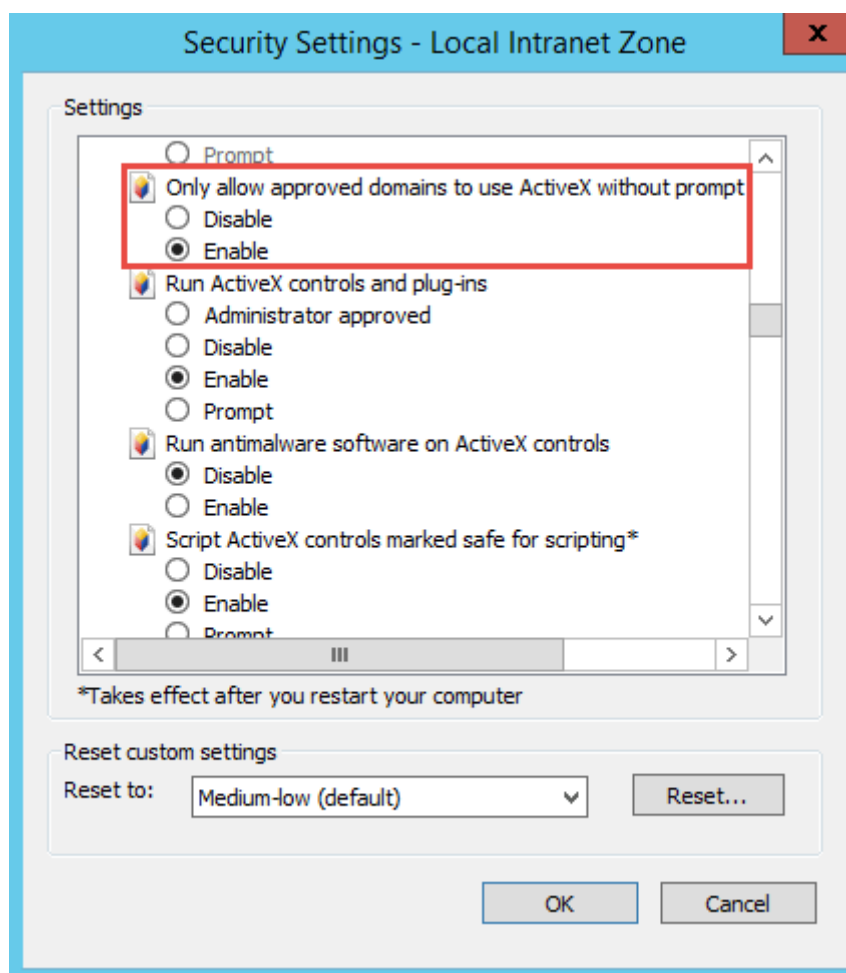
- [ActiveX Controls Fail to Load in Internet Explorer on page 161](#)
- [ActiveX Controls Fail to Load in Internet Explorer After an Upgrade on page 164](#)
- [ActiveX Controls Fail to Load in a Virtualization Environment on page 164](#)

ActiveX Controls Fail to Load in Internet Explorer

ActiveX controls may fail to load on workstations running Internet Explorer. Depending on the workstation's Internet Explorer security settings, one of the following symptoms may occur:

- The ActiveX control fails to load, and an icon with a red x is displayed in the ActiveX component's location.
- The Information Bar is displayed, providing the option to **Run** or **Don't Run** the ActiveX control. When the user clicks **Run**, the ActiveX control fails to load.
- Internet Explorer displays the error, **Failed to load [control name] ActiveX control**.

Cause — ActiveX controls may fail to load as a result of an ActiveX security setting in Internet Explorer. When enabled, the **Only allow approved domains to use ActiveX without prompt** setting can prevent ActiveX controls from loading properly in OnBase Web applications, including the OnBase Web Client, integrations for SharePoint and SAP, and the Medical Records Management Solution.



Solution — To ensure that ActiveX controls can load properly, preset the allowed OnBase ActiveX controls and the associated sites in the registry as described in “Per-Site ActiveX Controls,” available at the following location:

[http://msdn.microsoft.com/en-us/library/dd433050\(VS.85\).aspx#_itpro](http://msdn.microsoft.com/en-us/library/dd433050(VS.85).aspx#_itpro)

This article describes how to allow specific ActiveX controls to run for specific sites. See the “Code Samples” topic for sample scripts to update the registry. These scripts use the CLSIDs of the ActiveX controls being enabled. The CLSIDs for the OnBase Web ActiveX controls are provided in the following table:

ActiveX Control	{CLSID}
HylandDocumentSelect	{C5526B6F-F197-4705-A554-0612494ADD7D}

ActiveX Control	{CLSID}
HylandViewer	{7F1D1BFA-E7D1-41E0-834F-98C2544CFB9D}
OBXAltDocumentSelect	{22198BEF-75F7-4117-885A-40CCC22F5C88}
OBXAltViewer	{B4E711EF-3137-4E2C-940B-1223BC7103C0}
OBXFileSvc	{CAAB6896-E95D-4476-9B0C-B968FADE56AD}
OBXPopup	{826F6DD1-7095-4BB5-BE96-CB4E8EE0C324}
OBXWebControls	{0FCFCB28-BAF6-422B-985D-A662E207F4A6}
OBXWebDocumentSelect	{A1955722-2B57-4B6D-B5E4-2900AE424672}
OBXWebPrint	{3F2F1376-BD9E-495D-BB8B-66E7A872160B}
OBXWebScan	{DB601251-258A-4743-A522-B45AC1E45B7F}
OBXWebViewer	{A8A7310D-814C-4695-AD02-235675E4BD60}
OBXWorkflowLoadBalance	{D6DB39B0-5BA5-476D-B0A5-3A2D7E937840}

Caution: Modify the registry at your own risk. Incorrectly editing the Windows registry can cause serious problems that may require you to reinstall your operating system. Be sure to back up the registry before making any changes to it. For more registry information, see the following Microsoft articles: <http://support.microsoft.com/kb/256986> and <http://technet.microsoft.com/en-us/library/cc725612.aspx>

For example, a script that allows the ActiveX viewer (OBXWebViewer) to run on all domains may include the following:

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{A8A7310D-814C-4695-AD02-235675E4BD60}\iexplore\AllowedDomains]
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{A8A7310D-814C-4695-AD02-235675E4BD60}\iexplore\AllowedDomains\*]
```

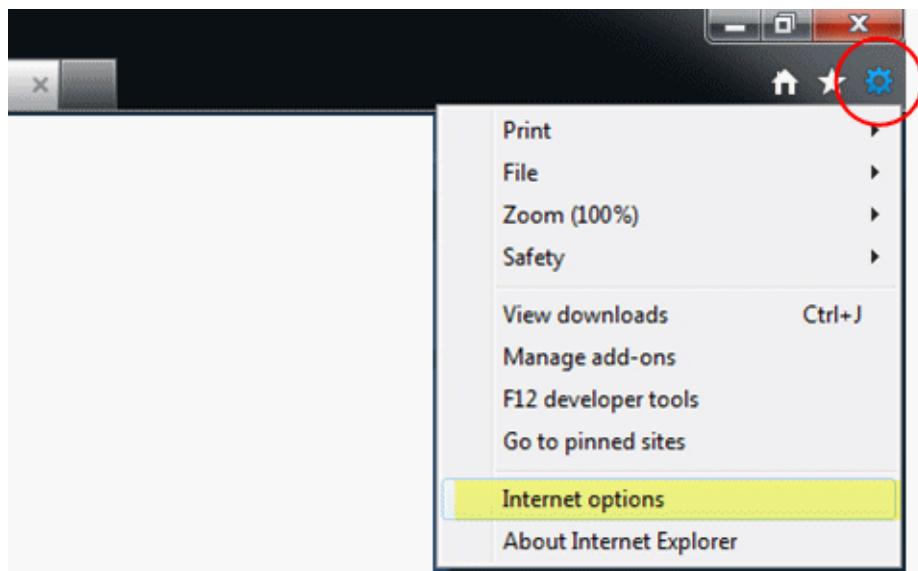
More information about writing registry scripts can be found at the following location: <http://support.microsoft.com/kb/310516>

ActiveX Controls Fail to Load in Internet Explorer After an Upgrade

After an upgrade, users running Internet Explorer may be unable to successfully download the Web ActiveX controls through the browser. For example, a user may be continuously prompted to download the controls.

This issue may be due to the presence of older versions of the ActiveX controls in the users' Temporary Internet Files. To address this issue, clear the Temporary Internet Files on the affected workstations.

1. Open Internet Explorer.
2. Click **Internet options** from the Tools menu (represented by the gear icon).



3. Under **Browsing history**, click **Delete**.
4. Clear all options except for **Temporary Internet Files**.

Note: The **Preserve Favorites website data** option must not be selected.

5. Click **Delete**. The temporary files are deleted.
6. Click **OK** to close **Internet Options**.

ActiveX Controls Fail to Load in a Virtualization Environment

If the Web ActiveX controls are installed in a virtualization environment, they may not load successfully when a user attempts to access the Web Client or DocPop through a published application. The **Loading ActiveX controls** message is displayed, but the controls never load.

This issue can be resolved by modifying the Internet Options on the workstation running Internet Explorer. In a remote session, this is the Remote Desktop Server, not the client workstation.

To modify the Internet Options:

1. From an Internet Explorer window, select **Tools | Internet Options**.
2. Click the **Advanced** tab.
3. Under **Security**, select **Allow active content to run in files on My Computer**.
4. Click **OK** to close **Internet Options**.
5. Restart Internet Explorer. Internet Explorer must be restarted for the setting to take effect.

Text Is Too Small

In the Web Client, you can increase the size of text on HTML components by editing the locale-specific **font.css** file that resides in [dmsVirtualRoot]\Styles\XP.

When you increase the font size for one style, you should also increase the font size on all styles that have the same font size as the original. This practice ensures that text is sized consistently throughout the Web Client.

For example, if a font size of 10px is too small, you can replace all instances of **font-size: 10px** with **font-size: 11px**. The default font size in most Web Client contexts is 11px.

By default, Web Client styles are set to expire after seven days, so any style changes are not reflected until the styles expire. To apply changes immediately during testing, delete the contents of the client's **Temporary Internet Files** folder and set the [dmsVirtualRoot]\Styles contents to **Expire Immediately**. This setting is applied on the **HTTP Headers** tab of the **Styles Properties** dialog box in the Internet Information Services Manager. Change the expiration back to seven days when you are finished testing to preserve Web Server performance.

Note: Settings in onbasemain.min.css do not apply to text displayed in ActiveX components, which include many dialog boxes and the Document Search Results list in the ActiveX Web Client.

Thumbnails Are Blank

This issue may occur if a user makes a request for a document while the volume is online, but the file that needs to be retrieved is not on the volume.

Using the Tab Key to Navigate the HTML Web Client in Safari

In order to use the **Tab** key to navigate between areas in the HTML Web Client in Safari, you must enable the **Press Tab to highlight each item on a webpage** option in Safari. After this option is enabled, users will be able to navigate the HTML Web Client in Safari by using the **Tab** key.

Scroll Bars Don't Display in Safari

By default, in macOS, scroll bars are not always displayed, which may suggest to users that there is no additional content in certain windows or scrollable boxes. This is due to a system setting within macOS that enables scroll bars to be hidden by default.

To allow scroll bars to always be visible, navigate to **System Preferences | General** and set the **Show scroll bars** option to **Always**.

Troubleshooting Microsoft Office Documents

The following topics describe possible Microsoft Office issues that Web Client users may encounter.

- [The Web Client Loses Focus When Word Documents Are Opened on page 166](#)
- [OLE Documents Are Opened Externally on page 167](#)
- [Users Cannot Print Microsoft Word Documents on page 167](#)
- [Users Cannot Open Microsoft Visio Documents on page 167](#)
- [Excel Documents Opened Externally Are Unresponsive on page 168](#)
- [Users Cannot Open CSV Files in Excel on page 169](#)

The Web Client Loses Focus When Word Documents Are Opened

Web Client users may have trouble viewing Microsoft Word documents in the Web Client if they currently have Microsoft Word open. When a user attempts to open a Word document from the Web Client, the open Word application becomes active, taking the focus away from the Web Client.

This behavior is the inherent behavior of Microsoft Word and is not specific to OnBase. Placing a hyperlink to a Word document on a HTML page that is loaded directly in Internet Explorer will exhibit the same behavior outside of OnBase.

To resolve this issue in the Web Client, ensure **openOfficeDocumentsInSeparateWindow** is set to **true** in the Web Server's Web.config file. This setting is set to **true** by default, allowing Office documents to be opened externally in their native applications. For more information about this setting, see [Office Documents Setting on page 281](#).

OLE Documents Are Opened Externally

By default, Microsoft Office documents are opened in their native applications instead of the Web Client's document viewer. You can control this in two ways: the **openOfficeDocumentsInSeparateWindow** setting in the Web Server's Web.config file, and by modifying the Windows Registry to allow Microsoft Office files to open in the same window.

To prevent Web Server applications from opening documents externally, set **openOfficeDocumentsInSeparateWindow** to **false**, and implement the workaround outlined in Microsoft KB article 927009 (<http://support.microsoft.com/kb/927009>). Under these conditions, the Web Client attempts to open Office documents within the browser window.

Note: When **openOfficeDocumentsInSeparateWindow** is set to **true**, and you have implemented the Microsoft workaround, it overrides the modified registry setting. For more information about the **openOfficeDocumentsInSeparateWindow** setting, see [Office Documents Setting on page 281](#).

The fix provided by Microsoft KB article 927009 affects how Internet Explorer opens any document with the selected file extension, not just OnBase documents. For example, Word documents are always displayed within the browser window when opened from a Web site.

Note: In some cases, applying this setting may interfere with users' work. If users need to work with Microsoft Excel documents in another application while viewing Excel documents within their Internet browsers, the documents in the other application may become unresponsive. For more information, see [Excel Documents Opened Externally Are Unresponsive on page 168](#).

Users Cannot Print Microsoft Word Documents

Users may be unable to print Microsoft Word documents that they opened from the OnBase Web Client. When users attempt to print Word documents by pressing **Ctrl + P** or clicking the **Print** button in Word's standard toolbar, a page containing the URL to the Web page is printed.

To allow a user to print the Word document by pressing **Ctrl + P** or by clicking the **Print** button, instruct the user to clear the **Always ask before opening this type of file** option from the **File Download** dialog box that is displayed when the user attempts to open the document. After this option is cleared, the user can print the document using the **Print** toolbar button.

See [Printing OLE Documents on page 129](#) for logging limitations associated with these printing methods.

Users Cannot Open Microsoft Visio Documents

Users may be unable to open Microsoft Visio documents from the Web Client. For Visio documents to be viewable in the Web Client, the OnBase file format associated with the documents must be configured to use the Custom viewer type. You can configure the file format so that documents are opened using either of the following:

- The full installation of Microsoft Visio
- Only the Visio viewer

To open Visio documents using the full installation of Microsoft Visio on the user's workstation, set the following options within the **File Format Settings** dialog box in OnBase Configuration:

Option	Value
Viewer Type	Custom
Command Line for Custom Viewer	"C:\Program Files\[Path to Visio executable]" %P%N
MIME Type	application/vnd.ms-visio
Default Extension	VSD

To open Visio documents using only the Visio viewer, set the following options within the **File Format Settings** dialog box:

Option	Value
Viewer Type	Custom
Command Line for Custom Viewer	"C:\Program Files\Internet Explorer\iexplore.exe" -nohome %P%N
MIME Type	application/vnd.ms-visio.viewer
Default Extension	VSD

Excel Documents Opened Externally Are Unresponsive

Users may notice that when they have one Microsoft Excel document open, opening another Excel document in the OnBase Web Client causes the first Excel document to become unresponsive. This behavior occurs when all of the following conditions are met:

- The user has one or more Excel documents open.
- The user accesses another Excel document through an iframe in a browser window. (Iframes, or in-line frames, are panes embedded in a Web page that display external content, such as documents or other Web pages.)
- The Excel document in the iframe has been clicked or activated, shifting the focus from the Excel document that was opened first to the one displayed in the iframe.

Under these conditions, the Excel document the user was originally working on becomes unresponsive. When the Excel document in the iframe is closed (for example, by navigating away from the Web page or by closing the browser window), the original document becomes available. This behavior also occurs in environments external to OnBase. It may be more noticeable in the OnBase Web Client because the Web Client's document viewer is an iframe.

To address this issue, use one of the following methods:

- [Modifying the Web.config Setting for Office Documents on page 169](#)
- [Changing the Order of Document Access on page 169](#)

Modifying the Web.config Setting for Office Documents

To address this issue, set **openOfficeDocumentsInSeparateWindow** to **true** in the Web Server's Web.config file. When this setting is **true**, Microsoft Office documents (including Excel worksheets) are opened in their native applications rather than in the browser window. Users then can work with the original Excel document and the OnBase document without either one becoming unresponsive.

For more information about the **openOfficeDocumentsInSeparateWindow** setting, see [Office Documents Setting on page 281](#).

Note: This resolution affects only OnBase Web Server applications. Other, third-party Web sites that display Excel documents in iframes are not affected, and the issue will persist for those sites.

Changing the Order of Document Access

Users can avoid this behavior by changing the order in which they access Excel documents. The issue does not occur when the Excel documents are opened in the OnBase Web Client before other Excel documents are opened in another application. Users can work with Excel documents in both the Web Client and another application if the documents are opened in the Web Client first.

Users Cannot Open CSV Files in Excel

To let users open .csv file formats in the Web Client using Microsoft Excel, ensure that the file format is configured as follows:

Option	Value
Viewer Type	Custom
Command Line for Custom Viewer	excel.exe
MIME Type	application/vnd.ms-excel
Default Extension	CSV

MHTML Documents Cannot Be Opened

When a Web Client user attempts to open an MHTML (.MHT) document using Firefox or Safari, the document does not load, and the user is prompted to open a Web Client ASHX file.

Only Internet Explorer allows MHTML documents to be opened from the Web Client. Firefox and Safari do not natively support MHTML documents.

Folders: Internet Explorer Is Unresponsive

In the OnBase Web Client, opening or searching a file cabinet containing a large number of folders may cause Internet Explorer to become unresponsive. The recommended child folder display option for a file cabinet or Folder Type containing a large number of folders is **Only Display Child Folders from Search**. When users select the file cabinet or folder, they will be prompted to search for folders by Folder Type and Keyword values.

Displaying child folders from folder search can greatly improve folder retrieval time, provided that users know information about the folder they are searching for, such as Folder Type and Keyword values.

For more information about configuring folders, see the Configuration module Help.

Web Client Won't Load—Server Application Unavailable

The Web Client may not load if the account running the ASP.NET worker process is locked. This account is typically named ASPNET. When the ASPNET user is locked, the following errors are displayed in the Windows Event Viewer:

- aspnet_wp.exe could not be started. The error code for this failure is 800700CB. This error can be caused when the worker process account has insufficient rights to read the .NET Framework files. Please ensure that the .NET Framework is correctly installed and that the ACLs on the installation directory allow access to the configured account.
- aspnet_wp.exe could not be launched because the user name and/or password supplied in the processModel section of the .config file are invalid.

Users attempting to log on to the Web Client may be presented with the message, **Server Application Unavailable**.

If the Web Client will not load because the ASPNET user is locked, you can unlock the user in Computer Management.

1. To open Computer Management, select **Start | Run**. In the **Run** dialog box, type **compmgmt.msc** and click **OK**. Computer Management is displayed.
2. In the left pane, navigate to **System Tools | Local Users and Groups | Users**. The right pane displays a list of users.
3. Right-click the ASPNET user and select **Properties**.
4. Clear the **Account is locked out** check box and click **OK**.
5. If impersonation is used, ensure that the impersonation credentials are correct in the Web.config file of the Application Server or Web Server. See [Enabling Impersonation on page 52](#).

Characters Are Cut Off in Text Documents

Users may notice that text documents viewed from the OnBase Web Client display a different number of characters per line than those viewed from the OnBase Client. This inconsistency occurs because text documents are rendered as images in the Web Client. In the OnBase Client, text documents are rendered as text.

In the Web Client, the number of characters displayed per line is controlled by the **Characters per line** setting for the Document Type. For example, if the **Characters per line** setting is 132, only characters in columns 1–132 are displayed for documents in the Web Client. Characters in columns 133+ are not displayed.

In the OnBase Client, the number of characters displayed per line depends on the width of the document viewer. The **Characters per line** setting controls how narrow the viewer must be before the horizontal scroll bar is displayed. For example, if the **Characters per line** setting is 132, the horizontal scroll bar is displayed only when width of the viewer accommodates 132 characters or fewer. If the width of the viewer accommodates more than 132 characters, the horizontal scroll bar is not displayed, and the characters that do not fit in the viewer appear to be cut off.

The **Characters per line** setting is accessed by clicking **View/Print** from the **Document Types** dialog box in OnBase Configuration. Before configuring this setting for a Document Type, consider whether the Document Type will contain text documents and how users will access these documents.

External Text Search: Documents Not Opened to Correct Page

When users open external text search results from the OnBase Web Client, they may be taken to the first page of the document, even though they clicked a different page number from the hit list.

This behavior occurs when the image rendition of a document has a different number of pages than the text rendition, and the Document Type is not configured to display the text rendition by default for external text searches.

Image and text renditions often have a different number of pages when the image rendition contains graphics or white space. Because these elements are not included in text renditions, the page breaks between the text and image renditions do not align.

Alternative Options

To avoid this behavior, configure the Document Type to display the text rendition by default when the document is retrieved using external text search. See the OnBase Configuration help files for information about the **Use Text Display Format For External Text Search Results** option.

Another option is to increase or decrease the number of lines per page for text renditions so that they more closely align with the lines per page on the image rendition. See the OnBase Configuration help files for information about the **Lines per page** setting.

Print Formats Aren't Available in the HTML Web Client

When users print documents in the HTML Web Client using the **Print** button or right-click option, OnBase printing features, such as print formats, are not available.

To access OnBase printing features in the HTML Web Client, users should print documents using the **Send To | Server Print Queue** right-click option. This option displays the following dialog box, which allows users to take advantage of additional print options.

Notes Configured to “Never Print” Are Printed

In some cases, documents printed from the Web Client may display notes whose Notes Types are configured to never print.

HTML documents and E-Forms printed from the Web Client viewer will display any notes that are open on the document, even if the notes are configured to never print. This behavior occurs because HTML-based documents printed using the viewer's right-click **Print** option will use Internet Explorer's **Print** dialog box rather than the OnBase **Print** dialog box.

To ensure note attributes are respected, have users print HTML-based documents using the Document Search Results list's right-click **Print** option.

Notes Configured to Print After a Document are Printed Before

In some cases, documents containing notes that are configured to print after a document may print the notes before the document. This occurs with PDF documents, and can also occur when users select the **Note Text After Document** option during printing. The problem occurs due to an issue with the timing of the program used to display the PDF document. OnBase will attempt to print the note text after the document, however, note text may be printed before the document.

Document Printing Differs Between Core and OnBase Client

Issue: Text documents printed from Core Services applications like the OnBase Web Client may not line up exactly with documents printed from the OnBase Client. This behavior occurs because text documents printed from the Web Client are rendered as images before being printed.

Resolution: To make text documents print consistently between the Web Client and the OnBase Client, create a blank overlay, and then configure the Document Type to always use the overlay when text documents are printed. This overlay ensures that the text documents are rendered as images when printed from either the Web Client or the OnBase Client. The resulting printouts then match between the OnBase applications. If the text documents already have an overlay configured, then the overlay may need to be altered to accommodate printing in both clients.

Color Documents Do Not Print in Black and White

In the ActiveX Web Client, it is possible for color documents to print in color, even when users select the **Black & White** print option in the Print dialog box. This is caused by the individual print drivers for various physical printers. If a printer is currently configured to print documents in color and users choose the **Black & White** print option when printing in the Web Client, OnBase will attempt to override the printer's default print color setting. Not all printer drivers will allow OnBase to override the default print setting.

As a workaround for this issue, adjust the printer's default print color setting to print in grayscale or black and white.

Document Handle Search Results Differ Between Core and OnBase Client

Document handle searches in Core Services applications, such as the Web Client, may return fewer documents than they do in the OnBase Client. This inconsistency occurs because the OnBase Core does not retrieve documents belonging to Document Types that you lack privileges to view or that are restricted based on Security Keywords.

Document handle searches in the OnBase Client let you retrieve all documents regardless of Document Type privileges and Security Keyword constraints, but you cannot open or view information about restricted documents other than their Document Types.

For example, if a document handle search in the OnBase Client retrieves a document that you lack privileges to view, the OnBase Client displays the document in a results list in the following format: **(Restricted): [Document Type Name]**. The same search in the OnBase Web Client would display the message **No Documents Found**.

Keyword Issues

Document Dates and Date Keywords Prior to 1/1/1753

SQL databases do not store date Keyword values or document dates prior to 1/1/1753. This is a known limitation of SQL databases.

To preserve data integrity, the OnBase Web Client will display an error if a user tries to save dates prior to 1753 on a SQL database.

The ActiveX Web Client may display one of the following errors:

- The conversion of a datetime2 data type to a datetime data type resulted in an out-of-range value. The statement has been terminated.
- An Error occurred while parsing a keyword value for Keyword Type [name] (ID #), check the inner exception for details.
- There was an error re-indexing the document.
- The following keyword input contains an invalid value: [keyword name]. Please enter a date in the format MM/dd/yyyy.
- The following keyword values are invalid: [keyword name]

The HTML Web Client may display one of the following errors:

- There was an error while performing the requested action.
- There was an error re-indexing the document.
- The following keyword input contains an invalid value: [keyword name]. Please enter a date in the format MM/dd/yyyy.

E-Forms & HTML Content Don't Render Correctly

E-Forms and HTML content must be written in a way that will work properly in Standards mode for all browsers that the customer wants to support.

If possible, address the HTML content's compatibility issues by following the guidelines available at the following location in the Microsoft Developer Network (MSDN®) library:

- Internet Explorer 11 Compatibility Cookbook:
[https://msdn.microsoft.com/en-us/library/bg182625\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/bg182625(v=vs.85).aspx)

Saving E-Forms

When a user modifies an E-Form in the OnBase Web Client, the user must click a submit button in order for the changes to be saved.

Printing E-Forms

Printing is not working correctly for E-Forms with tabs in the Web Client. If a user selects a tab other than the default, then right clicks and prints, when the Internet Explorer print dialog box opens, the E-Form refreshes, and the default tab is selected. If the user chooses the print button, the default tab is printed. The user must then select the tab they would like printed again.

Error Messages and Errors

Access to the path "C:\inetpub\wwwroot\appnet\temp\icons" is denied

This configuration issue occurs when the account that is running the Web Server's application pool has insufficient rights to create/delete files or folders on the server. As a result, an exception is thrown when the account tries to create or delete the "appnet\temp\icons" folder.

To address this issue, do one of the following:

- In the Web Server's Web.config, enable identity impersonation using an account with the **Modify** NTFS permission to the AppNet directory.
- Give the account that is running the Web Server's application pool the **Modify** NTFS permission to all folders and subfolders in the AppNet directory.

Note: For the purpose of this example, the path C:\inetpub\wwwroot\appnet\temp\icons is used. The path in the error message may vary depending on your installation.

Another session is currently active

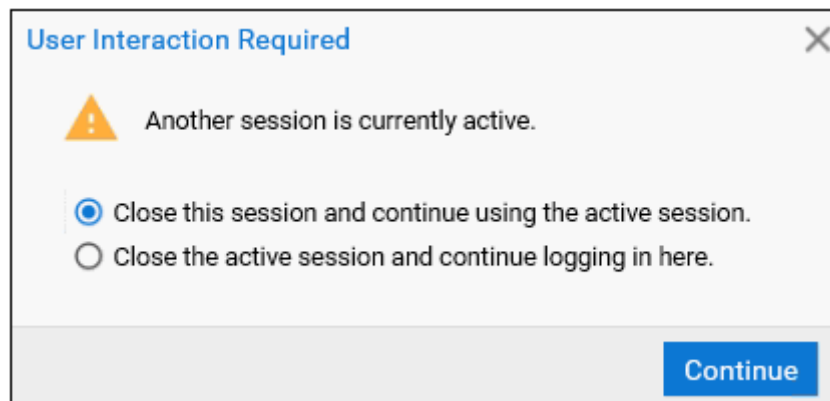
When a user accesses the Web Client while logged on to DocPop or FolderPop, the following message may be displayed:

- Another session is currently active.

The user can choose from the following options:

- **Close this session and continue using the active session.** This stops the Web Client from loading and leaves the DocPop/FolderPop session open.
- **Close the active session and continue logging in here.** This closes the DocPop/FolderPop session and continues loading the Web Client with a new session.

Note: This option is not available in Firefox or Chrome. In these browsers, you can only continue using the active session.



This behavior occurs because the Web Client detects the active DocPop session and prevents the user from logging on to OnBase multiple times. In Internet Explorer, this behavior can be avoided by doing the following:

- In Internet Explorer, log on to DocPop and the Web Client using separate browser sessions.

Authentication failed. Please check the configuration settings.

This message may be displayed on the login screen for several reasons, such as an invalid setting in the Web Server's Web.config or an outdated database schema. To protect sensitive information from being displayed to the end user, the login screen does not describe the error's cause in detail. Use the OnBase Diagnostics Console to pinpoint the issue and make the necessary modifications. Several messages logged by the Diagnostics Console are covered in this Troubleshooting section.

Cannot create channel sink to connect to URL

When users access the Web Client, the following error may be logged to the Diagnostics Console:

- Cannot create channel sink to connect to URL ". An appropriate channel has probably not been registered.

On the login page, the following error is displayed:

- The server encountered an error when connecting to the database. If this problem persists, you should contact your administrator for resolution.

These errors occur when the URL to the Application Server is blank or incorrect in the AppNet (Web Server) Web.config file. The correct value will depend on the communication method used: Remoting or SOAP.

Remoting allows the Web Server to use binary over HTTP to communicate with the Application Server. If the **ServiceClientType** attribute in Web.config is set to **Remoting**, then the **ApplicationServer URL** should be set to **http://ServerName/AppServer/service.rem**.

SOAP allows the Web Server to use XML SOAP over HTTP to communicate with the Application Server. If the **ServiceClientType** attribute in Web.config is set to **SOAP**, then the **ApplicationServer URL** should be set to **http://ServerName/AppServer/service.asmx**.

Client found response content type of 'text/plain; charset=utf-8'

When users access the Web Client, the following error may be logged to the Diagnostics Console:

- Client found response content type of 'text/plain; charset=utf-8', but expected 'text/xml'. The request failed with the error message...

On the login page, the following error is displayed:

- The server encountered an error when connecting to the database. If this problem persists, you should contact your administrator for resolution.

These errors occur when the Web Server is configured to communicate with the Application Server using SOAP, but the Web Server's **ApplicationServer Url** setting in Web.config is incorrect.

In the Web Server's Web.config, when the **ServiceClientType** setting is set to **SOAP**, the **Url** in the same element must point to **service.asmx** rather than **service.rem**, which is the default setting.

To resolve this issue, change the extension from **.rem** to **.asmx** for the **Url** value. For more information about SOAP and remoting, see [Configuring Service Client Settings on page 51](#).

Content length too large

When users attempt to upload large files, the following error may be displayed:

- HTTP Error 404.13 - CONTENT_LENGTH_TOO_LARGE

This error may be displayed in an IIS environment when users attempt to upload files that exceed the value configured for the **maxAllowedContentLength** setting in the Web.config files of the Web and Application Servers. This setting is provided in bytes, and it is commented out by default. For steps to update the setting in both the Web and Application Servers' Web.config files, see [maxAllowedContentLength on page 260](#).

Could not create Windows user token

The following error may be displayed when users attempt to log on to the Web Client:

- Server error in '/VirtualDirectoryName' Application.

Configuration Error

Description: An error occurred during the processing of a configuration file required to service this request. Please review the specific error details below and modify your configuration appropriately.

Parser Error Message: Could not create Windows user token from the credentials specified in the config file. Error from the operating system 'Logon failure: unknown user name or bad password.'

This error is displayed if the Web Server is configured to use impersonation and the impersonated identity account's credentials are either invalid or not configured properly. This issue may occur when a Web Server that uses impersonation is moved to a different domain.

Impersonation is enabled in the Web Server's Web.config file by removing the comment tags (<!-- and -->) that enclose the following element.

```
<identity impersonate="true"
userName="registry:HKLM\SOFTWARE\Wow6432Node\Hyland\YOUR_APP\Identity\
ASPNET_SETREG,userName"
password="registry:HKLM\SOFTWARE\Wow6432Node\Hyland\YOUR_APP\Identity\
ASPNET_SETREG,password"/>
```

The impersonated identity account's domain user name and password are encrypted in the registry using the aspnet_setreg.exe utility provided in the **..\utilities\misc** subdirectory in the build distribution package. These registry entries are referenced by the **userName** and **password** parameters in the element above.

To resolve the issue, ensure the **userName** and **password** parameters point to the correct registry locations and are delimited by quotation marks. If necessary, re-encrypt the impersonated identity account's credentials using aspnet_setreg.exe, as described under [Enabling Impersonation on page 52](#).

Caution: Modify the registry at your own risk. Incorrectly editing the Windows registry can cause serious problems that may require you to reinstall your operating system. Be sure to back up the registry before making any changes to it. For more registry information, see the following Microsoft articles: <http://support.microsoft.com/kb/256986> and <http://technet.microsoft.com/en-us/library/cc725612.aspx>

Could not get database driver information for data source

When users access the Web Client, the following errors may be logged to the Diagnostics Console:

- Could not get database driver information for data source 'data source name'
- Failure on login. Invalid datasource.

On the login page, the following error is displayed:

- The server encountered an error when connecting to the database. If this problem persists, you should contact your administrator for resolution.

These errors occur when the data source name has been incorrectly specified in the Web Server's web.config file. Update the web.config file with the correct data source name.

The data that you have requested is currently off line

When a user opens a document, the following error may be displayed in the document viewer:

- The data that you have requested is currently off line. It can be retrieved by mounting the following disk:

Disk Group#: 102

Volume#: 1

This message is displayed when the platter for a document cannot be reached. The following errors also may be logged to the **Errors** tab of Diagnostics Console:

- FindInIdFile error: \\UNCshare\DiskGroup\OnBase.ID : [#FindInIdFile Factory:Get failed: "Id file is inaccessible"]
- Document file not found on disk group volume [102:[102:1] - \V1\0\107.tif

These errors could mean the following:

1. The platter has been detached from OnBase, as might be the case with network storage.
2. The platter is configured with an invalid UNC path.
3. The Application Server account accessing the Disk Groups has insufficient permissions.

If you suspect the account accessing the Disk Groups has insufficient permissions, perform one of the following tasks, depending on whether impersonation is enabled.

If impersonation is ENABLED

Grant the Application Server's impersonation account **Read/Modify** NTFS and **Change** share permissions to the Disk Group directory location.

If impersonation is DISABLED

Grant the account running the Application Server's application pool **Read/Modify** NTFS and **Change** share permissions to the Disk Group directory location.

Error occurred Sharing Envelope

When a user attempts to share an envelope with a large number of users, the following error may be displayed:

- Error occurred Sharing Envelope

This error may be displayed because the request timed out due to the large number of users. The **executionTimeout** value in the Web Server's Web.config file may need to be increased to allow for this operation to succeed. For more information, see [httpRuntime on page 259](#).

Failed to create object element for control

When users attempt to log on to the ActiveX Web Client, the following error may be displayed:

- Failed to create object element for control: There is no cache to operate on.

This error may be displayed if the ActiveX controls are not properly installed. To resolve this issue, install the Web ActiveX controls on the client workstation using the Hyland Client Side Components installer. Be sure to remove all previous versions of the ActiveX controls from the workstation before running the installer.

Failed to find Web Server license for data source

When users access a Web application such as the Web Client or DocPop, the following error is logged to the Diagnostics Console:

- Failed to find Web Server license for data source

On the login page, the following error is displayed:

- The server encountered an error when connecting to the database. If this problem persists, you should contact your administrator for resolution.

This error is may be displayed for any of the following reasons:

- The data source is not specified in the Web Server's Web.config file.
- The data source in Web.config is incorrect.
- OnBase is not correctly licensed for the Web Server.

To resolve this issue, change the data source setting in Web Server's Web.config to the correct data source name on the Application Server. The setting you need to change depends on the module you want to access. For example, the Web Client uses the **dmsDataSource** setting located under **appSettings**, and DocPop uses the **datasource** setting located under **Hyland.Web.DocPop**.

If you suspect the issue is due to a licensing issue, contact your first line of support.

Failed to get session for session id

When users are working in the OnBase Web Client or another OnBase Web application like DocPop, the application may become unresponsive. The OnBase Event Log records the "Application End" and "Application Start" events, which are followed by a series of errors. The Diagnostics Console logs the following error message

- Failed to get session for session id.

The Web Client also may display either of the following messages:

- Message: Required property: SessionID is unavailable.
- Error processing request.

Modifying the contents of the Web Server or Application Server's virtual directory will cause these applications to restart. When this occurs, connected users will lose their sessions and their applications will become unresponsive. This behavior occurs because the OnBase Web Server and Application Server are ASP.NET Web Applications. ASP.NET detects file changes, including changes to file system attributes and time stamps, and restarts the application if a change is detected. You can view the shut down message of the "Application End" event in the OnBase Event Log to determine why the application stopped. (For example, the virtual directory contents or Web.config settings have been changed.)

Unintended application restarts can occur when virus scanning software, backup software, or indexing services access the contents of an application's virtual directory. These processes don't modify the contents of an application's files, but they can modify the files' attributes, which is enough for ASP.NET to restart the application. To properly configure virus scanning, backup software, or indexing service software, follow these guidelines:

- Exclude both the OnBase Web Server's and Application Server's virtual directories and the ASP.NET Temporary Files directory from antivirus, backup, or indexing service scanning. The ASP.NET Temporary Files directory is below:
 - 32-bit installations:
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Temporary ASP.NET Files
 - 64-bit installations:
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files
- If these files are scanned by antivirus, backup, or indexing software, IIS will restart the application pool for the OnBase application. When an application pool restarts, all existing OnBase sessions are reset, causing errors for connected users.
- Real-time scanning of script execution, which is available in some antivirus software, should only be engaged according to the software manufacturer's instructions. Some manufacturers do not intend this functionality to be used on servers.

Consult your antivirus, backup, or indexing service software's documentation for other recommended settings for Web servers. Ensure that any virus scanning, backup or indexing service changes will not be overwritten by the automatic policy settings configured for your network.

The Microsoft Knowledge Base describes this issue in greater detail. For more information, refer to the following articles:

- <http://support.microsoft.com/kb/821438>
- <http://support.microsoft.com/kb/312592/en-us?spid=8940&sid=global>
- <http://support.microsoft.com/kb/316148/EN-US/>

Failed to load Popup Blocker Assistant ActiveX control

When users attempt to access the Web Client's login page, the following error may be displayed:

- Failed to load Popup Blocker Assistant ActiveX control.

The Popup Blocker Assistant ActiveX control may fail to load under the following conditions:

- The Web Client's virtual directory cannot be found.
- The user clicked **Don't Install** when prompted to install the ActiveX control.
- An HTTPS connection is enabled, but content expiration has not been set to 1 hour on the **AppNet\activex** directory.
- The requirements for the Popup Blocker Assistant ActiveX control are not met. For example, the client workstation may not allow ActiveX controls to be downloaded.

For information about this ActiveX control's function and requirements, see [Pop-up Blockers on page 11](#).

Failed to receive valid XML Response from Server

When a user attempts to retrieve documents in the ActiveX Web Client, the message **No documents found** is displayed, followed by an ActiveX error message similar to the following:

- [ERROR] Module: PresentationServices,
Class: COBElementResultsSvc,
Method: COBElementResultsSvc::GetNext,
Message: Caught service exception: Failed to receive valid XML Response from Server. Response was: '↵' - Error Code:

In addition, **SOAP** is specified as the **ServiceClientType** in the Web Server's web.config.

This problem may occur for multiple reasons. One possible cause is the installation of Dynamic Content Compression on the OnBase Application Server. Dynamic Content Compression is a feature of the Performance Role Service within IIS. This feature is not necessary and should not be installed on the OnBase Application Server, because it interferes with the XML that is sent between the Application Server and the Web Server.

File or directory not found

The **File or directory not found** error message may be displayed for multiple reasons, as described in the following topics:

- [Login Page Error](#)
- [Importing Documents Error](#)

Login Page Error

When users attempt to access the Web Client's login page, the following error may be displayed:

- The page cannot be found.
- ...
- HTTP Error 404 - File or directory not found.

This error indicates that the Web Server virtual directory cannot be found. To address this error, perform the following tasks:

1. In the Web Server's Web.config file, ensure the **dmsVirtualRoot** value points to the correct server and virtual directory.
2. In Internet Information Services Manager, ensure the Web Service Extensions display the appropriate ASP.NET extensions as **Allowed**.

Importing Documents Error

When users attempt to import a document using the Web Client, the following error may be displayed in the Navigation Panel:

Server Error
404 - File or directory not found.
The resource you are looking for might have been removed, had its name changed, or is temporarily unavailable.

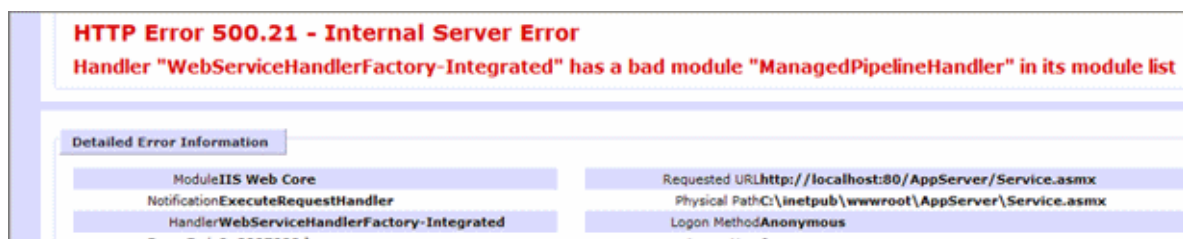
The Web Client displays this error when the **maxAllowedContentLength** setting in the Web Server's Web.config is not large enough.

For information about configuring this setting, see [maxAllowedContentLength on page 260](#).

Handler "PageHandlerFactory-Integrated" has a bad module

When you attempt to access the Application Server's service page or the Web Client login page, one of the following errors may be displayed:

- HTTP 500.21 - Internal Server Error Handler "PageHandlerFactory-Integrated" has a bad module "ManagedPipelineHandler" in its module list
- HTTP 500.21 - Internal Server Error Handler "WebServiceHandlerFactory-Integrated" has a bad module "ManagedPipelineHandler" in its module list



This issue may occur under either of the following conditions:

- The required version of Microsoft .NET Framework is not installed, or
- The .NET Framework was installed prior to the installation of Internet Information Services (IIS).

To address this issue, perform the following steps on the Web Server and Application Server:

1. Ensure the required version(s) of Microsoft .NET Framework are installed on the Web Server and Application Server.
2. Open a command prompt. (Depending on the operating system, it may be necessary to run command prompt with the **Run As Administrator** option.)
3. Run the following command:
C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -i
4. Verify that the web page originally throwing the error now loads successfully.
It is not necessary to reset IIS or recycle any application pools during the course of these troubleshooting steps.

Input stream is not a valid binary format

When users attempt to log on to the Web Client, either of the following errors may be logged to the Diagnostics Console.

- Input stream is not a valid binary format.
- <title>Could not load file or assembly 'System.Web.Extensions'...</title>

The first error is displayed if the Web Server is using **remoting** as its **ServiceClientType**. The second error is displayed if the Web Server is using **SOAP**.

On the login page, the following error is displayed:

- The server encountered an error when logging in. If this problem persists, you should contact your administrator for resolution.

Similar errors are captured when users attempt to access the service.asmx page of the Application Server.

This issue may occur for several reasons.

1. This issue may occur because the home directory at the Web site level has the option **A directory located on this computer** selected with the **Local path** pointing to a virtual directory (e.g., **C:\DMS\AppNet**). Because the Web Server and Application Server reside in two separate virtual directories, a virtual directory cannot be specified as the home directory at the Web site level. The Web site level home directory should point to the root rather than a specific virtual directory.
To allow users accessing the Web site to go directly to the OnBase login page without having to specify the virtual directory, use redirection. For information about redirection, refer to the Microsoft® TechNet Web site.
2. The Application Server may be unavailable. Ensure that the Application Server's application pool is running. Then ensure that the Web Server is properly configured to communicate with the Application Server using remoting or SOAP. To do so, see [Configuring Service Client Settings on page 51](#).

3. This issue may also occur if the Application Server's Web.config file has been directly modified to include an error, such as a duplicate **section** element. Contact your solution provider for help resolving this issue.
4. A **bin** directory for a given application contains an invalid file. Remove any unnecessary files from the **bin** directory and recycle the application pool. Duplicate files should not exist in the **bin** directory even if one has been renamed (e.g., **Hyland.Core.dll** and **Hyland.Core.dllold** should not exist in the same directory).
5. There may be an issue with the DNS settings or the host name on the server. If there are issues with DNS settings on a server, a temporary workaround is to change the Web Server's Web.config file to point to the IP address. The host name cannot contain an underscore character (_). If the server's machine name contains an underscore character, use its IP address instead, or change the machine name. For information about valid host names, see <http://support.microsoft.com/kb/101785>.
6. There may be an issue with the security login accounts in the OnBase database. Contact your first line of support if you believe this to be the issue.
7. The account running the application pools may not have the appropriate permissions. Grant the application pool's identity account **Read** permissions as described under [Enabling Impersonation on page 52](#).
8. There may be an issue with the impersonation account configured on the Web Server. Verify that the impersonation account has not expired and that the password has not changed. Verify that the **impersonate** attribute is appropriately set in the Web.config files for the Web Server and Application Server.

Input string was not in a correct format

When users attempt to either log on to the Web Client or submit a form using LoginFormProc, the following error may be logged to the Diagnostics Console:

- Input string was not in a correct format.

On the login page, the following error is displayed:

- An unknown error occurred.

If this error is displayed when a user attempts to submit an HTML form using LoginFormProc, then the Document Type number may not be specified correctly in the OBDocumentType field on the form. Check the HTML form and ensure that the Document Type's number is specified as the OBDocumentType value, not the Document Type's name.

If this error is displayed when a user attempts to log on to the Web Client, this issue may be due to a version mismatch between OnBase Core Services and the ActiveX controls on the client workstation. To remove the older ActiveX controls, perform the following steps.

1. From the client workstation, use Windows Explorer to navigate to C:\WINDOWS\system32. This is the default location where ActiveX controls are installed.
2. Search all files and folders for **OBX**.
3. Display the **Product Version** column. You can display the column by right-clicking a column header and selecting **More**. Then, select **Product Version** and click **OK**.

4. Delete any OBX files whose product version does not match the current version of Core Services.
5. Re-launch the Web Client login page.

Is not a valid Win32 application

When a user attempts to log on to the Web Client after a Web Server installation, the following message may be displayed:

- Server Error in '/AppNet' Application
is not a valid Win32 application. (Exception from HRESULT: 0x800700C1)

This error occurs when the Web Server (a 32-bit application) attempts to run under the 64-bit version of the Microsoft .NET Framework. To resolve this issue, perform the steps under [Post-Installation on page 199](#).

For more information about running the Web Server in a 64-bit environment, see [Installing Servers in a 64-Bit Environment on page 199](#).

Keyword does not validate as masked or unmasked

When a Web Client user attempts to index, re-index, or modify Keyword values on a document, the following error may be logged to the Diagnostics Console:

- Keyword [value] does not validate as masked or unmasked.

Depending on the task the user was performing, the user may be presented with one of the following errors:

- Upload failed.
- An Error occurred while parsing a keyword value, check the inner exception for details.
- There was an error re-indexing the document.

This issue occurs when a user attempts to index a document with a masked Keyword value, and the mask contains leading blank spaces. In the OnBase Core, Keyword values cannot be stored with leading spaces. To address this issue, remove the leading spaces from the Keyword Type's mask.

ODBC SQL Server Driver: Communication link failure

On Windows Servers, the following errors may be logged in the Diagnostics Console when OnBase applications access SQL Server:

- [Microsoft][ODBC SQL Server Driver][DBNETLIB] General Network error. Check your network documentation
- ERROR [08S01] [Microsoft][SQL Native Client]Communication link failure
- System.Data.SqlClient.SqlException: A transport-level error has occurred when sending the request to the server. (provider: TCP Provider, error: 0 - An existing connection was forcibly closed by the remote host.)

Users working in the Web Client may receive an "Error processing request" message when these errors are logged.

These errors occur because the TCP Chimney Offload feature of the Scalable Networking Pack is enabled on the database server. This feature may cause problems when used with some network adapters. For more information about the error's cause as well possible solutions, refer to the following Microsoft Knowledge Base articles:

- <http://support.microsoft.com/kb/942861/en-us>
- <http://support.microsoft.com/kb/945977/en-us>

Please verify size of image has not exceeded the maximum size limit

This message is displayed in the Web Client when a user attempts to import a file whose size exceeds the maximum size configured in the Web Server's Web.config. The default limit is 4096 KB. For information about changing the limit, see [httpRuntime on page 259](#).

The remote server returned an error. (404) Not Found.

This message may be logged when a user attempts to import a large file. The OnBase Web Server logs this error when the Application Server's **maxAllowedContentLength** and **maxRequestLength** Web.config values are not large enough to accommodate the file's request size.

Note that the request size is larger than the file size. When a file is sent from the Web Server to the Application Server, the request size increases due to encoding. The increase amount varies depending on whether the Web Server is using SOAP to communicate with the Application Server. Requests sent using SOAP are larger than requests sent using remoting.

For more information about **maxRequestLength** and **maxAllowedContentLength**, see [httpRuntime on page 259](#) and [maxAllowedContentLength on page 260](#).

The requested page cannot be accessed

When a user attempts to access the OnBase Web Client, the following error may be displayed:

- HTTP Error 500.19
The requested page cannot be accessed because the related configuration data for the page is invalid.

This error may be displayed because the Web Server is installed on a 64-bit machine with Dynamic Content Compression enabled. Because Dynamic Content Compression interferes with the XML sent between the Application Server and the Web Server, it must not be enabled on either server.

The OnBase Web Server and Application Server must not be installed on the same server as Windows Server Update Services (WSUS), which enables Dynamic Content Compression during its installation.

- See [Notes on Dedicated Web Server Hardware on page 27](#) for information about dedicated server requirements.
- For a list of Role Services allowed on the Web Server and Application Server, see [Installation Order on page 231](#).

Requested registry access is not allowed

When a user attempts to log on to the Web Client, the following error may be displayed:

- **Security Exception**
Description: The application attempted to perform an operation not allowed by the security policy. To grant this application the required permission please contact your system administrator or change the application's trust level in the configuration file.
Exception Details: System.Security.SecurityException: Requested registry access is not allowed.

This error is displayed when the Web Server doesn't have sufficient permissions to the **Eventlog** registry key.

Caution: Modify the registry at your own risk. Incorrectly editing the Windows registry can cause serious problems that may require you to reinstall your operating system. Be sure to back up the registry before making any changes to it. For more registry information, see the following Microsoft articles: <http://support.microsoft.com/kb/256986> and <http://technet.microsoft.com/en-us/library/cc725612.aspx>

To assign appropriate permissions, perform the following steps on the server machine:

1. Select **Start | Run**.
2. Type **regedt32** and click **OK**.
3. Navigate to **HKLM | System | CurrentControlSet | Services | Eventlog**.
4. Right-click the **Eventlog** key and select **Permissions**.
5. Click **Add**.
6. Add the .NET process account (the application pool's identity account).
7. With the process account selected, select **Full Control**.
8. Click **OK**.

Request timed out

After users attempt to view or upload very large documents, the attempt fails and the following message is logged to the Diagnostics Console:

- Request timed out

This message is displayed when the requested action (such as uploading or downloading a document) takes longer than the configured execution timeout.

The execution timeout specifies the number of seconds the application has to execute a request before the request times out. Depending on your network architecture, you may need to increase the execution timeout at one of the following levels:

- Application Server
- Web Server
- Gateway Caching Server

If users' requests are passing through more than one of these applications, start with the application that has the lowest execution timeout. To increase the execution timeout:

1. Open the application's Web.config file.
2. Locate the **executionTimeout** setting.

Note: The Gateway Caching Server's Web.config file does not contain an **executionTimeout** setting. As a result, it uses the default ASP.NET execution timeout of 110 seconds. Add **<httpRuntime executionTimeout="110"/>** on a new line directly above the **</configuration>** tag in the Gateway Caching Server's Web.config file, and modify the value accordingly.

3. Specify (in seconds) how long the server should allow a request to be executed. Keep in mind this value controls how long the server is allowed process a user's request. If the server cannot execute the user's request within the period allowed, the user will have to wait the entire duration of the **executionTimeout** before an error is logged.

Note: If you intend to export PCL documents to PDF, the executionTimeout value must be set to 86000. This allows an export to succeed without timing out.

4. Save the Web.config file.
5. Test whether the issue is resolved. If it is not, then repeat these steps as needed until the **executionTimeout** is large enough for the request to be executed. You may need to perform these steps for more than one server application.

Tip: For assistance troubleshooting timeout issues, contact your first line of support.

The server encountered an error when logging in

This error is discussed in a different topic. See [Input stream is not a valid binary format on page 184](#).

This page is asking you to confirm that you want to leave - data you have entered may not be saved.

When users are interacting with notes on a document in the HTML Web Client while using Firefox ESR 31, they may be prompted by the following message when trying to close the window:

This page is asking you to confirm that you want to leave - data you have entered may not be saved.

This message will display under the following set of circumstances:

- A user accesses the HTML Web Client using Firefox ESR 31.
- A user opens a document from a document search results list.
- The user adds or moves a note that is displayed on the document.
- The user closes the window containing the document.

After users attempt to close the window, they are presented with the option to **Leave Page** or **Stay on Page**. Regardless of the option that a user selects, the note data and location on the document are still saved.

When users click **Leave Page**, the window containing the document is closed. The user can verify that the note location and data was saved by reopening the document.

When users click **Stay on Page**, they are presented with the following message:

Prevent this page from creating additional dialogs

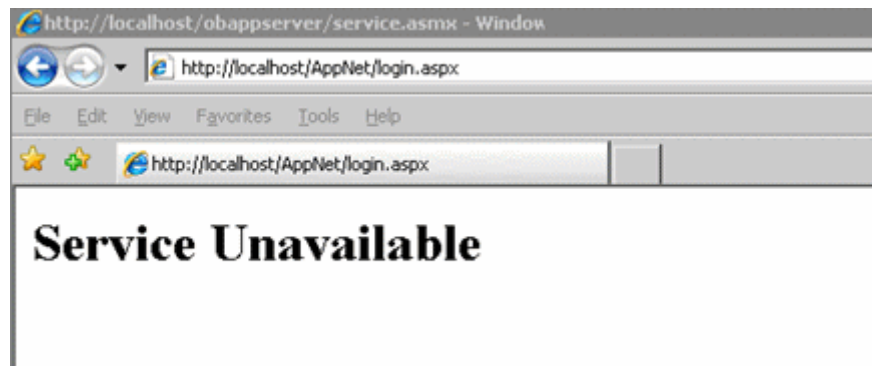
Clicking **OK** will continue closing the window. Clicking **Cancel** will display a window containing the following message:

The following issue(s) occurred and will be addressed by the system on your behalf:
Document. You have unsaved notes data.

Click **Continue** to save the note data and to continue closing the page. The user can verify that the note location and data was saved by reopening the document.

Service Unavailable

When users attempt to access the OnBase Web Client, the **Service Unavailable** message may be displayed within the browser window.



This behavior may occur for any of the following reasons:

- Cause:** The password for the identity account running the Web Server's application pool is not specified correctly, or the account's password has changed since the initial configuration.
Resolution: Update the identity account configuration with the correct user name and password.
 - Open Internet Information Services (IIS) Manager.
 - Right-click the Web Server's application pool (AppNet, by default), and select **Properties**.
 - Click the **Identity** tab.
 - Specify a valid password and click **OK**.
- Cause:** The identity account running the Web Server's application pool is locked out.
Resolution: Unlock the account.

3. **Cause:** The identity account is not a member of the IIS_WPG group on the Web Server.
Resolution: Add the identity account to the IIS_WPG group on the Web Server.
 - a. Open Windows Local Users and Groups by entering **LUSRMGR.MSC** in the Windows Run dialog box.
 - b. Under **Groups**, double-click the **IIS_WPG** group.
 - c. Click **Add**.
 - d. Choose the account that is running the Application Pool.
 - e. Click **OK**.
 - f. Click **OK** again to save changes.

System is currently locked out

When a user attempts to log on to the Web Client, the following error may be displayed:

- System is currently locked out. Please contact your system administrator.

This message indicates that the system is locked for maintenance. A system administrator must unlock the system before other users can log on. For information about system lockouts, please refer to the OnBase Configuration (Config) help files or the System Administration module reference guide.

There was an error when loading the document

When a user opens a document, the Web Client may not completely download the ActiveX controls, or the following error may be displayed:

- There was an error when loading the document

The Diagnostics Console logs the following errors:

- Failed to get property for pageData
Failed to get the pages from the service
A general error occurred.
Error 0xFFFFFFFFA9 occurred.
Failed to display the document

These errors may occur under several conditions. Refer to the following topics for troubleshooting steps.

- [Mismatched ActiveX Controls](#)
- [Color Overlays](#)

Mismatched ActiveX Controls

The errors may occur because the workstation has older versions of the ActiveX controls installed. Check the workstation for older ActiveX controls, and then delete them. New controls can be deployed either directly by the Web Client or by using the Hyland Client Side Components installer. See the Core Enterprise Installers reference guide for installation steps.

Color Overlays

If the errors are displayed for a document that uses a color overlay, decrease the color depth of the overlay. Overlays are decompressed as they are processed by the Application Server. For higher color depths, more processing is necessary to render the colors and retrieve larger files.

An overlay should not exceed an 8- to 16-bit color depth. To change the color depth, open the overlay or image with an image processor that will allow you to change the color depth to a lower setting. Refer to the processor's documentation for more information.

This document is not accessible by the current user

When a user re-indexes a document in the HTML Web Client, the following message may be displayed:

- This document is not accessible by the current user.

This message is displayed when the re-indexed document becomes restricted to the user due to Security Keywords. If a user re-indexes a Security Keyword on a document to a value prohibited to the user, the user can no longer view that document.

Unable to automatically add itself to the pop-up blocker white list

Web Client users may be presented with the following error when they access the login page:

- The application was unable to automatically add itself to the pop-up blocker white list. In order to use this application, you will either have to turn off the pop-up blocker or manually add this site to the white list.

This error is usually displayed after the user chooses to allow the Web Client to automatically add itself to the pop-up blocker's allowed sites, but it may also be displayed when the user first accesses the login page. This error is displayed when the Web Server's **WebClientType** setting is set to **activex** or **selectable**.

The error may be displayed because an unsupported pop-up blocker is enabled. For example, Firefox users may encounter the error because the Firefox pop-up blocker is enabled. The Web Client supports only the following pop-up blockers: Google Toolbar and Internet Explorer

In this case, the Popup Blocker Assistant ActiveX control cannot add the Web Server as an allowed site for pop-ups. To address this issue, either disable the pop-up blocker, or manually add the Web Server as an allowed site.

For more information, see [Pop-up Blockers on page 11](#).

Unable to complete transform of the XML document

When opening an XML document in the Web Client, users may be presented with the following error message:

- Unable to complete transform of the XML document. Please try again. If this problem persists, please contact your system administrator.

This message is displayed when users attempt to open an XML document type with an invalid style sheet. Ensure that the style sheet for that document type is configured properly.

Web Server version cannot connect to Application Server version

When users attempt to log on to the Web Client, the following error may be logged to the Diagnostics Console:

- **Web Server version [X,X,X,XXX] can not connect to Application Server version [Y,Y,Y,YYY]**

On the login page, the following error is displayed:

- The server encountered an error when connecting to the database. If this problem persists, you should contact your administrator for resolution.

This occurs when the Web Server is attempting to connect to an Application Server of a different version and service pack than the Web Server. Ensure that both the version and service pack of the Web Server match that of the Application Server it will be connecting to.

IIS and .NET Framework Errors

The following errors are caused by problems with the installation or configuration of Internet Information Services (IIS) and .NET Framework on Windows Server operating systems.

Failed to Access IIS Metabase

This message is displayed when a user attempts to log on to the Web Client. If .NET Framework is installed before IIS, the ASPNET user account may be denied required permissions to the IIS metabase.

To address this issue:

1. Open a Command Prompt.
2. Change to the following directory: **%windir%\Microsoft.NET\Framework\v4.0.30319**
3. Run the following command: **aspnet_regiis -ga aspnet**

For more information about this issue, you can access the Microsoft Knowledge Base article by following the URL displayed in the error message.

Web Page Displays Code

On Windows Server, if .NET Framework is installed before IIS, then the mappings between file types and the information the computer needs in order to handle them can be lost. Corrupt file mappings can cause a Web page to display code instead of meaningful content. If a Web page displays code, verify that the file mappings are correct for .NET. If they are not correct, completely uninstall .NET, and then re-install. The following table displays the correct file mappings, assuming .NET is installed to the default location:

Extension	Included Verbs	Script Processor
.asp	GET, HEAD, POST, TRACE	%windir%\system32\inetsrv\asp.dll

Extension	Included Verbs	Script Processor
.cer	GET, HEAD, POST, TRACE	%windir%\system32\inetsrv\asp.dll
.cdx	GET, HEAD, POST, TRACE	%windir%\system32\inetsrv\asp.dll
.asa	GET, HEAD, POST, TRACE	%windir%\system32\inetsrv\asp.dll
.idc	GET, POST	%windir%\system32\inetsrv\httpodbc.dll
.shtm	GET, POST	%windir%\system32\inetsrv\ssinc.dll
.shtml	GET, POST	%windir%\system32\inetsrv\ssinc.dll
.stm	GET, POST	%windir%\system32\inetsrv\ssinc.dll
.ashx	GET, HEAD, POST, DEBUG	%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
.asmx	GET, HEAD, POST, DEBUG	%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
.aspx	GET, HEAD, POST, DEBUG	%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
.axd	GET, HEAD, POST, DEBUG	%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
.rem	GET, HEAD, POST, DEBUG	%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
.soap	GET, HEAD, POST, DEBUG	%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
.licx	GET, HEAD, POST, DEBUG	%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
.resx	GET, HEAD, POST, DEBUG	%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
.resources	GET, HEAD, POST, DEBUG	%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll

Diagnostics Console

The Diagnostics Console is a tool that can be used to troubleshoot issues that may arise from Web Server clients, including Application Start, Application End, and DataSource Open. The Diagnostics Console works with ASP, .NET and script/API clients. Keep this utility running on the server at all times to facilitate troubleshooting.

Note: The Diagnostics Console can be used as a standalone or with the Diagnostics Service. For detailed information about configuring and using the Diagnostics Console and the Diagnostics Service, see the Diagnostics Service reference guide.

The following example displays information from the Diagnostics Console's **Error** tab when a user provides an invalid password:

Message	Module	Class	Method
Authentication Failed for user 'JOHN ADAMS' on Datasource 'DBase'.	Hyland.Core	Session	authenticate
	Hyland.Core	Session	Connect
	Hyland.Services	AppServices	Connect
	Hyland.Core.ServiceHandlers	Login	Connect
	Hyland.Core.ServiceHandlers	Login	AuthenticateStandardLogin
	Hyland.Core.ServiceHandlers	Login	Authenticate
Authentication Failed for user 'JOHN ADAMS' on Datasource 'DBase'.	Hyland.Core	Session	authenticate
	Hyland.Core	Session	Connect
	Hyland.Services	AppServices	Connect

Note: The **Severity** column displays **Trace** if the entry is the result of a trace message and **Error** if it is the result of an exception.

Method	Source File	Source Line	Severity
GetUser	.IOBSession.cpp	3976	Error
GetUser	.IOBSession.cpp	3976	Error
Connect	.IOBSession.cpp	1913	Error
Connect		0	Error

Diagnostics Console Executable Location

The Diagnostics Console and the Diagnostics Service are installed by the Core Services Enterprise installer.

- In a 32-bit environment, the executable is typically located in C:\Program Files\Hyland\Diagnostics Console.
- In a 64-bit environment, the executable is typically located in C:\Program Files (x86)\Hyland\Diagnostics Console.

Saving a Log

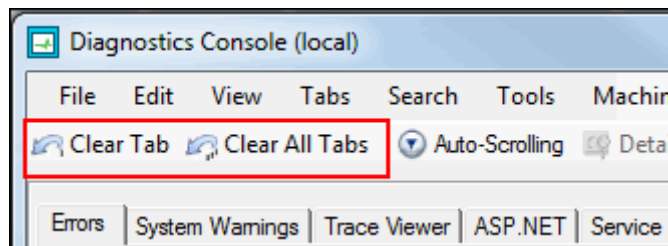
In the event that you cannot resolve the issue on your own, the logging that is produced in this tool will be very helpful to your first line of support. In some instances, you will need to save the log and send it to Technical Support. To save the log:

1. Select **File | Save As**.
2. Enter a name for the file.
3. Click **Save**.

Clearing a Log

The Diagnostics Console toolbar contains buttons for clearing data from the console.

- To clear data from the selected tab only, click the **Clear Tab** button:
- To clear data from all tabs in the Diagnostics Console at once, click the **Clear All Tabs** button:



Clicking the **Clear All Tabs** button displays a dialog box that requesting confirmation that all tabs should be cleared. Click **Yes** to clear all tabs.

Script Exceptions

The Web Server logs script exceptions to the Diagnostics Console's **Script Exceptions** tab. Script exception logging is enabled by default. For information about enabling or disabling logging, see [Hyland.Logging on page 294](#).

When script exception logging is enabled, all handled exceptions are logged. The logging of unhandled exceptions varies depending on the browser's **Disable Script Debugging in Internet Explorer** setting, which is located on the **Advanced** tab in Internet Options. When this setting is selected, both handled and unhandled exceptions are logged to the Diagnostics Console. When this setting is not selected, only handled exceptions are logged to the Diagnostics Console, and unhandled exceptions are displayed in the browser's debug dialog box.

Invalid Password Error

The following example displays information from the Diagnostics Console's **Error** tab when a user provides an invalid password:

Message	Module	Class	Method
Authentication Failed for user 'JOHN ADAMS' on Datasource 'DBase'.	Hyland.Core	Session	authenticate
	Hyland.Core	Session	Connect
	Hyland.Services	AppServices	Connect
	Hyland.Core.ServiceHandlers	Login	Connect
	Hyland.Core.ServiceHandlers	Login	AuthenticateStandardLogin
	Hyland.Core.ServiceHandlers	Login	Authenticate
Authentication Failed for user 'JOHN ADAMS' on Datasource 'DBase'.	Hyland.Core	Session	authenticate
	Hyland.Core	Session	Connect
	Hyland.Services	AppServices	Connect

Locked User Error

The following example displays information from the Diagnostics Console's **Error** tab when a user whose account is locked attempts to log on:

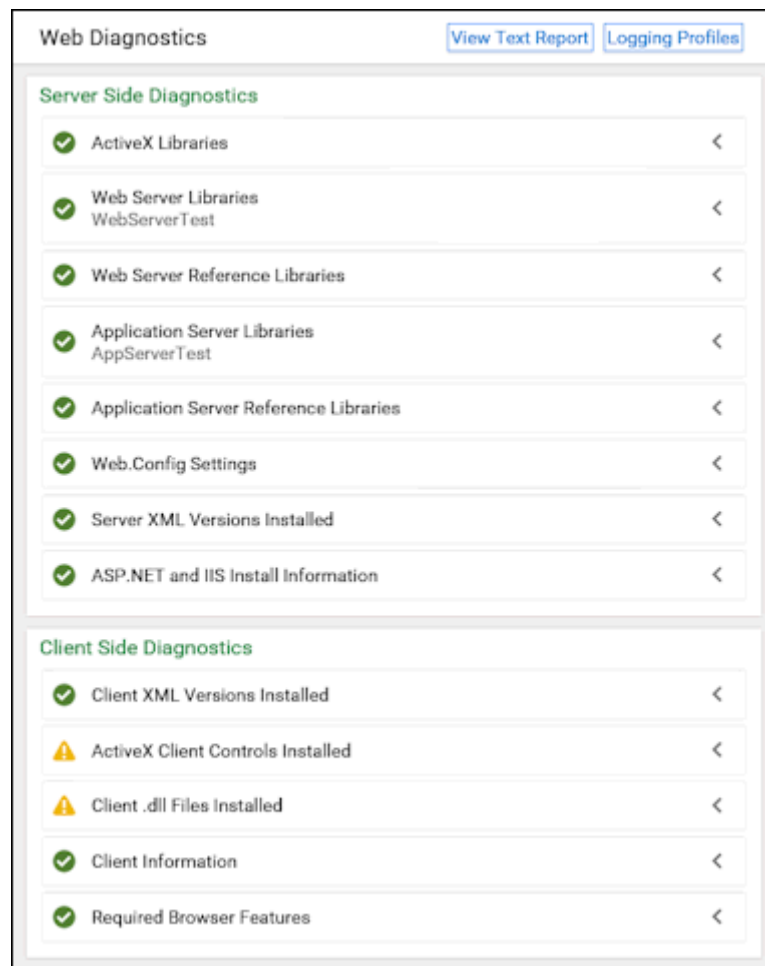
Message	Module	Class	Method
Authentication Failed for user 'JOHN ADAMS' on Datasource 'DBase'.	Hyland.Core	Session	authenticate
	Hyland.Core	Session	Connect
	Hyland.Services	AppServices	Connect
	Hyland.Core.ServiceHandlers	Login	Connect
	Hyland.Core.ServiceHandlers	Login	AuthenticateStandardLogin
	Hyland.Core.ServiceHandlers	Login	Authenticate
Failed to connect. User account 'JOHN ADAMS' is locked.	Hyland.Core	Session	authenticate
	Hyland.Core	Session	Connect
	Hyland.Services	AppServices	Connect

Mail Services Errors

The Diagnostics Console can record and display errors encountered when sending external mail or using the OnBase mail integration modules.

Web Diagnostics Page

To assist with troubleshooting, the Web Diagnostics page displays the results for a series of checks, which may be run against both the server and the client workstation used to access the page. These checks can help you diagnose and resolve configuration issues. If necessary, results can be emailed to a Technical Support Representative for additional assistance.



See the following topics:

- [Required Rights for Accessing Web Diagnostics on page 199](#)
- [IE Security Requirements on page 199](#)
- [Accessing the Web Diagnostics Page on page 199](#)
- [Diagnostics Status Symbols on page 202](#)
- [Diagnostics Categories on page 203](#)

- [Changing Logging Profiles on page 205](#)
- [Viewing a Diagnostics Text Report on page 207](#)
- [Diagnostics Using trace.axd on page 207](#)

Required Rights for Accessing Web Diagnostics

The following table outlines the product rights required for viewing Web Diagnostics page components.

Web Diagnostics Component	Required Rights
Server Side Diagnostics	Web Client Product Right Web Server Product Right
Client Side Diagnostics	Web Client Product Right
Logging Profiles	Web Client Product Right Web Server Product Right

Note: To access the Web Diagnostics page through the Web Client's Administration layout, you must have additional user configuration privileges. For more information, see [Required Administrative Rights on page 136](#).

IE Security Requirements

Ensure the workstation's Internet Explorer security settings are correct for the Web Server's security zone. Because the Microsoft scripting object is not marked safe for scripting, you must set the **Initialize and script ActiveX controls not marked as safe** setting to **Prompt**.

If you disable this setting, you will get the following error message for Client Side Diagnostics checks: **Unable to create File System Object**.

Accessing the Web Diagnostics Page

There are two ways to access the Web Diagnostics page: by loading the URL directly, or by opening it from the Administration layout in the Web Client.

- [Accessing the Diagnostics Page Directly on page 199](#)
- [Accessing Diagnostics Through the Administration Layout on page 201](#)

Accessing the Diagnostics Page Directly

Any OnBase user with the **Web Client** product right can access the Web Diagnostics page by following these steps:

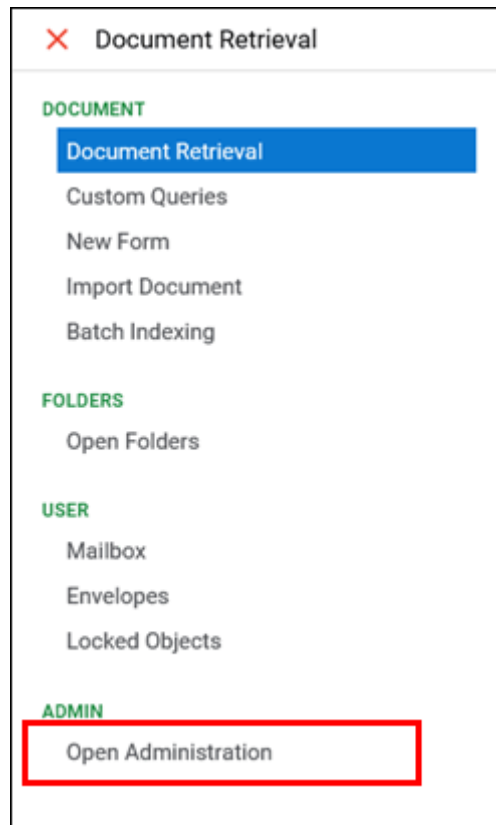
1. Access the following URL, where <servername> and <virtualdirectory> represent the name of the server and the directory where the OnBase Web Server is installed:
http://<servername>/<virtualdirectory>/diagnostics/diagnostics.aspx

2. If prompted, log on to OnBase.
3. The resulting page displays file information about the Web Server installation. See the following topics for more information.

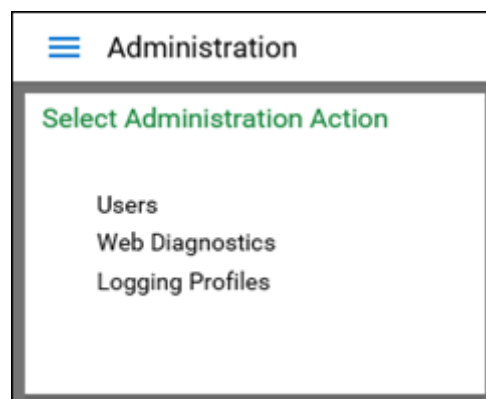
Accessing Diagnostics Through the Administration Layout

Only administrators can access the Web Diagnostics through the Web Client's Administration layout. To ensure you have sufficient privileges, see [Required Administrative Rights on page 136](#).

1. Log on to the OnBase Web Client.
2. Select the Main Menu button, and then scroll down and select **Open Administration** from the menu list.






The **Administration** panel is displayed.



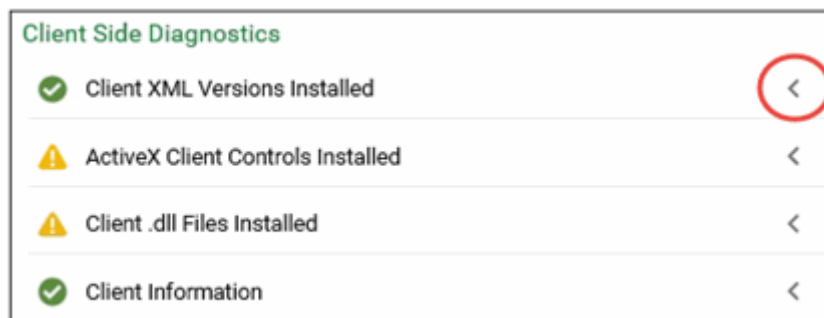
3. Select **Web Diagnostics**. The resulting page displays file information about the Web Server installation. See the following topics for more information.

Diagnostics Status Symbols

The Web Diagnostics page displays the results for a series of server-side and client-side checks. For each category of checks, one of the following symbols is displayed:

Symbol	Description
	The pass symbol indicates that all category checks passed.
	The alert symbol indicates that there are potential problems with the current configuration. When the category is expanded, the warnings that triggered the alert are displayed in blue.
	The fail symbol indicates that one or more category checks failed. When the category is expanded, the failed checks are displayed in red.

To expand a category and view the results for individual checks, click the plus sign next to the category's name:



Warnings are displayed in blue. Failed checks are displayed in red. Possible triggers include duplicate and missing files, invalid settings, and missing software requirements.

Client Side Diagnostics

Client XML Versions Installed

ActiveX Client Controls Installed

Client .dll Files Installed

DM DLL File Information	Version	Date Created
AEXCommServer.dll	Unable to perform File System check.	
olemsg32.dll	Unable to perform File System check.	
cdo.dll	Unable to perform File System check.	
dmimage_web170.dll	Unable to perform File System check.	
dmlocale_web170.dll	Unable to perform File System check.	
dmMailServices.dll	Unable to perform File System check.	
dmmailsvc_web170.dll	Unable to perform File System check.	
dmtrace_web170.dll	Unable to perform File System check.	
snbd19cm.dll	Unable to perform File System check.	

Client Information

Required Browser Features

Diagnostics Categories

The Web Diagnostics page is divided into Server Side Diagnostics and Client Side Diagnostics information. Server Side Diagnostics information is available only to users who have the **Web Server** administrative product right. This category includes the following:

Server Side Diagnostics	Description
ActiveX Libraries	Lists information for all ActiveX CAB files on the Web Server.
Web Server Libraries	Lists information for OnBase C# Core files on the Web Server. The Server Designation (if applicable) or machine name of the Web Server is also displayed.
Web Server Reference Libraries	Lists information for non-OnBase library files used by the Web Server.

Server Side Diagnostics	Description
Application Server Libraries	Lists information for OnBase C# Core files on the Application Server. The Server Designation (if applicable) or machine name of the Application Server is also displayed.
Application Server Reference Libraries	Lists information for non-OnBase library files used by the Application Server.
Web.Config Settings	Lists values for select Web Server Web.config settings.
Server XML Versions	Lists MSXML versions installed on the server.
ASP.NET and IIS Install Information	Lists the server's IIS and ASP.NET installation status. Also lists relevant ASP.NET extension mappings for the current virtual directory. If this check fails, .NET Framework may have been installed before IIS. Installing .NET Framework after IIS can corrupt the extension mappings. To resolve this issue, see IIS and .NET Framework Errors on page 193 .

Client Side Diagnostics information is available to any user who has the **Web Client** product right. This category includes the following:

Client Side Diagnostics	Description
Client XML Versions Installed	Lists MSXML versions installed on the client workstation. This section is available only when the Web Diagnostics page is accessed using Internet Explorer.
ActiveX Client Controls Installed	Lists information for ActiveX controls installed on the client workstation. This section is available only when the Web Diagnostics page is accessed using Internet Explorer.
Client .dll Files Installed	Lists information for DLL files installed on the client workstation. This section is available only when the Web Diagnostics page is accessed using Internet Explorer.
Client Information	Lists browser information for the client workstation.

Changing Logging Profiles

Use the Logging Profiles page in the Administration layout to enable or disable diagnostics logging without disrupting current users' sessions.

You also can enable and disable logging through the Application Server's or Web Server's Web.config file, but that method causes the associated server application to restart, and current users' sessions are lost. Because the Logging Profiles page does not modify the Web.config files, neither application is restarted, and existing sessions are maintained.

Note the following about changing logging profiles in the Web Client Logging Profiles page:

- To view and change logging profiles, you must have the **Web Server** administrative product right.
- If you modify the Web Server's Web.config file or recycle its application pool, the Web Server's logging profiles are reset to use the settings in the Web.config file. Similarly, the Application Server's logging profiles are reset if you recycle its application pool or modify its Web.config file.
- Depending on the message profile types you select, one or more warnings may be displayed. These warnings indicate whether the selected logging profile is a high-traffic profile. Be sure to disable high-traffic profiles as soon as you are done troubleshooting the issue.

To change logging profiles:

1. In the OnBase Web Client, click the Main Menu button and select **Open Administration**. The **Administration** layout is displayed.
2. Select **Logging Profiles**. The **Logging Profiles** page is displayed.

The left column displays the Web Server's logging profiles, and the right column displays the Application Server's logging profiles. If any other diagnostics logging routes have been configured, those routes are also displayed. Click a column heading to expand the list of logging profiles.

Logging Profiles

The following summarizes the editable logging routes found within the Web Client and Application Server config files. If necessary, adjust the minimum error level and enable one or more profiles to help troubleshoot and trace issues. When complete, revert back to the production level settings by clicking the Restore Defaults button below. Any changes saved will be applied instantly in memory and will not require a restart.

WEB SERVER LOGGING PROFILES
SRV-123 Web Server

APPLICATION SERVER LOGGING PROFILES
SRV-456 Application Server

DiagnosticsConsole

Warning: This logging route is configured to log all profiles by default. To enable one or more specific profiles, check the respective boxes below.

Minimum Error Level: Trace

- ☐ ASPNet (Default: Disabled)
- ☐ Cache (Default: Disabled)
- ☐ Configuration (Default: Disabled)
- ☐ Database (Default: Disabled)
- ☐ Errors (Default: Disabled)
- ☐ File (Default: Disabled)
- ☐ LDAP / NT Authentication (Default: Disabled)
- ☐ Lock Activity (Default: Disabled)
- ☐ Report Services (Default: Disabled)
- ☐ Script Exceptions (Default: Disabled)
- ☐ Service (Default: Disabled)
- ☐ Trace (Default: Disabled)
- ☐ VB Script (Default: Disabled)
- ☐ Warnings (Default: Disabled)
- ☐ WCF (Default: Disabled)
- ☐ Web Service (Default: Disabled)
- ☐ Workflow (Default: Disabled)

Restore Defaults

The Database Logging Profile is a high traffic profile that will increase memory usage. It should only be enabled when checking for a Database specific error and should be disabled afterwards.

The Service Logging Profile is a high traffic profile that will increase memory usage. It should only be enabled when checking for a Service specific error and should be disabled afterwards.

Save Cancel

3. In the column for each server application, use the **Minimum Error Level** drop-down list to set the minimum level of messages logged for that application's logging route. The levels are based on standard logging levels for Microsoft .NET Core and ASP.NET Core applications, and they include the following:
 - **Trace**
 - **Debug**
 - **Information**
 - **Warning**
 - **Error**
 - **Critical**

4. In the column for each server application, select the profiles for the types of messages that you want to log from that application. Deselect any profiles for which you do not want to log messages.

For descriptions of available message types, see [Diagnostics Profiles on page 294](#).

Note: If no specific profiles are selected for an application's logging route, then all profiles will be logged by default.

5. Click **Save**. The Web Server and Application Server are now respecting your changes, and the Web.config files remain unchanged.

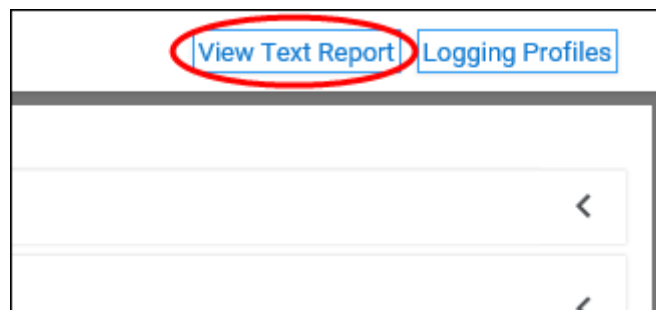
Restoring Default Logging Profiles

When you are finished troubleshooting, return to the Logging Profiles settings, and then click **Restore Defaults**. This button causes the Web Server and Application Server to again respect the logging settings configured in their respective Web.config files.

Viewing a Diagnostics Text Report

If you accessed the Web Diagnostics page directly using Internet Explorer, Firefox, or Safari, you can view a text report containing diagnostics information. This information can then be copied and pasted into an email, or into a text editor outside of OnBase.

1. Click the **View Text Report** button at the top of the Web Diagnostics page.



The **Diagnostics Report** window is displayed.

2. Press **Select All** to select all of the diagnostics information.
3. In Internet Explorer, you can click the **Copy To Clipboard** button to automatically copy the selected text to the clipboard. In other Web browsers, press **CTRL+C** to copy the text.
4. Paste the text into a text editor or into a new email message. The diagnostics information can then be saved or sent via email to another email address.

Diagnostics Using trace.axd

Some diagnostic information can also be obtained using the utility that is located at appnet/trace.axd. This tracing software is a part of Microsoft's .NET package. Full information on this utility can be found on MSDN (Currently, the page is located at <http://msdn2.microsoft.com/en-us/library/ms972204.aspx>).

Web Server Availability

To confirm that the Web Server is available and communicating with the database, enter the following URL in a web browser, where **[Server Location]** is the network location of the server hosting the Application Server, and **[Server Name]** is the name of the Web Server:

https://[Server Location]/[Server Name]/api/Server/IsAlive

The browser returns a **True** page if the Web Server is available, and a **False** page if the Web Server is unavailable.

Contacting Support

When contacting your solution provider, please provide the following information:

- The OnBase module where the issue was encountered.
- The OnBase version and build.
- The type and version of the connected database, such as Microsoft SQL Server 2014 or Oracle 12c, and any Service Pack that has been installed.
- The operating system that the workstation is running on, such as Windows 10 or Windows Server 2012 R2, and any Service Pack that has been installed. Check the supported operating systems for this module to ensure that the operating system is supported.
- The name and version of any application related to the issue.
- The version of Internet Explorer and any Service Pack that has been installed, if applicable.
- A complete description of the problem, including actions leading up to the issue.
- Screenshots of any error messages.

Supplied with the above information, your solution provider can better assist you in correcting the issue.

Web Server Information Required When Contacting Support

In addition to the information listed in [Contacting Support on page 208](#), for Web Server issues, provide the following information to your customer support representative:

- Browser type and version.
- Operating System version and Service Packs for the machine(s) running the Web Server and accessing the Web Server.

Prior to contacting Technical Support for Web Server related issues, it is recommended that a problematic client PC connect to the **diagnostics.aspx** page to run an extensive diagnostics test. Providing these test results at the time of an initial call will often reduce the time required to resolve the problem. See the [Web Diagnostics Page on page 198](#) for details on running the test and capturing the test results.

Configuration Module

OnBase Configuration Considerations

The OnBase Web Server is primarily configured through the OnBase Configuration module in the same way as the OnBase Client module is configured. In some cases, configuration options differ. These differences are noted below. See the Client module help files for configuration details.

Feature	Description of Difference
Scanning	User groups must have the Create privilege (in addition to the Scan product right) in order to scan documents in the Web Client. Users must also have Web Scanning Named User selected in the User Settings dialog box. The Create privilege is not required to scan documents through the Client module.
Redactions	The redaction Document Type must have exactly the same attributes as the original's Document Type (for instance, keywords must be identical).
Custom Splash Screen	Custom HTML splash screens must be archived under the SYS HTML Forms document type. For more information, see the OnBase Configuration documentation.

For specific configuration instructions, see the appropriate module's documentation or the OnBase Configuration module help files.

Limit your configuration to the functionality available in the Web Server.

Web Server Client Considerations

The Web Server functions similarly to the OnBase Client module, but currently has the following limitations:

Feature	Description
Import processes	Scanning from disk and ad hoc import are the only means for bringing documents into OnBase through the Web Client. The scan capability is designed for low-volume processing. There is no interface for COLD, DIP and check import processing.

Feature	Description
Workflow timers	You cannot manually execute Workflow timers. They are managed by the Workflow Server Manager.
Override permissions for creating and uploading documents	If you have the proper permissions to use a Workflow, then you can update documents in that Workflow, even if you would normally not have permissions to update that document otherwise.

Keyword Considerations

Required Keyword Types

Some Document Types contain Keyword options that require Keyword values to be entered in order to create and/or retrieve documents. Required Keywords are displayed in red for these operations, which may include the following: Document Retrieval, upload, indexing, re-indexing, viewing/modifying keywords, and scanning.

Masked Keyword Types

Keyword Type masking is supported in the OnBase Web Client, as long as the masks do not have leading blank spaces.

Caution: Do not configure Keyword Type masks that begin with leading blank spaces. Keyword values with leading blank spaces are not supported in the OnBase Core.

Custom Query Configuration

The following information describes Custom Query configuration settings that can be used with the Web Client. For further information on Custom Query configuration, see the **System Administration** documentation.

Grouping Columns

Custom Queries that have been configured with display columns can be configured to automatically group results by a display column.

Note: Custom Written SQL Custom Queries cannot be configured for column grouping.

To configure Custom Query column grouping:

1. Select a Custom Query in the OnBase Configuration module's **Custom Query** dialog box.
2. Click **Group Columns**. The **Query Results Group Columns** dialog box is displayed:

The screenshot shows a dialog box titled "Query Results Group Columns". It has two main sections: "Available Columns" on the left and "Selected Columns" on the right. The "Available Columns" list contains the following items: Document Type, Vendor Name, PO #, Invoice #, Invoice Amount, and Status. Between the two lists are two buttons: "Add >>" and "<< Remove". To the right of the "Selected Columns" list are two buttons: "Move Up" and "Move Down". At the bottom of the dialog box are two buttons: "Save" and "Cancel".

3. Double-click a column in the **Available Columns** list, or select it and click **Add**. The selected column is displayed in the **Selected Columns** list.
4. Repeat the previous step to add additional columns.
5. Order the columns in the **Selected Columns** list by selecting them and using the **Move Up** and **Move Down** buttons.
6. Click **Save**.

User Groups & Rights

Users must have the Web Client product right in order to use the Web Client.

1. From the Configuration Module, select **Users | User Groups/Rights**.
2. Select a User Group and click **Product Rights**.
3. Ensure **Web Client** is selected. Click **Save** to save any changes and exit.

4. Click **Exit** to exit **User Groups & Rights**.

Note: If you have users who are members of more than one User Group, you have the option to override Document Type privileges. Exercise caution when using this feature. To view this setting, log on to OnBase Configuration and select **Users | Global Client Settings**. The setting is on the **Security** tab under **Document Type Permission Overrides**. Choosing **Least Restrictive** means that if any one user group has the privilege for this Document Type, the user has the privilege for the Document Type. Choosing **Most Restrictive** means that if any one user group does not have the privilege for this Document Type, the user does not have this privilege for the Document Type.

Disable Change Password

You can disable the user's ability to change their password.

1. From the Configuration module, select **Users | User Names/Passwords**.
2. Select a User and click **Settings**.
3. Select the **Disable Change Password** check box.
4. Click **Save**.

The ability for this user to change his/her password is now suspended.

Modify Users

Only the Manager and Administrator users can modify the Manager or Administrator accounts using the Admin context in the Web Client.

Granting Disk Group Access

For users to be able to retrieve files, you must grant the accounts accessing the Disk Groups sufficient share/NTFS permissions to the Disk Group directories.

The Application Server domain account that accesses the Disk Group requires the following permissions.

- Share permissions: **Change** (which includes **Read**)
- NTFS permissions: **Modify** (which includes **Read & Execute**, **List Folder Contents**, **Read**, and **Write**).

If impersonation is enabled on the Application Server, then the impersonation account requires these permissions. If impersonation is not enabled, then the identity account running the Application Server's application pool requires these permissions.

For more information about Disk Group access, see the Configuration help files.

Disk Group Fault Tolerance

If your disk groups are set up for fault tolerance, documents that are not found on the first copy of a disk group, but exist on a subsequent online copy, will be displayed using the subsequent copy's file. To learn more about fault tolerance, see the Configuration help files.

Refreshing the Application Server After OnBase Configuration Updates

Modules that use an Application Server do not reflect changes made in OnBase Configuration until after the Application Server is refreshed. You can refresh the Application Server by recycling its application pool or resetting its cache. For example, if you add a new print queue or a print format, you need to refresh the Application Server in order for the changes to be reflected in the Web Client. A refresh is not required for clients to reflect changes to user privileges and rights, because these configurations are not cached.

Caution: Recycling the application pools disconnects users who are logged on to OnBase through the Application Server or Web Server. Any unsaved work by these users will be lost. Application pool recycling should occur during scheduled maintenance hours when no users are connected to the Application Server.

To reset the Application Server's cache without recycling the application pool, use the **Reset Cache** option in OnBase Configuration. This option resets the cache for all Application Servers using the current data source. All clients and modules that communicate with the Application Server are affected when the cache is reset.

Caution: Using the **Reset Cache** option in OnBase Configuration or the **Reset Server Cache** option in OnBase Studio may have a negative impact on system performance. Requests to the Application Server will be forced to wait until the cache is rebuilt before they can be processed. Depending on the size of the OnBase system, as well as the current server load, the performance impact of resetting the cache may be severe.

To avoid performance issues, only reset the cache of the Application Server during off-peak hours. For more information about the Reset Cache option in OnBase Configuration, see the **System Administration** documentation. For more information about the Reset Server Cache option in OnBase Studio, see the **Studio** documentation.

Note: Changes can take up to a minute to take effect after a reset. Some changes will take effect without requiring users to log off; however, it is considered a best practice to have users log off and log back on to ensure all changes take effect. Notify users of changes only after the Application Servers have had time to reset.

Caution: The **Reset Cache** option should be used only for small, additive changes, such as adding a new Note Type. Do not use this option for large changes, such as Workflow process changes or removal of a configuration someone might currently be using. For large changes, schedule system downtime to recycle the application pool. For more recommendations, see the OnBase Configuration help files.

OnBase Authentication Schemes and Security

Contact your service provider for detailed information regarding OnBase authentication schemes and security. For information about configuring OnBase to work with Directory Service Authentication, see the **Legacy Authentication Methods** module reference guide.

For information about configuring the Web Server to work with Active Directory authentication, see [Active Directory Authentication on page 54](#).

The Integrated Office Viewer Integration

The OnBase Integrated Office Viewer (previously known as the WOPI Viewer or WOPI Server) integrates with the Microsoft Office Online Server or Office for the web. It provides users with integrated access to OpenDocument and Microsoft Office documents within OnBase and seamlessly displays Word, Excel, and PowerPoint documents to end users within the familiar OnBase client interfaces.

In addition to the OnBase Integrated Office Viewer, depending on whether you use the Microsoft Office Online Server or Office for the web, two additional configurations may be used: the WOPI endpoint and the Hyland Broker for Microsoft Office.

The WOPI endpoint is a communication layer between the separately installed and configured Microsoft Office Online Server or Office for the web and the OnBase Application Server.

The Hyland Broker for Microsoft Office is used to enable communication between the OnBase Integrated Office Viewer and Office for the web.

For information about the Integrated Office Viewer configuration, see the **Integrated Office Viewer** module reference guide.

Email Web Integration Settings

You can configure OnBase to use an external web email service to email documents from the Web Client using the **Send To | Mail Recipient** functionality.

Some configuration with the external web email service is required, to expose the email service to integration with OnBase. Additionally, you must enable email integration in the Web Server web.config file and configure the integration in the OnBase Configuration module.

See the following sections for more information on enabling a specific email service for the Web Client:

- [Enabling Google Gmail on page 215](#)
- [Enabling Microsoft Office 365 on page 217](#)
- [Enabling Microsoft Exchange on page 218](#)

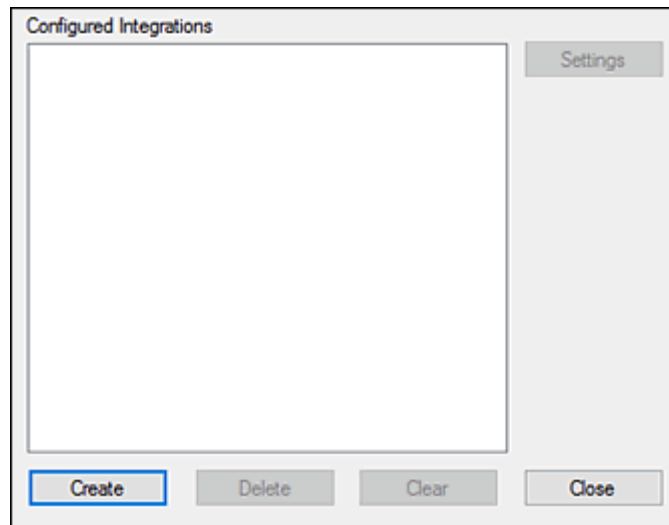
Enabling Google Gmail

To connect to a Google Gmail email service from the OnBase Web Client, you must first create a project in the Google Developers Console to obtain a Client ID and Client Secret. These credentials allow OnBase to connect to the email service. For more information on completing these requirements, see Google's documentation.

To enable Google Gmail functionality for the Web Client:

1. Open the Web Server web.config file in a text editor, such as Notepad.
2. Locate the **UseWebMail** setting in the **appSettings** section, and set the **value** to **true**.
3. Save and close the file.

- In the Configuration module, select **Utils | Web Integration Settings**. The **Web Integration Settings** dialog box is displayed, listing **Configured Integrations**.



- Click **Create** to configure a new integration. The **Web Integration Settings** dialog box is displayed, containing settings for the integration.

- Select **Web Client (Mail Sending)** from the **Integration Type** drop-down list.
- Select **Google** from the **Service Type** options. The **Client ID** and **Client Secret** fields become available, and the **Authentication Type** is automatically set to **OAuth**.

8. Enter the **Client ID** field with the client ID created in the Google Developers Console.
9. Enter the **Client Secret** field with the client secret acquired from the Google Developers Console.
10. Click **Save**.

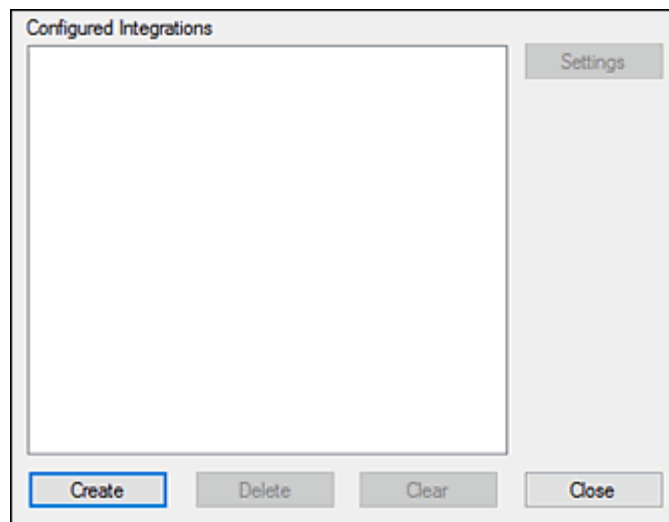
Note: Changes in the Configuration module require an IIS reset before they take effect in the Web Client.

Enabling Microsoft Office 365

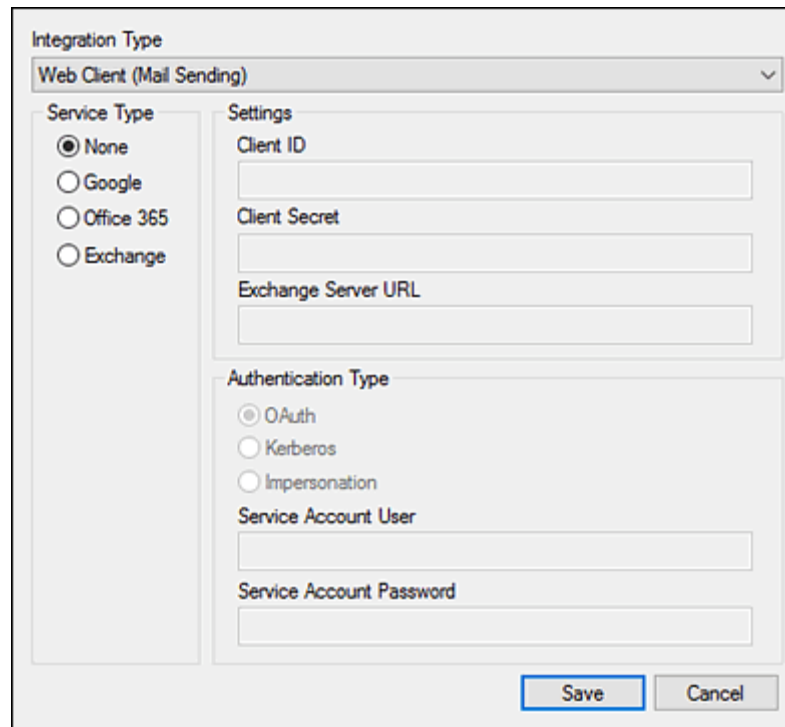
To connect to a Microsoft Office 365 email service from the OnBase Web Client, you must first create a project in the Microsoft Azure portal to obtain a Client ID and Client Secret. These credentials allow OnBase to connect to the email service. You also must enable accounts in any organizational directory for supported account types to ensure that your application supports multi-tenancy. For more information on completing these requirements, see Microsoft's documentation.

To enable Microsoft Office 365 email functionality for the Web Client:

1. Open the Web Server web.config file in a text editor, such as Notepad.
2. Locate the **UseWebMail** setting in the **appSettings** section, and set the **value** to **true**.
3. Save and close the file.
4. In the Configuration module, select **Utils | Web Integration Settings**. The **Web Integration Settings** dialog box is displayed, listing **Configured Integrations**.



- Click **Create** to configure a new integration. The **Web Integration Settings** dialog box is displayed, containing settings for the integration.

The image shows a 'Web Integration Settings' dialog box. At the top, there is a dropdown menu for 'Integration Type' with 'Web Client (Mail Sending)' selected. Below this, on the left, is a 'Service Type' section with four radio buttons: 'None' (selected), 'Google', 'Office 365', and 'Exchange'. To the right of the 'Service Type' section is a 'Settings' area. It contains three text input fields: 'Client ID', 'Client Secret', and 'Exchange Server URL'. Below these is an 'Authentication Type' section with three radio buttons: 'OAuth' (selected), 'Kerberos', and 'Impersonation'. Underneath are two more text input fields: 'Service Account User' and 'Service Account Password'. At the bottom right of the dialog are two buttons: 'Save' and 'Cancel'.

- Select **Web Client (Mail Sending)** from the **Integration Type** drop-down list.
- Select **Office 365** from the **Service Type** options. The **Client ID** and **Client Secret** fields become available, and the **Authentication Type** is automatically set to **OAuth**.
- Enter the **Client ID** field with the client ID created in the Microsoft Application Registration Portal.
- Enter the **Client Secret** field with the client secret acquired from the Microsoft Application Registration Portal.
- Click **Save**.

Note: Changes in the Configuration module require an IIS reset before they take effect in the Web Client.

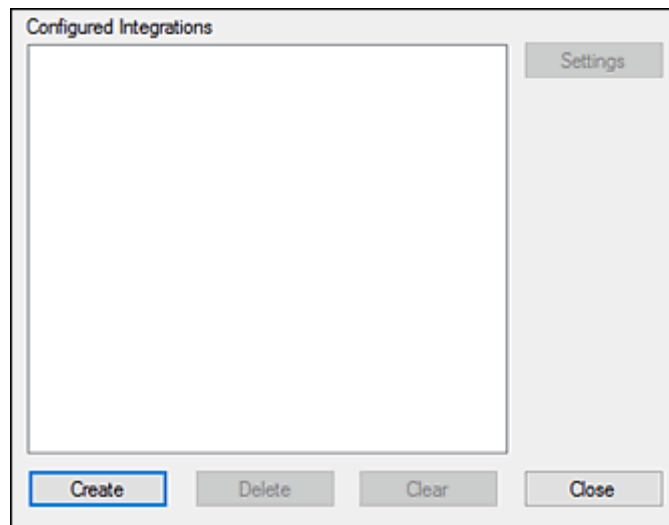
Enabling Microsoft Exchange

To connect to a Microsoft Exchange email service from the OnBase Web Client, you must have a functioning Exchange Server and authentication enabled through either Kerberos or impersonation with a service account. For more information on completing these requirements, see Microsoft's documentation.

To enable Microsoft Exchange email functionality for the Web Client:

- Open the Web Server web.config file in a text editor, such as Notepad.
- Locate the **UseWebMail** setting in the **appSettings** section, and set the **value** to **true**.

3. Save and close the file.
4. In the Configuration module, select **Utils | Web Integration Settings**. The **Web Integration Settings** dialog box is displayed, listing **Configured Integrations**.



5. Click **Create** to configure a new integration. The **Web Integration Settings** dialog box is displayed, containing settings for the integration.

6. Select **Web Client (Mail Sending)** from the **Integration Type** drop-down list.

7. Select **Exchange** from the **Service Type** options. The **Exchange Server URL** field and **Authentication Type** options become available.
8. Enter the **Exchange Server URL** field with the URL for the Microsoft Exchange email server.
9. Select the **Authentication Type** option to use for authentication into the email service:
 - **Kerberos**: Select to use Kerberos authentication.
 - **Impersonation**: Select to use impersonation. You must also enter the user name and password of the service account used for impersonation.
10. Click **Save**.

Note: Changes in the Configuration module require an IIS reset before they take effect in the Web Client.

Client and Server Configuration

The following topics cover workstation and server configuration information for the OnBase Web Server:

- [Browser Session Cookies on page 221](#)
- [Persistent Cookies or DOM Storage for Client Settings on page 221](#)
- [Client Browser Deployments on page 222](#)
- [Client Email Requirements on page 227](#)
- [Audio and Video File Requirements on page 227](#)
- [Video On Demand/Media Stream Requirements on page 227](#)
- [Regional Formats for Currency, Dates, and Numbers on page 228](#)
- [Application Server Session Timeout on page 228](#)
- [HTTP Compression on page 229](#)
- [Windows Performance Monitor Counters on page 229](#)
- [Changing the Data Source on the URL on page 230](#)
- [3GB Startup Parameter for Windows on page 230](#)
- [Ensuring Proper .NET Installation on page 231](#)
- [IIS and ASP.NET Configuration for Web Server Autologin on page 233](#)
- [Application Pool Configuration on page 237](#)

Browser Session Cookies

Because HTTP and HTTPS are stateless protocols, a Web server can only store server-side information for each user by the use of a unique Client-side identifier for each open browser session. The session cookie is an example of such an identifier. When Active Server Pages are served from Internet Information Services (IIS), a unique session cookie is delivered to a Client's browser when the first ASPX page is requested. This session cookie identifies the user while the user's session is active on the site. The cookie is stored in the browser PC's memory only while the session is open; the cookie is never stored on the Client's hard drive like a normal persistent cookie. Each HTTP request sent by the user's browser includes the ASP.NET session ID information from the session cookie in memory.

Note: A single Internet Explorer process cannot run more than one instance of the Web Client. Attempting to log on multiple times using the same Internet Explorer process will generate a prompt to close either the new session or the existing session. The Web Client can be opened multiple times using different Internet Explorer processes.

One related security concern exists. Though unlikely, it is possible for a malicious user to perform a network trace to obtain a user's session cookie when it is sent to the Web Server. With this session ID, a malicious user can make server requests to the server and effectively see that user's information stored in the session variables. For a more secure environment, Microsoft recommends that HTTPS secure connections be used to encrypt the HTTP data stream, which includes the session cookie. It is recommended that HTTPS only be used on connections requiring the higher security level, since encryption is an extremely processor-intensive task.

It is also critical that all appropriate security patches from Microsoft be installed and configured properly on the Internet Information Services (IIS) Web server. Information on obtaining Microsoft security patches can be found at: <http://www.microsoft.com/technet/security/tools/default.mspx>.

Persistent Cookies or DOM Storage for Client Settings

The Web Server tracks each user's client settings using either a persistent client-side cookie or DOM Storage. Client settings include the following:

- Browser window size and position—The size and position of the main Web Client browser window, and the size and position of the browser window that displays only the Document Search Results list and Document Viewer. Examples include the cross-reference results window and the DocPop results window.
The cookie also tracks the size of the browser window displayed when the **Open in New Window** option is used.
- Document Search Results list—Row coloring.
- Document Search Results list—Height of Document Search Results list. The **RememberHitListHeight** setting must be set to **true** in the Web Server's Web.config file.
- Favorites—The contexts that the user has designated as "favorites."
- Folders—Height and width of folder navigation panes.

- HTML Viewer—Zoom and scaling settings. The ActiveX viewer also preserves these settings, but it uses the system registry rather than a cookie.
- Home Page—The context that the user has designated as his or her home page.
- Import—The Document Date lock and settings for clearing the Document Type and Keyword values upon import.
- WorkView—Document Viewer position and **Reuse Existing** viewer option. These settings are saved only if the **Remember Position** and **Reuse Existing** viewer options are enabled. See the WorkView module reference guide for more information about viewer options.

These settings are saved per machine and per domain user.

Users can restore the default size-related settings by accessing **Client Settings** from the Web Client's **User** context.

Client Browser Deployments

The first time a new client browser connects to the OnBase Web Server configured for the ActiveX Web Client, the Web Server sends the current client-side ActiveX files through the Internet connection to the client workstation, where they are automatically installed in the **C:\Windows\SysWOW64** directory.

This installation can be handled also by the Client Setup page, which installs the files and guides the users through any messages they may encounter during the installation. For more information about this deployment approach, see [Client Setup Page on page 224](#).

On the Web Server, ActiveX files are stored in a set of compressed CAB files that are digitally signed by Hyland Software. When the Web Server source files are updated with new versions or service packs of the ActiveX files, future client browsers that connect are pushed a set of the new files.

When determining whether to upgrade a client's files, the Web Server compares the file version of the client's controls to the file version of the server's controls. If the first three numbers in the file version match, no files are upgraded. If the first three numbers differ, the server pushes a set of the new files to the client. The build number, which is the fourth number in the file version, is ignored. This versioning ensures that all client browsers are using a compatible set of ActiveX files and the associated client-side DLLs required.

Note: For information about configuring Internet Explorer security settings for the Web Client, see [Security & Browser Settings on page 6](#).

Whenever a Web Server is downgraded to an earlier release, newer clients connecting to the server will usually need to have the existing client-side OCX and DLL files deleted manually.

Server-side CAB files stored in the ..\ActiveX subdirectory	Client-side file contents
HylandDocumentSelect.cab	HylandDocumentSelect.ocx
HylandViewer.cab	HylandViewer.ocx
OBXAltCommon.cab	dmimage_alt.dll dmlocale_alt.dll dmMailServices.dll dmmailsvc_alt.dll dmtrace_alt.dll
OBXAltDocumentSelect.cab	OBXAltDocumentSelect.ocx
OBXAltViewer.cab	OBXAltViewer.ocx
OBXAppEnabler.cab	AECCommServer.exe AECCommServerNET.dll AEXCommServer.dll Hyland.Canvas.Automation.dll Hyland.Common.dll Hyland.Types.dll
OBXWebControls.cab	dmimage_web180.dll dmlocale_web180.dll dmMailServices.dll dmmailsvc_web180.dll dmtrace_web180.dll OBXWebControls180.ocx

Note: The OCX files are registered with the client PC registry automatically. The logged-in Windows workstation running the client browser must have permission to write to that directory and to modify the registry in order for the controls to be registered successfully. The client browser also must be configured to allow the downloading and scripting of signed ActiveX controls within Internet Explorer's **Tools | Internet Options | Security** dialog box.

Antivirus Software and Client-Side ActiveX Controls

If antivirus software is used on a client workstation running the ActiveX Web Client, the downloaded ActiveX controls on the client workstation should be excluded from virus scanning. Otherwise, the virus scan process can modify the ActiveX controls' file attributes in a way that can result in unresponsiveness or unintended application restarts.

The following ActiveX controls located in the **C:\Windows\SysWOW64** directory are involved, where *** represents the major version of the OnBase Web Server (for example, **OBXWebControls180.ocx** for version 18):

- OBXWebControls***.ocx
- dmimage_web***.dll
- dmlocale_web***.dll
- dmmailsvc_web***.dll
- dmtrace_web***.dll

You must whitelist these files every time you upgrade to a new major version of the OnBase Web Server, since the file names change with each version.

Note: It is not necessary to whitelist ActiveX controls that have been installed to the client workstation using the Web ActiveX Controls installer. Only the ActiveX controls downloaded from the web browser are affected.

Client Setup Page

The Client Setup page allows users to install the Web ActiveX files on their workstations without logging on to the Web Client. The page handles the download and installation of the files automatically. Users only need to click the **Begin Installation** button.

The Client Setup page is located at **http://Server/AppNet/ClientSetup.aspx**, where **http://Server/AppNet** is the value provided for **dmsVirtualRoot** in the Web Server's web.config file.

At the top of the page, you can view the status of the following features:

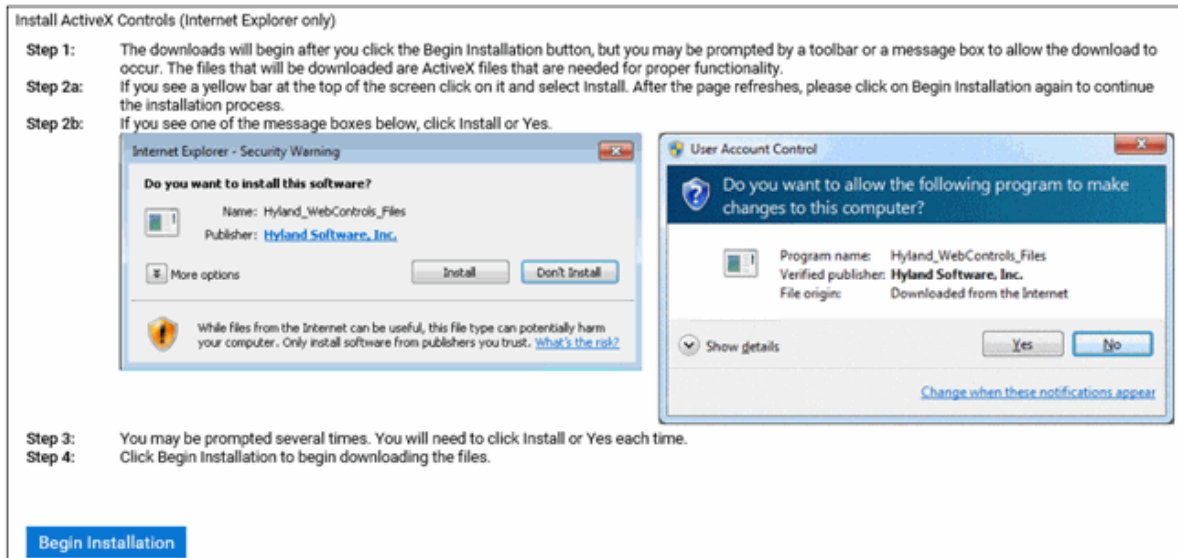
- JavaScript
- Cookies
- DOM Storage
- Show Pictures

Check Browser Features

All required features are enabled.

- ✓ JavaScript Enabled
- ✓ Cookies Enabled
- ✓ DOM Storage Enabled
- ✓ Show Pictures Enabled

If all features are enabled, they are listed as enabled with a green check mark. If any features are not enabled, a red X is displayed, and a message displays indicating that you need to review the list and then enable the feature in your web browser.



Files Installed

The Client Setup page installs the following files, where *** represents the major version of the OnBase Web Server (for example, **OBXWebControls180.ocx** for version 18):

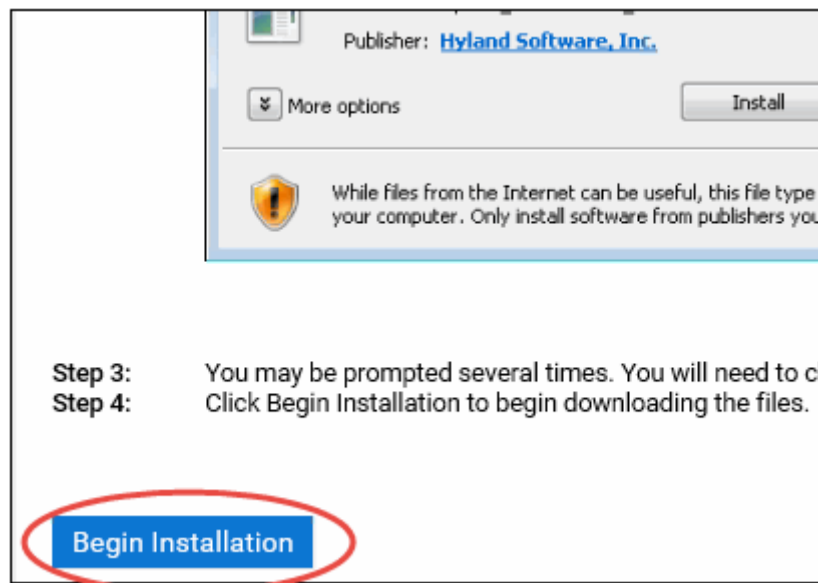
- dmimage_web***.dll
- dmlocale_web***.dll
- dmMailServices.dll
- dmmailsvc_web***.dll
- dmtrace_web***.dll
- OBXWebControls***.ocx

Note: If Application Enabler is configured on the Web Server, additional files are also installed.

Follow these steps to install ActiveX files using the Client Setup page:

1. Using Internet Explorer, access the Client Setup page URL (for example, **http://Server/AppNet/ClientSetup.aspx**).
2. Read the instructions provided.

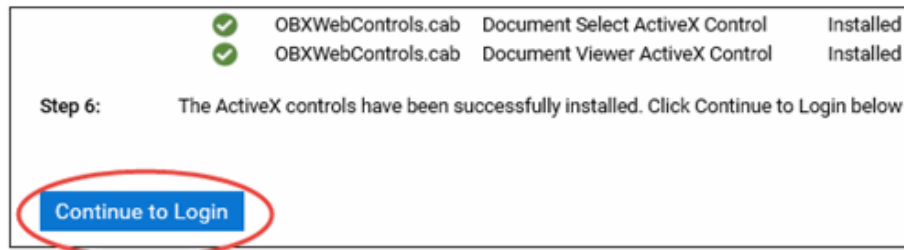
3. Click **Begin Installation**.



4. Depending on Internet Explorer's security settings, you may be prompted to continue with the installation. If prompted, choose to install the files.
5. Wait while the files are installed.

Wait for all files to be installed before navigating away from this page:			
✓	OBXWebControls.cab	File Service ActiveX Control	Installed
✓	OBXWebControls.cab	Popup ActiveX Control	Installed
✓	OBXWebControls.cab	Print ActiveX Control	Installed
✓	OBXWebControls.cab	Document Scan ActiveX Control	Installed
✓	OBXWebControls.cab	Document Select ActiveX Control	Installed
✓	OBXWebControls.cab	Document Viewer ActiveX Control	Installed

6. After the files are installed, click **Continue to Login** to proceed to the Web Client login page.



If one or more of the files fail to be installed, then you are prompted to refresh the page and try again.

Client Email Requirements

For Client-side emailing services the Web Client utilizes version 1.1 of Microsoft's CDO/Active Messaging API library. Various versions of the library will be installed on a Client PC, depending on the specific mail Client installed. The actual file that must be installed with the local mail Client is either CDO.DLL or OLEMSG32.DLL version 5.0.1457.3 or newer. Outlook Express is not a compliant email Client.

Audio and Video File Requirements

If users will be viewing audio and video documents, the user's workstation must have the proper applications or plugins installed for viewing specific file types. The type of application or plugin that is needed varies on the file type being accessed, as well as the browser being used to access the file. Additionally, some file formats may also require the configuration of a custom file format within the OnBase Configuration module. See the Configuration documentation for information on configuring custom file types. For information about the audio and video file types that each browser supports, refer to the specific browser's documentation to determine if a file type is supported for that browser.

Video On Demand/Media Stream Requirements

If users will be viewing Video On Demand, the Media Server and Wowza Server must be configured to work in their environment. View the specific configuration information in the OnBase Media Server manual.

The media stream files are viewed in the Web Client viewer using FlowPlayer. The FlowPlayer information returned by the web server must be viewed with Compatibility View disabled. This may require you to remove the Web Server from the Intranet zone in Internet Explorer, or to disable compatibility view for Intranet sites.

To disable compatibility view for all intranet sites:

1. Launch Internet Explorer.
2. Navigate to **Tools | Compatibility View Settings**.

3. Remove the check from the **Display intranet sites in Compatibility View** check box.
4. Click **Close**. The change is saved automatically.

Regional Formats for Currency, Dates, and Numbers

The OnBase Web Server supports only the default currency, date/time, and number settings for a locale; customizations are not supported. The following statement explains how formats are customized in Windows Server.

Default formats are those displayed by default when you select a **Format** from the **Formats** tab in the Region and Language applet. If you select a different date or time format, or if you change any formats accessed through the **Additional Settings** button, the Web Server will not respect the change.

If your deployment of the OnBase Web Server will be set in a locale other than **English (United States)**, please see [Internationalization And Localization Best Practices](#) on page 310.

Application Server Session Timeout

The Application Server's **enableTimeout** setting should be used to clean up sessions that have been abandoned. Abandoned sessions can present problems, because licenses are not released until the sessions are ended. A session might become abandoned if the user did not close the application properly. For example, the user might have terminated the application in Windows Task Manager, or there might have been a loss of network connectivity.

Do not use the **enableTimeout** setting to clean up sessions that are inactive only because the user has stopped working in OnBase. Not every application uses the Application Server's **enableTimeout** setting, and inactive sessions should be cleaned up by the OnBase application that initiated them. If you find licenses are not being properly released, try enabling the **enableTimeout** setting in the Application Server's web.config file. If enabling timeout resolves the behavior, then OnBase support representatives can use this information to help identify the problem's cause.

Enabling Timeout

To allow the Application Server to clean up abandoned sessions, set **enableTimeout** to **true** in the Application Server web.config file. Do not set **enableTimeout** to **true** if you want the Application Server to maintain sessions during periods of inactivity.

When timeout is enabled, the Application Server checks for inactive sessions using the **timeout** period specified in the **sessionState** element. The **timeout** period is approximate. Five minutes are added to the **timeout** value to calculate the timeout interval. The timer that is used to check for inactive sessions runs at half of the calculated timeout interval. Depending on when the timer last ran, an inactive session could remain for up to one and a half times longer than the configured **timeout** value. Therefore, if the **timeout** value is set to 15 minutes, the timer will run every 10 minutes, and a session will be cleaned up between 20 and 30 minutes of inactivity.

The minimum timeout value permitted for the Application Server is 10 minutes.

Note: The Application Server's **timeout** value should never be less than the **timeout** value specified in the Web Server's web.config.

HTTP Compression

HTTP compression allows Web servers to compress data sent to clients, thereby making better use of available bandwidth. This ability is very important in situations where there is low bandwidth, high latency, or both. Internet Information Services (IIS) 6.0 and later have a built-in ability to compress outgoing data, although some configuration is required.

The following procedures describe how to configure HTTP compression for the OnBase Web Server.

- [Configuring HTTP Compression in IIS 8.x on page 229](#)
- [Configuring HTTP Compression in IIS 10.x on page 229](#)

Note: Dynamic content compression must not be installed on the OnBase Application Server, because it interferes with the XML that is sent between the OnBase Application Server and the OnBase Web Server.

Configuring HTTP Compression in IIS 8.x

To configure HTTP compression in IIS 8.x, follow the procedure in the following Microsoft article:

[http://technet.microsoft.com/en-us/library/cc771003\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc771003(WS.10).aspx)

Configuring HTTP Compression in IIS 10.x

To configure HTTP compression in IIS 10.x, follow the procedure in the following Microsoft article:

[http://technet.microsoft.com/en-us/library/cc771003\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc771003(WS.10).aspx)

Windows Performance Monitor Counters

OnBase Core Services includes a set of Performance Monitor counters for administration and performance tuning purposes. These counters are installed automatically when the Hyland Server Side Components installer is used to install any server component.

The counters are available under the **Hyland** and **Hyland-Database** performance objects within Performance Monitor's **Add Counters** dialog box.

The following counters are available for the **Hyland** performance object:

- **Active Sessions:** Displays the current number of active sessions.
- **Failed login attempts:** Displays the current number of failed login attempts

- Object Locks: Displays the total number of object locks
- Total # of Document Queries
- Total # of Document Result Text Searches
- Total # of Full Text Searches
- Total # of Pages Rendered

The following counter is available for the **Hyland-Database** performance object:

- Total # of Database Queries

Changing the Data Source on the URL

You can access multiple data sources using the same Web Server without modifying the Web Server's Web.config file.

To access a data source other than the one specified in Web.config, append the query string **?datasource=<datasource_name>** to the start page URL. For example:

- **http://webserver/AppNet/login.aspx?datasource=testdb**

This URL instructs the Web Server to access the **testdb** data source rather than the **dmsDataSource** value configured in the Web Server's Web.config.

Note: You can also use query strings to execute a search as soon as users log on to the Web Client. For more information, see [Automatic Query Execution Upon Logon on page 65](#).

3GB Startup Parameter for Windows

On 32-bit versions of Windows, the /3GB boot.ini parameter (or startup switch) reallocates a system's virtual address space to give User mode programs access to more space.

The OnBase Web and Application Servers do not support the use of the /3GB startup parameter for Windows. Additionally, the use of this parameter limits the amount of memory available to the kernel and operating system.

Ensuring Proper .NET Installation

OnBase requires Microsoft .NET Framework 4.7.2 or later. The .NET Framework can be obtained from the Microsoft Download Center at <http://www.microsoft.com/downloads>.

Ensure that the required .NET Framework version is properly installed by checking the following items.

Installation Order

For .NET Framework to function properly, it must be installed after IIS is installed on the server. If .NET Framework was installed first, it must be re-installed after IIS is installed. Certain components of .NET Framework can only be registered when an IIS installation is present.

Note: The following steps cover the requirements for the OnBase Web Server and Application Server to function correctly. If other applications that require .NET Framework are installed on the server, then multiple versions of .NET may be required. When installing different versions of .NET, start with the lower required versions and work your way up to the latest.

These steps outline the correct order for installing .NET Framework:

1. Add the **Web Server (IIS)** role.
2. Install the appropriate .NET Framework Features.
3. Add the following role services and features:
 - Static Content
 - Default Document
 - ASP.NET
 - .NET Extensibility
 - ISAPI Extensions
 - ISAPI Filters
 - Windows Authentication (optional)
 - Request Filtering
 - IIS Management Console

Caution: Do not add the Dynamic Content Compression feature. This feature interferes with the XML sent between the Web Server and other servers or applications, and it should not be installed or enabled on the Web Server.

4. If necessary, install any available updates.

Manually Changing the .NET Version

Some supported peripheral products (such as some versions of SQL Server) change the default .NET version when they are installed. This means that subsequent virtual directories will inherit this default version. The following topics describe how to change the Web Server's .NET version manually. It should be set to version **4.0.30319**.

To change the .NET version on a virtual directory in Windows Server:

1. In the start menu or start screen, click **Run**.
2. Type **inetmgr** and click **OK**. The Internet Information Systems (IIS) Manager is displayed.
3. In the left pane, navigate to **Application Pools**.
4. From the list of application pools, double-click the application pool for the OnBase Web Server. The **Edit Application Pool** dialog box is displayed.
5. Under **.NET CLR version**, select **.NET CLR version v4.0.30319**.
6. Click **OK**.

IIS and ASP.NET Configuration for Web Server Autologin

The following topics describe the recommended IIS security and ASP.NET settings for the Web Server and Application Server when either interactive or non-interactive autologin is used. These recommendations are appropriate for all browser-based applications that use the OnBase Web Server.

ASP.NET impersonation is recommended for the Application Server, but it is not a requirement. If impersonation is not used, ensure the Application Server's identity account satisfies the criteria specified. The App Pool Identity and Local Service accounts would not satisfy these criteria for the Application Server.

These notes are organized under the following topics:

- [Overview on page 233](#)
- [Interactive Autologin on page 233](#)
- [Non-Interactive Autologin on page 234](#)
- [Other Important Notes on page 236](#)

Overview

The following table provides an overview of authentication settings for the Web Server and Application Server.

	Standard OnBase Authentication	Non-Interactive Autologin (NT/LDAP)	Interactive Autologin (NT/LDAP)
Web Server Virtual Directory	Anonymous Access	Integrated Windows authentication	Anonymous Access
Web Server Web.config	No impersonation needed	No impersonation needed	No impersonation needed
App Server Virtual Directory	Anonymous Access	Anonymous Access	Anonymous Access
App Server Web.config	Enable impersonation with a domain account that has modify privileges to the disk groups.	Enable impersonation with a domain account that has modify privileges to the disk groups and can query Active Directory.	Enable impersonation with a domain account that has modify privileges to the disk groups and can authenticate users against Active Directory.

Interactive Autologin

Interactive autologin prompts the user for credentials before granting the user access to OnBase. Interactive autologin presents stronger security because of this extra check.

The following topics outline recommended IIS security and ASP.NET settings for interactive autologin. An explanation of why each setting was chosen follows each table.

Web Server

The following table displays recommended Web Server IIS security and ASP.NET settings for interactive autologin.

Component	Recommended Setting
IIS	Anonymous Access
Application Pool Identity	App Pool Identity
Impersonation	N/A

Explanation:

- Integrated Windows authentication is not needed because the user is interactively providing credentials, allowing Anonymous Access to be the appropriate security setting.
- The App Pool Identity account without impersonation is appropriate because the ASP.NET worker process does not need elevated domain privileges.

Application Server

The following table displays recommended Application Server IIS security and ASP.NET settings for interactive autologin.

Component	Recommended Setting
IIS	Anonymous Access
Application Pool Identity	App Pool Identity
Impersonation	Domain user account with the Read Group Membership permission

Explanation:

- Anonymous Access is appropriate because the request is coming from the Web Server and not directly from the user.
- The identity or impersonation account needs the Account Operator role so that it can authenticate the user. It must also have permissions to the OnBase disk groups to retrieve content.

Non-Interactive Autologin

Non-interactive autologin obtains the username and domain from the browser using integrated Windows authentication, allowing the user to log on to OnBase without entering credentials.

The following topics outline recommended IIS and ASP.NET security settings for non-interactive autologin. An explanation of why each setting was chosen follows each table.

Web Server

The following table displays recommended Web Server IIS security and ASP.NET settings for non-interactive autologin.

Component	Recommended Setting
IIS	Integrated Windows authentication
Application Pool Identity	App Pool Identity
Impersonation	N/A

Explanation:

- Integrated Windows authentication is necessary to obtain the username and domain from the browser. Users must have NTFS **Read** permissions to read the Web Server content directory.
- The App Pool Identity account without impersonation is appropriate because the ASP.NET worker process does not need elevated domain privileges.

Application Server

The following table displays recommended Application Server IIS security and ASP.NET settings for non-interactive autologin.

Component	Recommended Setting
IIS	Anonymous Access
Application Pool Identity	App Pool Identity
Impersonation	Domain user account that has domain querying rights.

Explanation:

- Anonymous Access is appropriate because the request is coming from the Web Server and not directly from the user.
- The identity or impersonation account needs domain querying rights to look up the user's group in Active Directory.

Note: If you are using a module that directly communicates with the Application Server (e.g., Disconnected Scanning), then Anonymous Access may not be the appropriate setting for non-interactive Active Directory authentication.

Other Important Notes

When configuring IIS security and ASP.NET settings for your solution, also consider the following notes and recommendations:

1. Place a firewall between the Web Server and Application Server to ensure that the Application Server can only receive requests from a specific Web Server.
2. When Anonymous Access is used, the Anonymous Access account configured in IIS is still restricted by its NTFS permissions. Anonymous Access means that the user initiating the request is not being validated by IIS, but the Anonymous Access account is still key to everything.
3. If there is no need to authenticate the user who is accessing the Application Server, then there is no need to use integrated Windows authentication on the Application Server. If integrated Windows authentication is used on the Application Server, then the user account running the ASP.NET worker process on the Web Server will be authenticated for each request. The recommended way to restrict access to the Application Server is with a properly configured firewall.
4. In non-interactive authentication, the Web Server is not attempting to validate the user. This task is performed by the Application Server, which is why the domain account used for impersonation needs extra privileges.
5. IIS must be configured to use at least one authentication method. If no authentication method is selected, then the web application won't work.

Application Pool Configuration

The OnBase Web Server and Application Server should each run within its own application pool, separate from any other Web application on the IIS Web server. The following settings are best practices for application pools used for OnBase in order to maintain the highest system performance.

Note: Each OnBase Application Server should have its own IIS App Pool that is not shared with any other IIS Application or IIS Web Site.

To configure impersonation for the application that will be accessing the OnBase database and disk groups, see [Enabling Impersonation on page 52](#).

Application Pool Best Practices

The following topics describe application pool best practices for OnBase Web and Application Servers.

Tip: Configure the application pool from the **Advanced Settings** dialog box, which is accessible within Internet Information Services (IIS) Manager. This dialog box allows you to configure application pool settings from one location.

1. Log on to the server as an administrator.
2. Launch the Internet Information Services (IIS) Manager.
3. In the left pane of IIS Manager, browse to **Application Pools**.
4. From the list of application pools, select the application pool for the OnBase Web or Application Server.
5. In the **Actions** pane on the right, under **Edit Application Pool**, click **Advanced Settings**. The **Advanced Settings** dialog box is displayed.
6. Configure the application pool as described in the following topics:
 - [General on page 237](#)
 - [CPU on page 238](#)
 - [Process Model on page 238](#)
 - [Rapid-Fail Protection on page 238](#)
 - [Recycling on page 239](#)

General

Ensure the following General settings are applied:

General Setting	Value
.NET CLR Version	v4.0

General Setting	Value
Enable 32-Bit Applications	True - If installing a 32-bit server False - If installing a 64-bit server
Managed Pipeline Mode	Integrated
Queue Length	65535
Start Mode	AlwaysRunning

CPU

Set the CPU limit interval to 0.

CPU Setting	Value
Limit Interval	0

Process Model

Ensure the following Process Model settings are applied:

Process Model Setting	Value
Identity ^a	NetworkService
Idle Time-out (minutes)	0
Ping Enabled	False

a. For more information about identity, see [Application Pool Identity on page 239](#).

Rapid-Fail Protection

Rapid-Fail Protection must be disabled:

Rapid-Fail Protection Setting	Value
Enabled	False

Recycling

Recycling must be disabled.

Recycling Setting	Value
Regular Time Interval (minutes)	0

Application Pool Identity

Select **App Pool Identity** as the predefined security account, or use another account that has least privileges.

Caution: Do not assign the Local System account as the identity account. This account has elevated privileges and can pose a significant security risk.

It is recommended that you use the Network Service account combined with impersonation, which allows the worker process to use the credentials of a domain user for file or disk group access. The impersonation account should be a user with rights to the domain to allow NTFS file security. When using domain authentication, the impersonated account requires the Account Operator right for the domain.

For high-security deployments, follow Microsoft best practices. Information about creating a custom least-privileged service account is available in the Microsoft article titled "How To: Create a Service Account for an ASP.NET 2.0 Application," available at the following address: <http://msdn2.microsoft.com/en-us/library/ms998297.aspx>

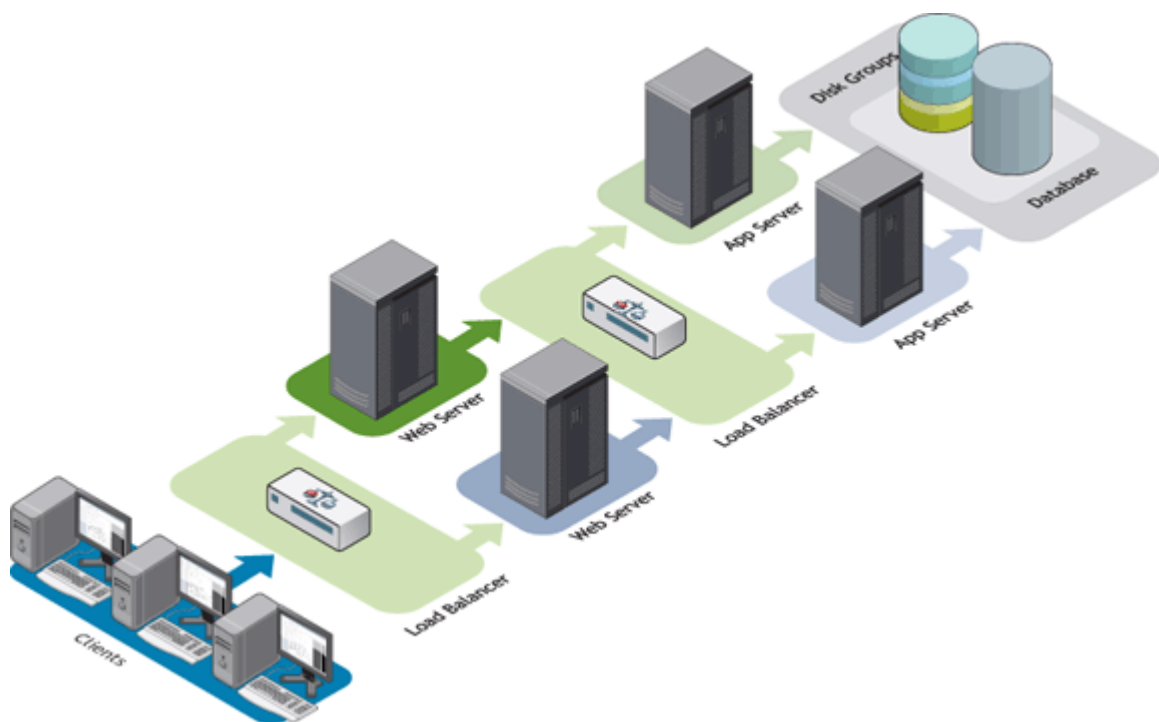
For file and folder permissions required with .NET 4.5, see "ASP.NET Required Access Control Lists (ACLs)," available at: <http://msdn.microsoft.com/en-us/library/kwzs111e.aspx>

Load Balancing

The OnBase Web Server supports load-balancing configurations for server farms. To configure and learn about load-balanced deployments, see the following topics:

- [Installing the OnBase Servers on page 240](#)
- [Configuring the Load Balancer on page 241](#)
- [Configuring the Web Server for Load Balancing on page 242](#)
- [Sample Load-Balancing Configurations on page 244](#)
- [Exceptions on page 250](#)

Note: In the following topics, **AppNet** refers to a Web Server virtual directory, and **AppServer** refers to an Application Server virtual directory. This convention is used to prevent confusion between the OnBase server applications and the server machines where they are installed.



Installing the OnBase Servers

Before configuring load balancing, ensure the AppNet (Web Server) directories and AppServer (Application Server) directories are correctly installed. The AppNet and AppServer directories can reside either on the same server or on different servers. To view diagrams of load-balancing configurations, see the following topics:

- [Load Balancing Across Web Servers Only: Single-Server Scenario on page 245](#)
- [Load Balancing Across Web Servers Only: Split-Server \(Dual\) Scenario on page 246](#)
- [Load Balancing Across Application Servers Only on page 247](#)

- [Load Balancing Across Multiple Web Servers and Application Servers on page 248](#)
- [Load Balancing Across Web Servers Only: Many-to-One Scenario on page 249](#)
- [Load Balancing Web Server Modules on page 250](#)

Caution: Any device or software placed between the Application Server and Web Server must not inhibit, cache, or alter the data passed between them.

To configure the load balancer, see [Configuring the Load Balancer on page 241](#). To ensure load-balanced requests are routed properly, see [Configuring the Web Server for Load Balancing on page 242](#).

Configuring the Load Balancer

The load balancer must support cookie-based or IP-based load balancing, which are sometimes referred to as layer-3, layer-4, or layer-7 load balancing. Hardware load-balancing devices are recommended. Software solutions, such as Microsoft's Network Load Balancing service, are also supported.

Note: Some modules are not supported with both cookie-based and IP-based load balancing. See [Module-Specific Load Balancer Requirements on page 241](#).

User-specific session state information must be maintained for each individual browser session within IIS's Web application memory. To maintain users' session state information, the load balancer must be configured to maintain a **persistent session** (also called client affinity or "sticky sessions") with a specific server. When properly configured, client affinity forces the load balancer to direct all connections for each Web session to the same server machine that originally logged in the user.

For session persistence to work correctly in a cookie-based load balancing environment, the load balancer must generate the cookie used to determine which server the requests are delivered to. Using the ASP.NET_SessionID cookie for cookie-based load balancing is not supported and will produce errors if the request is generated on one server and then processed on a different server. OnBase supports RFC 2109 or RFC 2965-based cookies. Any cookies defined by load balancers must be in either of these formats to work correctly.

For more information about client affinity (or persistence), consult the load balancer's documentation.

Note: Failover clustering of logged-in sessions is not possible due to session state persistence on the IIS Web server.

Module-Specific Load Balancer Requirements

Some modules are supported only with a specific type of load balancing. See [OnBase Servers on page 242](#) and [Application Enabler on page 242](#).

OnBase Servers

For load balancers placed between two OnBase servers, use only cookie-based load balancing. This recommendation applies to the following servers:

- Application Server
- Gateway Caching Server
- Web Server

For example, only cookie-based load balancing should be used between the Web Server and Application Server.

Load balancing between client workstations and the Web Server can be either cookie-based or IP-based.

Application Enabler

In Application Enabler, contexts that use the following modules are supported only with IP-based load balancing:

- DeficiencyPop
- FolderPop

Other Application Enabler contexts are supported with both cookie-based and IP-based load balancing.

Configuring the Web Server for Load Balancing

The AppNet Web.config file contains settings that must be properly configured for load-balanced environments. Information about these settings is provided in the following topics:

- [Load Balancing Across Multiple Web Servers on page 242](#)
- [Load Balancing Across Multiple Application Servers on page 243](#)
- [If You Are Not Load Balancing Across Application Servers on page 243](#)

Load Balancing Across Multiple Web Servers

If there is a load balancer between the client workstations and the Web Server, then modify the **dmsVirtualRoot** setting in the Web Server's Web.config file.

1. In the Web Server's Web.config, locate the **dmsVirtualRoot** setting.
2. Modify the value to specify load balancer's hostname rather than the Web Server's.
For example, if the load balancer's hostname is **WebLoadBalancer**, then the **dmsVirtualRoot** setting would resemble the following:

```
<add key="dmsVirtualRoot" value="http://WebLoadBalancer/AppNet" />  
<add key="dmsOEMProductName" value="ECM System" />
```

Load Balancing Across Multiple Application Servers

When a load balancer is placed between the Web Server and Application Server, you must update the AppNet Web.config file. The following steps describe how to modify the **ApplicationServer** element to allow the Web Server and Application Server to communicate through a load balancer.

1. In the AppNet Web.config, locate the **ApplicationServer** element.
2. For the **Url** attribute, specify the load balancer's hostname. For example, if the load balancer is named **AppLoadBalancer**, then the **Url** would resemble the following:
`http://AppLoadBalancer/AppServer/Service.aspx`
3. Change the extension at the end of the **Url** to **.asmx**, as shown in the previous step.
4. Set the **ServiceClientType** attribute to **SOAP**. If a load balancer is placed between the Web Server and Application Server, ensure the following conditions are met:

When you are finished, the **ApplicationServer** element should resemble the following:

```
<Hyland.Services.Client>
  <!-- All Urls Must end with 'Service.rem' for Remoting or 'Service.aspx' for SOAP. -->
  <ApplicationServer Url="http://AppLoadBalancer/AppServer/Service.aspx" ServiceClientType="SOAP" />
```

If You Are Not Load Balancing Across Application Servers

If there is no load balancer between the Web Server and Application Server, then the **ApplicationServer** setting should specify a specific server. For example, if the AppServer directory is installed on a server named **ecmAppServer1**, then the **ApplicationServer Url** setting would resemble the following:

```
<Hyland.Services.Client>
  <!-- All Urls Must end with 'Service.rem' for Remoting or 'Service.aspx' for SOAP. -->
  <ApplicationServer Url="http://ecmAppServer1/AppServer/Service.rem" ServiceClientType="Remoting" />
```

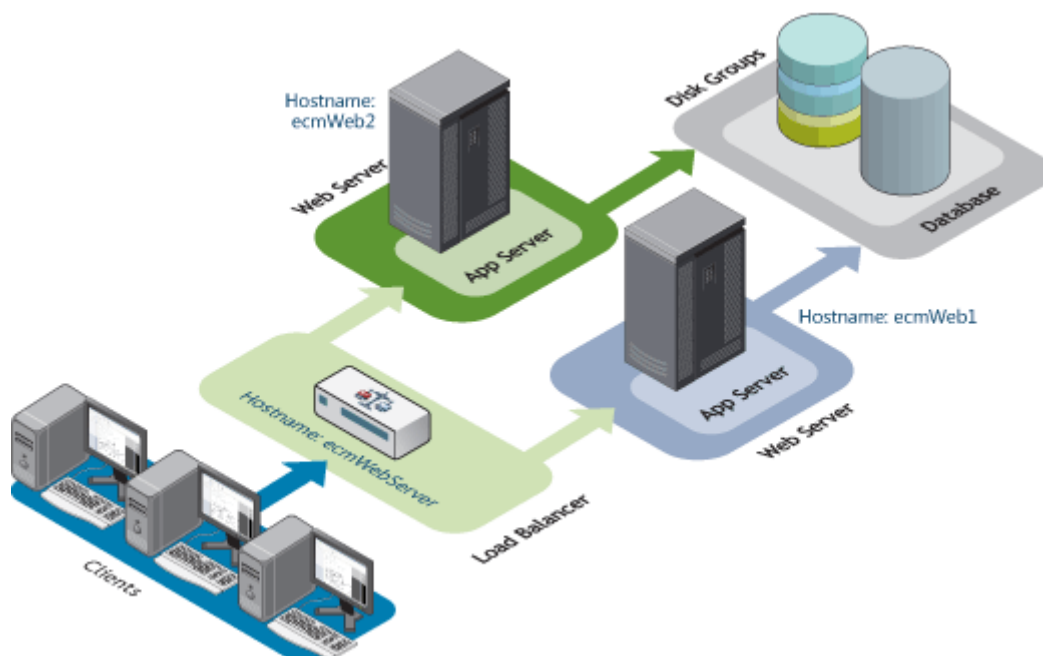
If both the Web Server and Application Server are installed on the same server machine, then **localhost** should be entered instead of the server's hostname.

Sample Load-Balancing Configurations

The Web.config values you provide will vary depending on your network configuration. For information about different deployment scenarios, see the following examples.

- [Load Balancing Across Web Servers Only: Single-Server Scenario on page 245](#)
A load balancer is in front of the Web Servers, and each Web Server is installed with an Application Server on the same server machine.
- [Load Balancing Across Web Servers Only: Split-Server \(Dual\) Scenario on page 246](#)
A load balancer is in front of the Web Server, but not in front of the Application Server. The Web Server and Application Server are installed on different server machines.
- [Load Balancing Across Application Servers Only on page 247](#)
A load balancer is in front of the Application Servers, but not in front of the Web Server.
- [Load Balancing Across Multiple Web Servers and Application Servers on page 248](#)
A load balancer is in front of the Web Servers, and another load balancer is in front of the Application Servers.
- [Load Balancing Across Web Servers Only: Many-to-One Scenario on page 249](#)
A load balancer is in front of the Web Servers, but not in front of the Application Server. All Web Servers are using the same Application Server, and the Web Servers and Application Server are installed on different server machines.
- [Load Balancing Web Server Modules on page 250](#)
Load balancers direct traffic from client machines to the Web Servers, and from the Web Servers to the Application Servers.

Load Balancing Across Web Servers Only: Single-Server Scenario



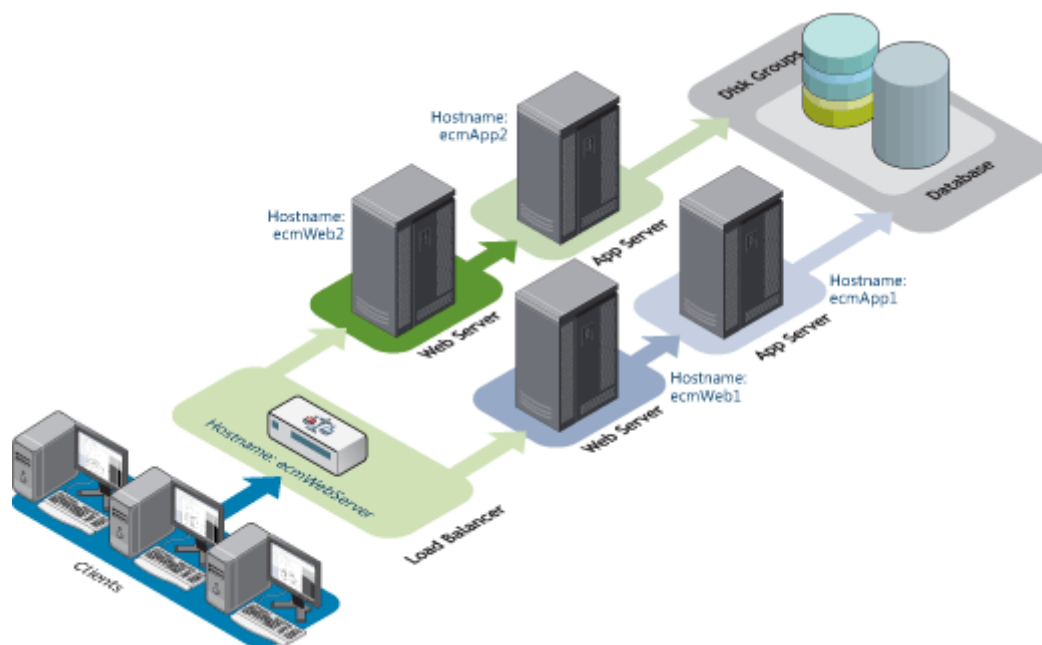
In this example, the Web Server (AppNet) and Application Server (AppServer) are on the same machine. The load balancer, **ecmWebServer**, balances only traffic between the clients and AppNet. On both **ecmWeb1** and **ecmWeb2**, AppNet communicates directly with the local AppServer. Traffic between the AppNet and AppServer directories is not load-balanced.

Web.config settings for each AppNet directory are provided in the following table. Because AppNet is on the same machine as AppServer, AppNet can specify **localhost** in the **ApplicationServer Url**. Refer to the diagram above for more hostname information.

Machine	AppNet Web.config Setting	Value
ecmWeb1	ApplicationServer Url	http:// localhost /AppServer/service.rem ^a
	dmsVirtualRoot	http:// ecmWebServer /AppNet
ecmWeb2	ApplicationServer Url	http:// localhost /AppServer/service.rem
	dmsVirtualRoot	http:// ecmWebServer /AppNet

a. Depending on the configured **ServiceClientType**, the service extension may be **.rem** or **.asmx**. For information, see page 51.

Load Balancing Across Web Servers Only: Split-Server (Dual) Scenario



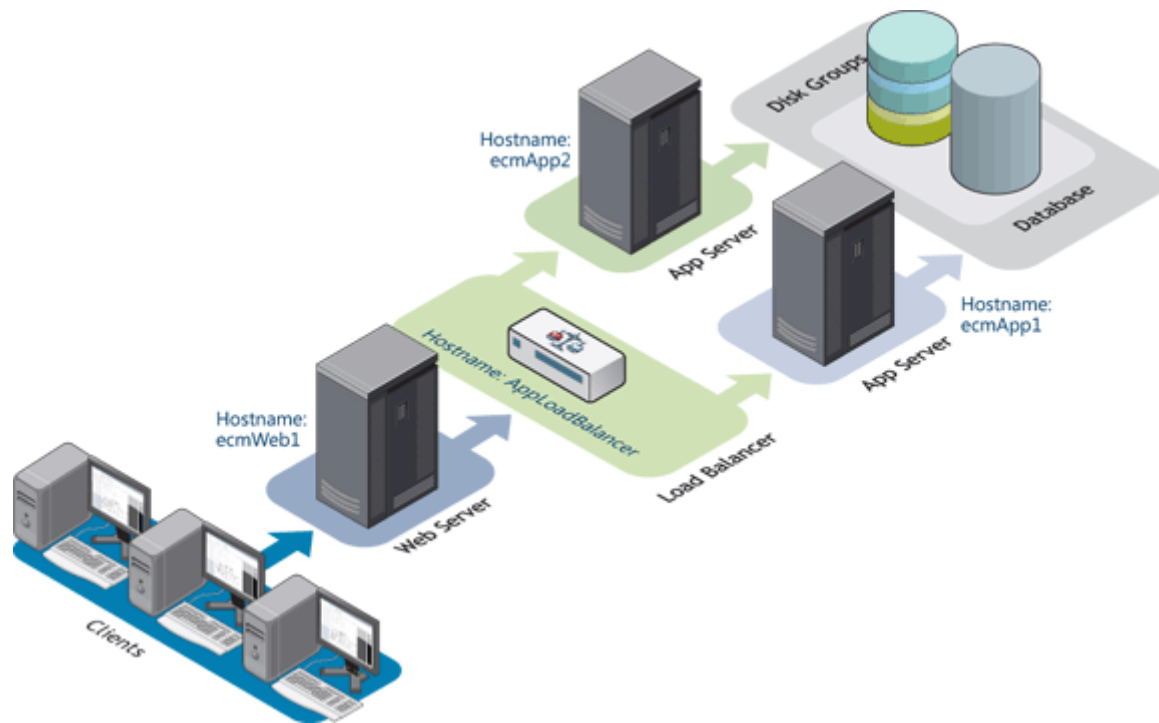
In this example, the Web Server (AppNet) and Application Server (AppServer) reside on separate machines. The load balancer, **ecmWebServer**, balances only traffic between the clients and AppNet. On **ecmWeb1**, AppNet communicates directly with the AppServer on **ecmApp1**. On **ecmWeb2**, AppNet communicates directly with the AppServer on **ecmApp2**. Traffic between the AppNet and AppServer directories is not load-balanced.

The Web.config settings for each AppNet directory are provided in the following table. Refer to the diagram above for more hostname information.

Machine	AppNet Web.config Setting	Value
ecmWeb1	ApplicationServer Url	http:// ecmApp1 /AppServer/service.rem ^a
	dmsVirtualRoot	http:// ecmWebServer /AppNet
ecmWeb2	ApplicationServer Url	http:// ecmApp2 /AppServer/service.rem
	dmsVirtualRoot	http:// ecmWebServer /AppNet

a. Depending on the configured **ServiceClientType**, the service extension may be **.rem** or **.asmx**. For information, see page 51.

Load Balancing Across Application Servers Only



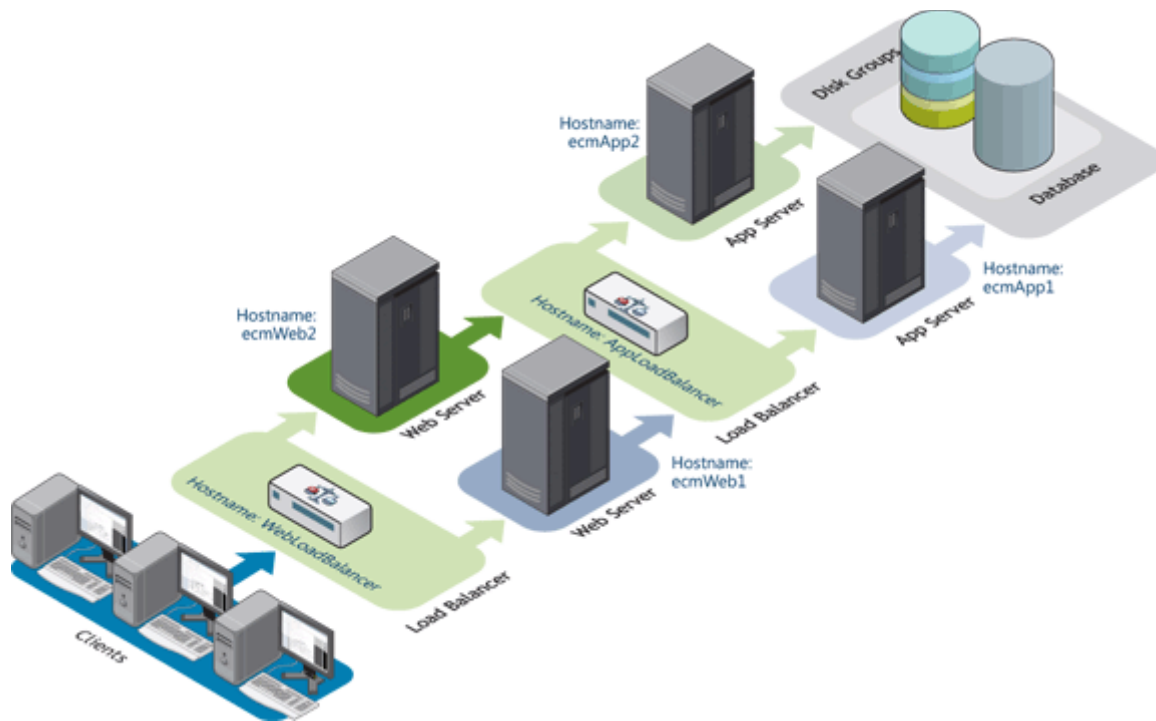
In this example, the Web Server (AppNet) is being load balanced across multiple Application Servers (AppServers). The load balancer is placed in front of the Application Servers only.

Web.config settings for the AppNet directory are provided in the following table. Refer to the diagram above for hostname information.

Machine	AppNet Web.config Setting	Value
ecmWeb1	ApplicationServer Url	http:// AppLoadBalancer /AppServer/service.asmx ^a
	dmsVirtualRoot	http:// ecmWeb1 /AppNet

a. Also ensure that the **ServiceClientType** attribute is set to **SOAP**.

Load Balancing Across Multiple Web Servers and Application Servers



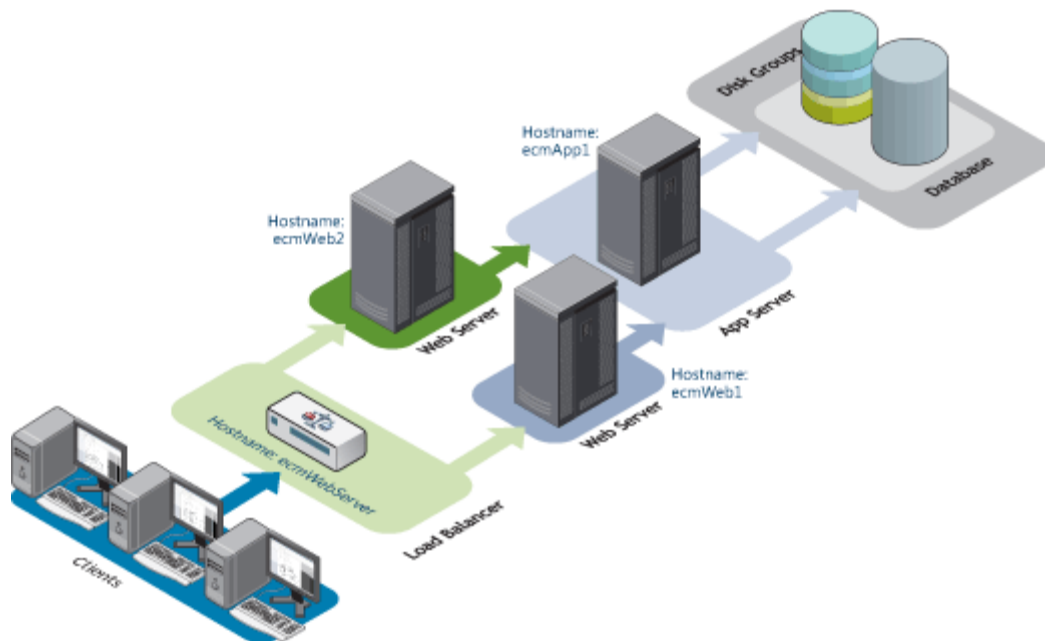
In this example, multiple Web Servers (AppNets) are being load balanced across multiple Application Servers (AppServers). Load balancers have been placed in front of the Web Servers and in front of the Application Servers.

Web.config settings for each AppNet directory are provided in the following table. Refer to the diagram above for hostname information.

Machine	AppNet Web.config Setting	Value
ecmWeb1	ApplicationServer Url	http:// AppLoadBalancer /AppServer/service.asmx ^a
	dmsVirtualRoot	http:// WebLoadBalancer /AppNet
ecmWeb2	ApplicationServer Url	http:// AppLoadBalancer /AppServer/service.asmx
	dmsVirtualRoot	http:// WebLoadBalancer /AppNet

a. Also ensure that the **ServiceClientType** attribute is set to **SOAP**.

Load Balancing Across Web Servers Only: Many-to-One Scenario



In this example, there are two Web Servers (AppNets) and two Application Servers (AppServer1 and AppServer2). Each AppNet directory resides on a separate machine, and both AppServer directories reside on another machine. Each AppNet directory communicates directly with a specific AppServer directory on **ecmApp1**. The load balancer, **ecmWebServer**, balances only traffic between the clients and AppNet directories. Traffic between the AppNet and AppServer directories is not load-balanced.

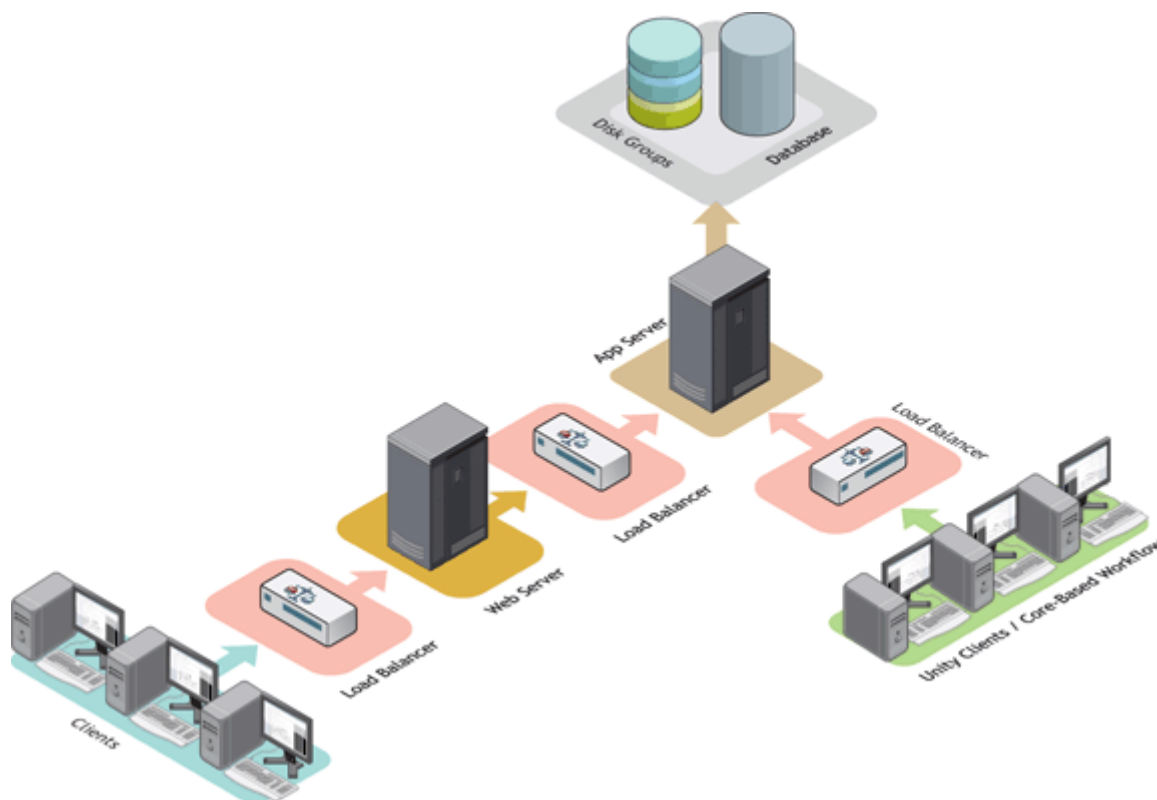
The Web.config settings for each AppNet directory are provided in the following table. Refer to the diagram above for more hostname information.

Machine	AppNet Web.config Setting	Value
ecmWeb1	ApplicationServer Url	http:// ecmApp1/AppServer1/service.rem ^a
	dmsVirtualRoot	http:// ecmWebServer/AppNet
ecmWeb2	ApplicationServer Url	http:// ecmApp1/AppServer2/service.rem
	dmsVirtualRoot	http:// ecmWebServer/AppNet

a. Depending on the configured **ServiceClientType**, the service extension may be **.rem** or **.asmx**. For information, see page 51.

Load Balancing Web Server Modules

The following graphic illustrates a possible setup, where Web Server users, Unity users, and Core-based Workflow users all access the Application Server through a set of load balancers.



Firewalls and HTTPS connections both are supported in these scenarios. For information about configuring firewalls for OnBase applications, see [Firewall Port Requirements on page 7](#).

Exceptions

Most OnBase modules support load balancing across multiple Web Servers and Application Servers, but there are some conditions where load balancing is not supported. These conditions are listed below.

Modules not listed here are supported in a load-balanced environment.

Integration for Microsoft Search

The Integration for Microsoft Search supports load balancing across multiple Web and Application Servers for the purposes of retrieving and viewing documents.

The Integration for Microsoft Search does not support load balancing across multiple Application Servers for the purpose of crawling documents. The server performing the crawl cannot communicate with the Application Server through a load balancer.

Web.config Configuration

The Web Server's Web.config file is an XML file used to configure the Web Server and control its behavior and feature sets. The file contains plain text and resides in the top-level of the Web Server's virtual directory. To change features, edit the appropriate value, save and close the file, and restart IIS.

As an alternative, use the Web Application Management Console to edit Web.config settings. This console simplifies the process of modifying configuration settings for the OnBase Web Server and Application Server. See the **Web Application Management Console** module reference guide for more information.

Caution: Do not modify the Web Server web.config file while users are using modules or applications that rely on the Web Server. Saving changes to the web.config file causes the users to lose their sessions, and their applications will become unresponsive.

The majority of configurable settings fall within the following sections:

- appSettings - see [appSettings on page 251](#)
- Viewer Vars - see [Context Menu Overrides and Viewer Vars on page 263](#)
- Navigation Panel Configuration - see [Main Menu Panel Configuration on page 284](#)
- CustomValidation - see [Custom Validation on page 291](#)

appSettings

The **appSettings** section of the Web Server's Web.config file controls feature and function availability in the Web Client. The generic section controls general functionality, while later sections are divided out for specific functions. The generic options are listed below.

dmsDataSource - Enter the name of the data source that the Web Server uses.

dmsVirtualRoot - The host name and virtual directory that users enter in the URL to the login page. For example, if users enter **https://DMS.yourdomain.com/AppNet/login.aspx** to access the Web Client login page, then the dmsVirtualRoot key would look like the following:

```
<add key="dmsVirtualRoot" value="https://DMS.yourdomain.com/AppNet"></add>
```

Note: The host name provided in **dmsVirtualRoot** must not contain an underscore character (_). If the server's machine name contains an underscore character, use its IP address instead, or change the machine name. For information about valid host names, see the following Microsoft article: <http://support.microsoft.com/kb/101785>.

dmsOEMProductName - Do not modify.

ServerDesignation - The value entered here is displayed in the Web Client browser's title bar. Entering a value for ServerDesignation can help identify which server a user is accessing in a load-balanced environment.

default_domainname - The default domain name displayed/entered on Login.aspx when using Interactive User Authentication with Active Directory and LDAP authentication.

default_username - For testing purposes only.

default_password - For testing purposes only.

EnableAutoLogin - Set this value to **true** if LDAP, Active Directory - Enhanced, or Integration for Single Sign-On is configured as the authentication method for logging in to OnBase. This means the source of user credentials is not OnBase. If the configured authentication method is also set to require interactive authentication, where the user must provide a user name and password to log in, then the user must provide the expected credentials to log in to the Web Client when **EnableAutoLogin** is set to **true**.

Note: If logins from the OnBase Web Client should use a single sign-on store for the source of authentication credentials (even when OnBase is configured to use Active Directory - Enhanced), the **forceSSOAutoLoginOverDomain** setting must also be set to **true**.

Set **EnableAutoLogin** to **false** to require interactive authentication using Internal security, which requires the user to provide their OnBase user name and password to log in to the Web Client, even when LDAP, Active Directory - Enhanced, or Integration for Single Sign-On is set as the authentication method.

Internal security takes precedence over the configured authentication method, even when using Integration for Single Sign-On. This can be useful for environments where users may need to log in to OnBase with their own user name and password on a group workstation, or users do not have credentials for Active Directory or LDAP.

forceSSOAutoLoginOverDomain - Set this value to **true** when OnBase is configured for LDAP or Active Directory - Enhanced authentication but single sign-on should be used for authentication when OnBase is accessed using the Web Client.

If single sign-on is configured and **forceSSOAutoLoginOverDomain** is set to **false**, users must log in to the Web Client using the authentication method configured in the Directory Service Authentication settings (standard, LDAP, or Active Directory - Enhanced) with respect to the **EnableAutoLogin** setting.

CustomSSOAuthenticationFailurePage - If a single sign-on authentication failure occurs, the user is redirected to the URL entered for the **CustomSSOAuthenticationFailurePage** element. If this value is blank and a single sign-on authentication failure occurs, users are redirected to a standard error page.

LogoutClose - If this is set to **true**, when the user is logged out of the Web Client, the browser window closes automatically. If this is set to **false**, when the user is logged out of the Web Client, the login screen is displayed.

logoutRedirectURL - Allows users to be redirected to a specified URL upon clicking exit.

webtheme - For support of skins. Currently, the only valid value is **XP**.

Note: version_num - In earlier versions, this option controlled the version number of your OnBase system to display on the login page as well as on the title bar. This setting has been removed from the Web Server's Web.config file and the version number can now be found in **version.xml**, available in the Appnet directory within the build.

targetPage - Do not modify.

loginPage - Do not modify.

spicerCodeBase - Do not modify. Location of the **ViewSpicer.cab** file.

selectDebug - Reserved for future use.

defaultPrintRange - Used when printing non-OLE documents from the viewer. OLE documents, such as Microsoft Word documents, always use **All** as the default print range. There are four options available for this setting:

- **all** - Print the entire document by default.
- **currentPage** - Print the current page by default
 - This setting only applies when using the right-click command from the open document. When using the right-click command in the Document Retrieval list, the **Print Range** setting defaults to **All**.
- **#** - where # is a page number. Print the specified page number by default
- **#-#** - Where # is a page number. Print the specified page range by default.
 - Complex page ranges can be entered (works only in ActiveX client) such as "1,5-12,17,23-26". There is a limit of 25 separate ranges. If you enter a range that is invalid, the print dialog will default to printing the entire document. If you enter a complex page range that contains values that are out of range for the current document, the range will be corrected.

promptUserQueries - Set to **true** if the Web Client should prompt users for confirmation when they attempt to execute a standard Custom Query without entering any constraints. Set to **false** if users should be able to execute unconstrained standard Custom Queries without being prompted.

showQueueCounts - Set to **true** to enable queue counts in Workflow. Enabling queue counts may hinder system performance.

reselectDelta - In Workflow, after an ad-hoc task is performed, the ActiveX control attempts to reselect the document. The **reselectDelta** setting controls how many places before and after the previous index to search for the document.

textSearchAutoView - When set to **true**, external text searches that return one hit for one document will automatically display the document.

MaxResults - Set a numerical value to specify the maximum number of results displayed in a Document Search Results list. The default value is **1000**.

WorkflowMaxResults - Set a a numerical value to specify the maximum number of results displayed in a Workflow filter results list. The default value is **2000**.

KeywordPanelViewType - Valid values are **flat** and **button**. This setting controls how Keyword Type names and Keyword operators are displayed in the Web Client Keyword Panel.

- If the value is set to **flat**, then the Keyword Type names and operators use the same background as the rest of the Keyword Panel until the user places the pointer on them. When the pointer is placed on the Keyword Type names or operators, they are highlighted to indicate that they are active buttons.
- If the value is set to **button**, the Keyword Type names and operators are displayed as active buttons regardless of whether the pointer is placed on them.

EnableKeywordOperators - Set this value to **true** to make logical and comparative Keyword operators (e.g., AND, OR, >, <, <>) available in the Web Client, DocPop, and StatusView. Set this value to **false** to disable logical and comparative Keyword operators in these contexts.

- Keyword operators are enabled by default, but you may want to disable them as a troubleshooting measure to prevent users from submitting queries that return a large number of results and slow down the database server.
- Disabling Keyword operators can hinder users' ability to find documents. Ensure you understand the effects of disabling Keyword operators before doing so.
- This setting does not affect Custom Queries in the Web Client's Document context. For Custom Queries, the availability of Keyword operators is controlled by the **Value Operators** and **Binary Operators** settings in each Custom Query's configuration.

EnableSessionExpiration - When set to **true**, the end user will be logged out when no activity is detected. The length of inactivity is set by the **sessionState**'s time-out period, which has a default value of 20 minutes. You can change the time-out period in the Web Server's Web.config, as described under [sessionState Timeout on page 259](#).

PromptOnSessionExpire - If **EnableSessionExpiration** is set to **true**, the user will be presented with a warning, giving them 30 seconds to decide to keep the current session open or to close it. If the user does not respond, the user is logged out. The user will need to log into the OnBase system again.

DisplaySingleDocument - Turns on or off the ability to automatically open a document if only one document is returned in the Document Search Results list.

DisplayRelatedDocuments - A Workflow setting for displaying documents that are related to a queue from a folder. Valid values are **always**, **document**, and **never**:

- **always** - The Work Folder tab in Workflow will always display after a user selects a document in a queue.
- **document** - The Work Folder tab in Workflow will only display when a selected document in a queue has at least one related document.
- **never** - The Work Folder tab in Workflow will never display when a user selects a document in Workflow.

OverrideUILanguage - When set to the default value of **false**, the user interface language will be that of the client's locale setting. When set to **true**, the language select option becomes available on the login page, and the user can select the language they want to use for the UI.

DefaultUILocale - Used with **OverrideUILanguage**. When **OverrideUILanguage** is set to **true**, this option sets the behavior of the UI. When **DefaultUILocale** is set to **default**, the drop-down for the language appears. To have a specific language be the default, regardless of the locale setting of the computer, set **DefaultUILocale** to that language. For example, to have the UI set to German, you would set **DefaultUILocale** to **de**. For more information, see [Supported Translations and Formats on page 313](#).

Note: The **DefaultUILocale** does not affect currency and date formats. Currency and dates are displayed in the format set on the user's workstation.

NativeMailSystem - Specifies the primary email system. Set to **0** by default. Do not change this setting without assistance from your technical support provider.

autoDisplayNotePanelPDFOffice - This setting controls whether the **Notes** pane is expanded by default next to the document viewer when the user opens an OLE document such as a PDF or Microsoft Office document. If set to **true**, the **Notes** pane is displayed when a user opens an OLE document. If set to **false**, the **Notes** pane is collapsed when a user opens an OLE document.

A user can override this setting on their workstation with the client setting **Automatically Display The Note Panel When Viewing PDF and Office Documents** in user Preferences.

ClearDocumentTypeAfterImport and **ClearKeywordsAfterImport** - These settings control whether or not the Document Type or Keyword Type values are automatically cleared from the **Import Document** dialog box once a document is imported. By default, this setting is set to **false**.

Note: Nothing is cleared after the initial upload and preview generation. This could mean that if the queue is empty and you type in keyword data, it will be used (and not cleared).

If set to **true**, note the following:

- The clear is performed after the document import is complete, but only on the current keyword data in the queue. If there are other documents in the queue that already have keyword data, those documents are left alone.
- If you select a file with input, the file will get the keyword data that was already in the keyword panel.
- If you drag and drop multiple documents, each document gets the keyword data that was already in the keyword panel.

If set to **false**, nothing is cleared at any point. After the import is complete, the keyword data remains from the previous import. If there are other documents left in the queue that already have keyword data, they are left alone.

Note: This setting does not apply when more than one document is queued for import in the Web Client's **Pending Import** queue.

If a user modifies the **Clear Document Types After Import** or **Clear Keywords After Import** settings in the Web Client's **Client Settings**, their change overrides the Web.config setting and the change is persisted until the browser's cookies are cleared.

AlwaysGeneratePreviewAfterUpload - This setting controls whether or not a preview can be generated for the document.

When set to **true**, the **Show Preview** check box is always selected on the Import Document panel. When set to **false**, the **Show Preview** check box must be manually selected each time users import documents, in order to preview image documents.

Note: Previews of image documents are only displayed when using Safari, Firefox, or Internet Explorer 11. Previews are not displayed for PDF documents larger than 100 MB.

WebClientType - This setting controls whether the ActiveX Web Client or HTML Web Client is used. See [Configuring the Web Client Type on page 258](#).

RememberHitListHeight - When this setting is set to **true**, then changes users make to the height of the Document Search Results list are remembered between Web Client sessions. If this setting is set to **false** in Web.config, the new height is respected only for the life of the current browser window.

NumDisplayedDocumentTypes - This setting controls the number of document types displayed in the **Document Types** select box in Document Retrieval mode. This setting also controls the height of the **Document Types** select box. The default value is **6**. Recommended values are between **1** and **30**.

CollapseCheckSelect - This setting controls whether CheckSelect list controls load initially in a collapsed or expanded state. CheckSelect list controls include the list of Document Types in the Web Client's Document Retrieval layout. When **CollapseCheckSelect** is set to **true**, the CheckSelect list controls load in a collapsed state. When set to **false**, the CheckSelect list controls load in an expanded state.

AllowViewSource - This setting controls whether the browser context menu, or right-click menu, is available in the Web Client. When **AllowViewSource** is set to **true**, users can access the **View Source** right-click option within the Web Client. When set to **false**, the browser context menu is not available. This setting also affects Web Client contexts like StatusView, Workflow, and WorkView.

Note: Even when **AllowViewSource** is **true**, the browser context menu is not available from all components, such as the Document Search Results list and the Document Viewer.

InternalMailTimerSeconds - This setting controls how often the Web Client check for new Internal Mail messages if the Notify on New Mail user option is selected. The default value of 300 is the minimum allowed value.

KeywordDropDownTypeaheadCharacterMinimum - This setting controls how many characters must be entered before the typeahead option is enabled on a keyword drop-down field. For example, if 5 characters must be entered for keyword 110 before the typeahead drop-down is enabled, enter 110:5 as the value.

WindowsServerLocaleFormat - This setting controls which version of Windows Server locale formats to use for data validation in the Web Client. Because the default locale formats may differ between versions of Windows Server, this setting allows an administrator to specify which Windows Server version's locale formats to use to display and validate values such as numbers, currency, dates, and times. The Web Server does not need to be running on the Windows Server version specified in this setting.

If this setting is blank, the Web Server automatically detects the version of Windows Server running the Web Server and uses that version's locale formats.

MaxImportQueueSize - This setting controls the maximum number of documents that a user can queue for import at one time. This value can be 1–25.

Note: The EDM Services license is required to import multiple documents at one time.

EnableDesktopHost - This setting controls whether the Web Client can communicate with the Hyland Desktop Host. The default value is **true**.

EnableBrowserPdfViewer - This setting controls whether the Web Client uses the web browser's PDF viewer or the Web Client's PDF viewer to display PDF documents. You can also allow the user to choose which PDF viewer to use.

- If set to **true**, PDF documents are displayed using the PDF viewer configured for the web browser. This PDF viewer may be the built-in PDF viewer for the browser or a browser extension, depending on the configuration of the browser.
- If set to **false**, PDF documents are displayed using the Web Client PDF viewer. The Web Client PDF viewer allows users to use standard Document Viewer toolbar and right-click functionality, such as applying notes and annotations to specific positions.
- If set to any other value (including no value), the user can choose which PDF viewer to use with the client setting **Open PDF Documents Using The Web Browser's Configured PDF Viewer** in user preferences.

Note the following:

- The setting **Open PDF Documents Using The Web Browser's Configured PDF Viewer** is unavailable in the Web Client user preferences if **EnableBrowserPdfViewer** is set to **true** or **false**.
- Password-protected PDF files cannot be viewed with the Web Client PDF viewer. The web browser's configured PDF viewer is used to display password-protected PDF files.

Configuring the Web Client Type

The **WebClientType** web.config setting specifies whether the ActiveX or HTML Web Client is used.

The ActiveX Web Client is only available in Internet Explorer. If a user accesses the login page using a browser other than Internet Explorer, the login page automatically redirects the user to the HTML Web Client. This redirection happens even when the **WebClientType** is set to **activex** or **selectable**.

This behavior ensures that users in a mixed-browser environment can access the application through the same virtual directory.

Caution: Do not modify the Web Server web.config file while users are using modules or applications that rely on the Web Server. Saving changes to the web.config file causes the users to lose their sessions, and their applications will become unresponsive.

To configure the Web Client type:

1. Open the **web.config** file of the Web Server for editing in a plain-text editor. In a default installation, the **web.config** file is located at **C:\inetpub\wwwroot\AppNet**.
2. Locate the **WebClientType** key under the **appSettings** element.
3. Set the **value** attribute in the **WebClientType** key with one of the following values:

Value	Description
activex	This setting enables the ActiveX Web Client. The ActiveX Web Client is only available in Internet Explorer.
html	This setting enables the HTML Web Client.
selectable	For users logging in interactively using Internet Explorer, this setting allows the user to choose on the login page which type of Web Client to use.

4. Save and close the **web.config** file.

sessionState Timeout

Sessions for OnBase Web applications, such as the Web Client, can be configured to time out after a period of inactivity. This time-out period ensures that Client licenses are not held unnecessarily, and it helps enforce a more secure OnBase environment.

The session time-out is configured in the Web Server's Web.config. It is set to 20 minutes by default, as shown below:

```
<sessionState mode="InProc" stateConnectionString="tcpip=127.0.0.1:42424"
sqlConnectionString="data source=127.0.0.1;Trusted_Connection=yes" cookieless="false"
timeout="20"/>
```

To specify a different interval, edit the **timeout** value to reflect the number of minutes an inactive Web Client session should remain open. The minimum value is **1**. To disable session expiration, set **EnableSessionExpiration** to **false**. This setting is also configured in the Web Server's Web.config under **appSettings**.

Note: The OnBase Web Server supports only in-process (**InProc**) mode for its session state settings.

maxconnection

The **maxconnection** setting specifies the number of outbound requests the Web Server can send simultaneously before requests are queued. For example, if the Web Server needs to send 10 requests to the Application Server, but the **maxconnection** is set to **1**, then all of the requests must wait for the previous request to finish before the next one can be sent. The default value for **maxconnection** is **24**.

If you think you are having connection queuing issues that are hindering performance, contact a Technical Support representative for assistance.

httpRuntime

The **httpRuntime** element in the Web Server's Web.config defines size and timeout settings for HTTP requests. You may need to increase these settings if users need to import large files through the Web Client.

The following example displays default **httpRuntime** settings.

```
<httpRuntime requestValidationMode="2.0" maxRequestLength="4096"
executionTimeout="90"/>
```

maxRequestLength controls the maximum request size allowed for a file upload. This value is represented in kilobytes, and the default is 4096 KB (4 MB). If users need to upload files larger than 4096 KB, you may need to increase the **maxRequestLength** value.

- The **maxRequestLength** setting specifies the maximum request size, not the maximum file size. When a file is sent from the Web Client to the Application Server, the request size is larger than the file size due to encoding. The Application Server's default **maxRequestLength** size is 30,000 KB.
- Standard document import in the Web Client allows import of files that are larger than the **maxRequestLength** size, because the file's binary data is split into smaller segments for import. This means that adjusting the **maxRequestLength** is not required for importing large files using standard document import in the Web Client, but it may be required for other import methods in the Web Client (such as importing through Workflow or other modules).
- For information about accommodating file uploads in IIS, see [maxAllowedContentLength on page 260](#).

executionTimeout defines the maximum period allowed for a request to execute. This value is represented in seconds, and the default is 90 seconds. If users frequently see **Request timed out** messages, or if they are viewing/uploading large documents, the **executionTimeout** value may need to be increased for proper processing. Document uploading may also exceed the timeout period due to heavy disk group activity.

Note: If you intend to export PCL documents to PDF, the **executionTimeout** value must be set to a larger number than 300. The recommended value is **86000**. This allows an export to succeed without timing out.

The **requestValidationMode** setting is present for internal use. Do not modify this setting.

maxAllowedContentLength

The **maxAllowedContentLength** setting allows the Web Server to override a security feature in IIS that prohibits requests over 30 million bytes (about 28.6 MB). This request filtering feature is enabled by default in IIS. To allow users to upload files that exceed the default request limit, you must complete the steps below, keeping the following in mind:

- The **maxAllowedContentLength** must be updated in both the Web Server and Application Server's web.config files.
- The Application Server's setting may need to be larger than the Web Server's because the request sent to the Application Server is larger than the request sent to the Web Server. See the following point.
- Request size does not mean file size. When a file is sent from the Web Client to the Web Server to the Application Server, the request size increases due to encoding. The increase amount varies depending on whether the Web Server is using SOAP to communicate with the Application Server. Requests sent using SOAP are larger than requests sent using remoting.
- If a user uploading a file receives a **404** error in the Web Client's navigation panel, then the Web Server's **maxAllowedContentLength** must be increased.

- If the Web Server logs an error stating “The remote server returned an error. (404) Not Found,” then the Application Server’s **maxAllowedContentLength** is not large enough; its **maxRequestLength** may not be large enough either.
- The **maxAllowedContentLength** doesn’t override the **maxRequestLength**, which specifies the Web Server’s maximum size for a file upload. If you change **maxAllowedContentLength**, you may also need to change the **maxRequestLength** value to accommodate larger files. The **maxAllowedContentLength** should exceed the **maxRequestLength**.

Follow these steps to increase the size of requests that the Web Server and Application Server can handle.

1. In the Web Server’s Web.config, locate the **security** element, which contains the **maxAllowedContentLength** setting. Change the **maxAllowedContentLength** to the appropriate value, in bytes.
2. Check the **maxRequestLength** to ensure that it accommodates the intended file size and is less than the **maxAllowedContentLength**.
Keeping the **maxRequestLength** less than the **maxAllowedContentLength** ensures that a logical error message is displayed to users when their upload attempts exceed the Web Server’s maximum file size to upload.
3. Perform the same steps in the Application Server’s Web.config.

Note: When modifying the **maxAllowedContentLength** setting in the Application Server’s Web.config file, the **security** element must first be uncommented. See the **Application Server** module reference guide for more details.

X-Frame-Options

The **X-Frame-Options** setting defines the value of the X-Frame-Options response header added to HTTP communication from the Web Server. This setting controls how a browser displays pages that contain embedded content such as in a frame or iframe.

For security purposes, this setting is set to **SAMEORIGIN** by default, which requires that the page and the embedded content must come from the same domain. If your solution includes embedding content from the Web Server into a different domain, you can change this setting to allow embedding Web Server content into a specified URI. For more information on configuring the X-Frame-Options header, consult an HTTP reference.

Note: Allowing embedded content from another domain only works on browsers that support the ALLOW-FROM directive of the X-Frame-Options header. Consult an HTTP reference to see how each browser in your solution supports the X-Frame-Options header.

cookieSameSite

The **cookieSameSite** setting in the **sessionState** element defines the behavior of cross-site cookie security in the Web Server. This setting controls the SameSite security attribute of cookies sent from Web Server, which affects whether the web browser allows Web Server content that is embedded in a parent page or application that is hosted from a different site or domain.

Caution: Do not modify the **cookieSameSite** setting except for deployments that absolutely require hosting the Web Server and the parent page or application from different domains. It is considered a best practice to host the Web Server and the parent page or application from the same domain if possible.

The **cookieSameSite** setting has the following possible settings:

Setting	Description
Strict	<p>This setting restricts all cross-site requests for Web Server content. The Web Server does not send cookies for top-level navigation that is triggered from a domain other than that of the Web Server.</p> <hr/> <p>Caution: The Strict setting can negatively affect browsing experience in solutions that rely on cross-site cookies for top-level navigation. For example, users logged into the Web Client would be required to re-authenticate when following a DocPop link.</p> <hr/>
Lax	<p>This setting limits cross-site requests for embedded Web Server content. The Web Server sends cookies for top-level navigation, but not for content embedded in an image or frame.</p> <p>This is the default setting.</p>
None	<p>This setting allows cross-site requests for embedded Web Server content to be accepted by the browser. Use this setting if your solution requires embedding Web Server content in a page or application hosted on a different domain.</p> <p>If this setting is used, you must also use an HTTPS connection for the Web Server. Requests sent through an HTTP connection are treated by the browser as SameSite=Lax, which prevents embedded Web Server content.</p>

Context Menu Overrides and Viewer Vars

The **Context Menu Overrides** and **Viewer Vars** sections allow you to customize the available options, and to control what users see in the Web Client. With these settings, administrators can fine-tune the Web Client display settings as needed. A complete listing of the available options follows.

addNoteMenu - When set to **true**, the **Notes | Add Note...** right-click option is available in both the ActiveX and HTML document viewers. When set to **false**, the option is not available.

documentPropertiesMenu - When set to **true**, the **Properties** right-click option is available in both the ActiveX and HTML document viewers. When set to **false**, the option is not available.

fileMenu - When set to **true**, the **Send To | File...** right-click option is available in both the ActiveX and HTML document viewers. When set to **false**, the option is not available in either document viewer.

historyMenu - When set to **true**, the **History** right-click option is available in both the ActiveX and HTML document viewers. When set to **false**, the option is not available.

keywordsMenu - When set to **true**, the **Keywords** right-click option is available in both the ActiveX and HTML document viewers. When set to **false**, the option is not available.

printMenu - When set to **true**, the **Print...** right-click option is available in both the ActiveX and HTML document viewers. When set to **false**, the option is not available in either document viewer.

reindexMenu - When set to **true**, the **Re-Index** right-click option is available in both the ActiveX and HTML document viewers. When set to **false**, the option is not available in either document viewer.

workflowMenu - When set to **true**, the **Workflow** right-click option is available in both the ActiveX and HTML document viewers. When set to **false**, the option is not available in either document viewer.

Context Menu Overrides for the HTML Only Viewer

sendToPrintQueueMenu - When set to **true**, the **Send To | Server Print Queue** right-click option is available in the HTML document viewer. When set to **false**, the option is not available.

Context Menu Overrides for the ActiveX Viewer

clipboardMenu - When set to **true**, the **Send To | Clipboard...** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

firstPageMenu - When set to **true**, the **Navigate | First Page** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

gotoPageMenu - When set to **true**, the **Navigate | Go To Page...** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

lastPageMenu - When set to **true**, the **Navigate | Last Page** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

mailRecipientMenu - When set to **true**, the **Send To | Mail Recipient** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

nextPageMenu - When set to **true**, the **Navigate | Next Page** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

pagesMenu - When set to **true**, the **Toolbars | Pages** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

previousPageMenu - When set to **true**, the **Navigate | Previous Page** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

savetofileMenu - When set to **true**, the **Send To | Create New Document** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

textSearchMenu - When set to **true**, the **Toolbars | Text Search** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

viewerControlMenu - When set to **true**, the **Toolbars | Viewer Control** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

zoomInMenu - When set to **true**, the **Scale | Zoom In** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

zoomOutMenu - When set to **true**, the **Scale | Zoom Out** right-click option is available in the ActiveX document viewer. When set to **false**, the option is not available.

Viewer Vars

Note: Unless otherwise noted, settings in the Viewer Vars section apply only to the ActiveX Web Client.

Note: Settings that enable or disable right-click options only determine whether the options are available from the ActiveX document viewer. Right-click menu options remain available from the Document Search Results list even when set to **false**.

gotoPageOR - Sets the default page to be displayed in the ActiveX and HTML Web Clients for image, text, and PCL documents. For example, if documents should be opened to the second page by default, change this setting to **2**. The default setting is **0**, which opens documents to the first page. If a user opens a document that has fewer pages than the **gotoPageOR** number, the following message is displayed to the user: **This document only has x page(s)**.

overlayOR - When this setting is left blank (default), the Document Type's overlay configuration controls the display of overlays. Set the value to **true** or **false** to override the overlay configuration and cause all overlays to be displayed default on or off, respectively, in the ActiveX and HTML Web Clients. If no overlay is available for a Document Type, then no overlays will be displayed on those documents in the Web Client.

Note: If the overlay display is set to **Required** for a Document Type in Configuration, and **overlayOR** is set to **False**, then the overlay won't be displayed in the viewer and the user won't be able to display it. This occurs because the **Required** setting disables the **Overlay** button. The **overlayOR** setting has no effect on the availability of the **Overlay** button. Verify these settings are configured to work together to exhibit the intended behavior.

zoomLevelOR - This setting allows you to set the default zoom level for documents opened from the ActiveX and HTML Web Client. If no value is specified, the Web Client displays documents at the last zoom level at which the user viewed a document. The following options are available:

- **actualsize** - Sets the default zoom level to 100%.
- **fittowindow** - Sets the default zoom level to Fit in Window, which scales the document to the size of the viewer.
- **fittowidth** - Sets the default zoom level to Fit Width, which scales the document to fit its width in the viewer.
- **zoomrect** - Scales the document to display the rectangle defined by the **rectLeftOR**, **rectRightOR**, **rectTopOR**, and **rectBottomOR** parameters.

rectLeftOR - When using the **zoomrect** option for **zoomLevelOR**, this is the pixel position of the left border.

rectRightOR - When using the **zoomrect** option for **zoomLevelOR**, this is the pixel position of the right border.

rectTopOR - When using the **zoomrect** option for **zoomLevelOR**, this is the pixel position of the top border.

rectBottomOR - When using the **zoomrect** option for **zoomLevelOR**, this is the pixel position of the bottom border.

Disable Context Menu

DisableContextMenu - When set to **true**, right-click options are unavailable from the document viewer, and the document options toolbar is unavailable from the OLE document viewer. When set to **false**, right-click options are available from the document viewer, and the document options toolbar is available from the OLE document viewer.

The HTML and ActiveX Web Clients both respect this setting in the full version of the Web Client and in DocPop and FolderPop, but the setting affects the document viewer only. It does not affect the Document Search Results list or other locations where documents are listed. Right-click options will remain available from document select lists when **DisableContextMenu** is set to **true**.

Viewer Vars for the HTML Only Viewer

PreventViewerClientCaching - This setting controls whether or not the following items are cached to the Temporary Internet Files folder on the user's workstation:

- Documents in the HTML Web Client Document Viewer¹
- Note, Folder, Document Type, and Workflow Life Cycle icons

To prevent the caching of these items, set **PreventViewerClientCaching** to **true**.

When this setting is set to **false**, documents in the HTML Document Viewer are cached on the workstation for five minutes, and icons are cached for seven days. When these items expire, they must be re-requested from the server.

Note: Setting **PreventViewerClientCaching** to **true** may impact HTML viewer performance.

KeywordDropdownTypeaheadCharacterMinimum - This setting allows the user to specify the minimum number of characters that must be typed before typeahead is enabled on a keyword drop-down field. For example, if the value is 112:8,125:6, this means that eight characters must be entered for keyword 112, and six characters must be entered for keyword 125 before typeahead is enabled on those keyword fields.

Viewer Vars for the ActiveX Viewer

autoOrientPrinting - When this setting is **true**, if an image document is wider than it is tall, printing will default to landscape mode. If the image document is taller than it is wide, printing will default to portrait mode. Auto-orientation is applied on a page-by-page basis to image documents. Also, the default print format is ignored, and the user cannot change the **Orientation** setting using the **Print** dialog box. When this setting is **false**, the default print format is respected.

ActiveX Viewer Toolbars

You can configure the ActiveX Viewer Toolbars section to enable or disable toolbars for the ActiveX document viewer. When a toolbar is enabled, a user can turn it on or off using the **Toolbars** right-click menu. When a toolbar is disabled, the toolbar is removed from the document viewer and from the **Toolbars** right-click menu. By default, all toolbars are enabled and displayed in the ActiveX document viewer.

Note: If you enable a toolbar that has been disabled, the toolbar is not automatically displayed in the document viewer. To display a toolbar that has been re-enabled, a user must select it from the **Toolbars** right-click menu.

enableViewerControlToolbar - When set to **true**, the Viewer Control toolbar is enabled. When set to **false**, the toolbar is disabled.

1. This applies to documents that are rendered into images in the HTML Web Client's document viewer. OLE documents are cached for five minutes regardless of this setting's configured value.

enableThumbnailPages - When set to **true**, the Pages toolbar is enabled. When set to **false**, the toolbar is disabled.

Note: This setting is also respected in the HTML Web Client.

enableAnnotationToolbar - When set to **true**, the Annotation toolbar is enabled. When set to **false**, the toolbar is disabled.

Note: This setting is also respected in the HTML Web Client.

enableNoteToolbar - When set to **true**, the Notes toolbar is enabled. When set to **false**, the toolbar is disabled.

Thumbnail Auto Zoom Configuration

autoZoomThumbnail - When set to **true**, the thumbnail toolbar's auto zoom feature is enabled by default and cannot be disabled by the user. When set to **false**, the feature is disabled and cannot be enabled by the user. When set to **local**, the feature is dependent upon whether the setting was enabled by the user (**Viewer Options | Enable Thumbnail Zoom** check box is checked or unchecked.) The default setting is **local**.

Security Keywords

AllowSecurityKeywordsAdmin - When **AllowSecurityKeywordsAdmin** is set to **true**, an administrator can assign Security Keywords through the Web Client's Admin context. When **AllowSecurityKeywordsAdmin** is set to **false**, Security Keywords are unavailable in the Web Client's Admin context.

Document Select Vars

enableRowColoring - When this option is set to **true**, alternating rows in data grids within the Web Client are shaded, making it easier to distinguish one result from others in a list. When set to **false**, all rows in data grids within the Web Client have the same background color. Examples of data grids include Document Select lists, External Text Search results lists, and the User Mailbox. This setting applies to both the ActiveX Web Client and the HTML Web Client.

If this setting is undefined, the Web Client will default to the user-defined setting for **Enable Row Coloring** under **User | Client Settings | Document Select List**.

Enabling Blocked or Overridden Function Keys

AllowedFunctionKeyList - This setting allows you to enable function keys that are normally blocked or overridden in the Web Client. Specify values for the function keys to enable, for example:

```
<add key="AllowedFunctionKeyList" value="F7,F8,F9" />
```

Allowing Insecure Connections

AllowInsecureConnection - This setting controls whether or not the server will only accept https:// connections, or if it will accept both http:// and https:// connections. By default, this setting is set to **false**.

To only allow https:// connections to the server, this setting should be set to **false**.

To allow both http:// and https:// connections to the server, this setting should be set to **true**.

Note: If **AllowInsecureConnection** is set to **false**, then the server must be correctly configured for HTTPS connections.

EnableLegacyChecksumFallback

This setting is used to provide support for legacy checksums in Pop integration URLs. Legacy checksums are created in versions of OnBase prior to version 14, created without using a unique string value as a checksum key, or created from a current version of OnBase that has the **EnableLegacyChecksumCreation** option in the Application Server web.config file set to **true**. By default, this setting is set to **false**.

Set **EnableLegacyChecksumFallback** to **true** in order to allow legacy checksums to be validated.

If this option is set to **false**, then legacy checksums will not validate and users will be unable to view documents whose generated URLs contain a legacy checksum. If this option is set to **false**, then **EnableLegacyChecksumCreation** must also be set to **false**.

EnableLoginAutocomplete

This setting controls whether or not to allow autocomplete to function in the fields on the login screen. By default, this setting is set to **false**.

Set **EnableLoginAutocomplete** to **true** to enable autocomplete on the login page.

Folder Window Vars

The following settings define the default parameters of the Folders window in the OnBase Web Client and FolderPop. Users can resize and collapse panes in the Folders window as needed. User adjustments are maintained across sessions on a per-user, per-workstation basis.

FolderTreeWidth - Set the width of Folder Tree pane. The must be a percentage. For example, value="30%".

FolderTreeHeight - The value can only be in percentages. The sum of FolderTreeHeight, DocumentListHeight and FolderListHeight must be equal to 100%

DocumentListHeight - The values can only be in percentages. The sum of FolderTreeHeight, DocumentListHeight and FolderListHeight must be equal to 100%

FolderListHeight - The values can only be in percentages. The sum of FolderTreeHeight, DocumentListHeight and FolderListHeight must be equal to 100%

DocPop Vars

DocPop-specific settings are located in the **Hyland.Web.DocPop** element of the Web Server's Web.config file. The only required setting is a data source. You can either configure one in the Web Server's Web.config or pass it along the query string. DocPop results can be displayed using the HTML or ActiveX Web Client.

The following settings are located in the **Hyland.Web.DocPop** element of the Web Server's Web.config file.

username - Enter the user name to use with default login for DocPop, if you want to use a single user account for When **enableDefaultLogin** is set to **true**, users can automatically log on to DocPop using the credentials provided in the **username** and **password** settings.

password - Enter the password to use with default login for DocPop, if you want to use a single user account for access. When **enableDefaultLogin** is set to **true**, users can automatically log on to DocPop using the credentials provided in the **username** and **password** settings.

datasource - Enter the name of the data source to use with DocPop. This is a required value.

domain - Enter the domain to log on to if you are using Active Directory authentication.

embedded - Set this to **true** when you are embedding DocPop results in a custom Web page and you want the DocPop results to be displayed in a frame or iframe within the same browser window. When set to **false**, DocPop results are opened in a new window.

- If **embedded** is set to **true** and results are not embedded in another Web page, then the address bar and browser toolbars will be displayed when a user accesses the DocPop URL.
- If DocPop results will not be embedded in Web pages, set **embedded** to **false**. The address bar and toolbars will be hidden when DocPop results are displayed.

enableDefaultLogin - Set this to **true** to have DocPop use the **username** and **password** credentials specified in the **Hyland.Web.DocPop** element. Set this to **false** to have DocPop either attempt other authentication methods (if they are configured) or prompt the user for credentials.

enableHTTPLogin - Set this to **true** to pass login credentials to the server on the query string or to post them through an HTML form. Set this to **false** if DocPop should either attempt other authentication methods (if they are configured) or prompt the user for credentials.

Note: For information about passing values using the query string, see the topic Modifying a DocPop URL in the DocPop help files or module reference guide.

enableAutoLogin - Set this to **true** to use domain credentials to log on to DocPop automatically. When this is set to **false**, DocPop either attempts other authentication methods (if they are configured) or prompts the user for credentials. If you enable this setting, ensure that the Web Server is configured for Active Directory authentication. See the **Legacy Authentication Methods** module reference guide for more information about Active Directory authentication.

Set **enableAutoLogin** to **true** if you are using Integration for Single Sign-On. If OnBase is configured for Active Directory or LDAP authentication, but you want to use Single Sign-On with DocPop, set both **forceSSOAutoLoginOverDomain** and DocPop's **enableAutoLogin** setting to **true**. For more information about Integration for Single Sign-On, see the **Legacy Authentication Methods** module reference guide.

enableHTTPDataSource - Set this to **true** to pass the data source on the query string. Set to **false** to use the DocPop data source in the Web Server's Web.config.

enableChecksum - If set to **true**, a checksum value will be added to the URL query string. To enable checksums, you are also required to enter a checksum key value in the DocPop **checksum** setting, which is used to create the checksum value in the URL. When a user attempts to retrieve a document using the URL, DocPop compares the checksum in the query string to the expected checksum. If the values match, the document is displayed. If the values do not match, the user is presented with an error. This is to prevent users from modifying query strings and accessing documents they should not access. Additionally, remote users accessing the DocPop URL Creator require the Web Server administrative privilege. If set to **false**, no checksum is created.

checksum - Enter the unique string value used as a key for external, dynamic checksum creation. This string value should not be well known. The **checksum** setting applies only when **enableChecksum** is set to **true** and an external automated process is being used to dynamically generate DocPop links.

Note: Configuration of this setting is required for checksum creation and validation.

- The Application Server web.config file also contains a Pop integration checksum setting: **ChecksumKey**. This setting is used for checksum generation when the docID is used from outside of the Web Client solution (for example, in Workflow notifications). If you use this feature, the **ChecksumKey** value in the Application Server web.config file must match the **checksum** value in the **Hyland.Web.DocPop** element of the Web Server web.config file. For more information about checksum generation, please refer to the Hyland SDK.
- If you are using the Workflow action **Med - Send HL7 Message**, the Hyland.Web.DocPop **checksum** value should be empty. If an external process will generate the DocPop URLs and you want to use checksums, then a separate virtual directory for DocPop should be configured.

enableCoreQueryAPILicense - This setting requires OnBase to be licensed for Core Query API (Retrievals Per Hour). Set this setting to **true** if you want users to consume Core Query API licenses when using DocPop. Core Query API licenses help prevent the unnecessary consumption of Concurrent Client licenses. When this setting is set to **true**, a Core Query API license is consumed as soon as a user logs on to DocPop and is released immediately after the user logs off. When the **enableCoreQueryAPILicense** setting is set to **false**, a Concurrent Client license is used.

Note: Core Query API licenses are only available for external users.

AutoDisplayOneDocument - Set this setting to **true** to always display only the viewer for DocPop queries that return a single result. When this setting is set to **false**, DocPop displays both the hit list and the viewer for queries that return a single result. This behavior can be overridden by the **viewerOnlyForSingle** variable in the DocPop query string. The **viewerOnlyForSingle** variable has no effect when **AutoDisplayOneDocument** is set to **true**.

disableContextMenu - Set this setting to **true** to disable right-click menu options in the DocPop results list and viewer. Set it to **false** (the default setting) if right-click menu options should be available. This setting affects the **HTML** and **ActiveX** Web Client Types. This setting does not affect right-click menu options in the OnBase Web Client outside of DocPop.

PDFPop Vars

PDFPop-specific settings are located in the **Hyland.Web.PdfPop** element of the Web Server's Web.config file. The only required setting is a data source. You can either configure one in the Web Server's Web.config or pass it along the query string. PDFPop results are displayed using the HTML Web Client. Results are displayed as read-only.

The following settings are located in the **Hyland.Web.PdfPop** element of the Web Server's Web.config file.

username - Enter the user name to use with default login with PDFPop, if you want to use a single user account for access. When **enableDefaultLogin** is set to **true**, users can automatically log on to PDFPop using the credentials provided in the **username** and **password** settings.

password - Enter the password to use with default login with PDFPop, if you want to use a single user account for access. When **enableDefaultLogin** is set to **true**, users can automatically log on to PDFPop using the credentials provided in the **username** and **password** settings.

datasource - Enter the name of the data source to use with PDFPop. This is a required value.

domain - Enter the domain to log on to if you are using Active Directory authentication.

embedded - Set this to **true** when you are embedding PDFPop results in a custom Web page and you want the PDFPop results to be displayed in a frame or iframe within the same browser window. When set to **false**, PDFPop results are opened in a new window.

- If **embedded** is set to **true** and results are not embedded in another Web page, then the address bar and browser toolbars will be displayed when a user accesses the PDFPop URL.
- If PDFPop results will not be embedded in Web pages, set **embedded** to **false**. The address bar and toolbars will be hidden when PDFPop results are displayed.

enableDefaultLogin - Set this to **true** to have PDFPop use the **username** and **password** credentials specified in the **Hyland.Web.PdfPop** element. Set this to **false** to have PDFPop either attempt other authentication methods (if they are configured) or prompt the user for credentials.

enableHTTPLogin - Set this to **true** to pass login credentials to the server on the query string or to post them through an HTML form. Set this to **false** if PDFPop should either attempt other authentication methods (if they are configured) or prompt the user for credentials.

Note: For information about passing values using the query string, see the topic Modifying a DocPop URL in the DocPop help files or the DocPop or PDFPop module reference guides.

enableAutoLogin - Set this to **true** to use domain credentials to log on to PDFPop automatically. When this is set to **false**, PDFPop either attempts other authentication methods (if they are configured) or prompts the user for credentials. If you enable this setting, ensure that the Web Server is configured for Active Directory authentication. See the **Legacy Authentication Methods** module reference guide for more information about Active Directory authentication.

Set **enableAutoLogin** to **true** if you are using Integration for Single Sign-On. If OnBase is configured for Active Directory or LDAP authentication, but you want to use Single Sign-On with PDFPop, set both **forceSSOAutoLoginOverDomain** and PDFPop's **enableAutoLogin** setting to **true**. For more information about Integration for Single Sign-On, see the **Legacy Authentication Methods** module reference guide.

enableHTTPDataSource - Set this to **true** to pass the data source on the query string. Set to **false** to use the PDFPop data source in the Web Server's Web.config.

enableChecksum - If set to **true**, a checksum value will be added to the URL query string. To enable checksums, you are also required to enter a checksum key value in the PDFPop **checksum** setting, which is used to create the checksum value in the URL. When a user attempts to retrieve a document using the URL, PDFPop compares the checksum in the query string to the expected checksum. If the values match, the document is displayed. If the values do not match, the user is presented with an error. This is to prevent users from modifying query strings and accessing documents they should not access. Additionally, remote users accessing the DocPop URL Creator require the Web Server administrative privilege. If set to **false**, no checksum is created.

checksum - Enter the unique string value used as a key for external, dynamic checksum creation. This string value should not be well known. The **checksum** setting applies only when **enableChecksum** is set to **true** and an external automated process is being used to dynamically generate PDFPop links.

Note: Configuration of this setting is required for checksum creation and validation.

- The Application Server web.config file also contains a Pop integration checksum setting: **ChecksumKey**. This setting is used for checksum generation when the docID is used from outside of the Web Client solution (for example, in Workflow notifications). If you use this feature, the **ChecksumKey** value in the Application Server web.config file must match the **checksum** value in the **Hyland.Web.PDFPop** element of the Web Server web.config file. For more information about checksum generation, please refer to the Hyland SDK.
- If you're using the Workflow action **Med - Send HL7 Message**, the **Hyland.Web.PdfPop checksum** value should be empty. If an external process will generate the PDFPop URLs and you want to use checksums, then a separate virtual directory for PDFPop should be configured.

enableCoreQueryAPILicense - This setting requires OnBase to be licensed for Core Query API (Retrievals Per Hour). Set this setting to **true** if you want users to consume Core Query API licenses when using PDFPop. Core Query API licenses help prevent the unnecessary consumption of Concurrent Client licenses. When this setting is set to **true**, a Core Query API license is consumed as soon as a user logs on to PDFPop and is released immediately after the user logs off. When the **enableCoreQueryAPILicense** setting is set to **false**, a Concurrent Client license is used.

Note: Core Query API licenses are only available for external users.

AutoDisplayOneDocument - Set this setting to **true** to always display only the viewer for PDFPop queries that return a single result. When this setting is set to **false**, PDFPop displays both the hit list and the viewer for queries that return a single result. This behavior can be overridden by the **viewerOnlyForSingle** variable in the PDFPop query string. The **viewerOnlyForSingle** variable has no effect when **AutoDisplayOneDocument** is set to **true**.

FormPop Vars

FormPop-specific settings are located in the **Hyland.Web.FormPop** element of the Web Server's Web.config file. The only required setting is a data source. You can either configure one in the Web Server's Web.config or pass it along the query string. FormPop results are displayed using the HTML Web Client.

The following settings are located in the **Hyland.Web.FormPop** element of the Web Server's Web.config file.

username - Enter the user name to use with default login with FormPop, if you want to use a single user account for access. When **enableDefaultLogin** is set to **true**, users can automatically log on to FormPop using the credentials provided in the **username** and **password** settings.

password - Enter the password to use with default login with FormPop, if you want to use a single user account for access. When **enableDefaultLogin** is set to **true**, users can automatically log on to FormPop using the credentials provided in the **username** and **password** settings.

datasource - Enter the name of the data source to use with FormPop. This is a required value.

domain - Enter the domain to log on to if you are using Active Directory authentication.

embedded - Set this to **true** when you are embedding FormPop results in a custom Web page and you want the FormPop results to be displayed in a frame or iframe within the same browser window. When set to **false**, FormPop results are opened in a new window.

- If **embedded** is set to **true** and results are not embedded in another Web page, then the address bar and browser toolbars will be displayed when a user accesses the FormPop URL.
- If FormPop results will not be embedded in Web pages, set **embedded** to **false**. The address bar and toolbars will be hidden when FormPop results are displayed.

enableDefaultLogin - Set this to **true** to have FormPop use the **username** and **password** credentials specified in the **Hyland.Web.DocPop** element. Set this to **false** to have FormPop either attempt other authentication methods (if they are configured) or prompt the user for credentials.

enableHTTPLogin - Set this to **true** to pass login credentials to the server on the query string or to post them through an HTML form. Set this to **false** if FormPop should either attempt other authentication methods (if they are configured) or prompt the user for credentials.

enableAutoLogin - Set this to **true** to use domain credentials to log on to FormPop automatically. When this is set to **false**, FormPop either attempts other authentication methods (if they are configured) or prompts the user for credentials. If you enable this setting, ensure that the Web Server is configured for Active Directory authentication. See the **Legacy Authentication Methods** module reference guide for more information about Active Directory authentication.

Set **enableAutoLogin** to **true** if you are using Integration for Single Sign-On. If OnBase is configured for Active Directory or LDAP authentication, but you want to use Single Sign-On with FormPop, set both **forceSSOAutoLoginOverDomain** and FormPop's **enableAutoLogin** setting to **true**. For more information about Integration for Single Sign-On, see the **Legacy Authentication Methods** module reference guide.

enableHTTPDataSource - Set this to **true** to pass the data source on the query string. Set to **false** to use the FormPop data source in the Web Server's Web.config.

enableChecksum - If set to **true**, a checksum value will be added to the URL query string. To enable checksums, you are also required to enter a checksum key value in the FormPop **checksum** setting, which is used to create the checksum value in the URL. When a user attempts to retrieve a document using the URL, FormPop compares the checksum in the query string to the expected checksum. If the values match, the document is displayed. If the values do not match, the user is presented with an error. This is to prevent users from modifying query strings and accessing documents they should not access. If set to **false**, no checksum is created.

checksum - Enter the unique string value used as a key for external, dynamic checksum creation. This string value should not be well known. The **checksum** setting applies only when **enableChecksum** is set to **true** and an external automated process is being used to dynamically generate FormPop links.

Note: Configuration of this setting is required for checksum creation and validation.

- The Web Server web.config file also has an **enableChecksum** setting within the **<Hyland.Web.DocPop>** node that must be set to **true**. You must also set the **checksum** setting to the appropriate value within that node.
- The Application Server web.config file also contains a Pop integration checksum setting: **ChecksumKey**. This setting is used for checksum generation when the docID is used from outside of the Web Client solution (for example, in Workflow notifications). If you use this feature, the **ChecksumKey** value in the Application Server web.config file must match the **checksum** value in the **Hyland.Web.FormPop** element of the Web Server web.config file. For more information about checksum generation, please refer to the Hyland SDK.
- If you are using the Workflow action **Med - Send HL7 Message**, the Hyland.Web.FormPop **checksum** value should be empty. If an external process will generate the FormPop URLs and you want to use checksums, then a separate virtual directory for FormPop should be configured.

enableCoreQueryAPILicense - This setting requires OnBase to be licensed for Core Query API (Retrievals Per Hour). Set this setting to **true** if you want users to consume Core Query API licenses when using FormPop. Core Query API licenses help prevent the unnecessary consumption of Concurrent Client licenses. When this setting is set to **true**, a Core Query API license is consumed as soon as a user logs on to FormPop and is released immediately after the user logs off. When the **enableCoreQueryAPILicense** setting is set to **false**, a Concurrent Client license is used.

Note: Core Query API licenses are only available for external users.

AutoDisplayOneDocument - Set this setting to **true** to always display only the viewer for FormPop queries that return a single result. When this setting is set to **false**, FormPop displays both the hit list and the viewer for queries that return a single result. This behavior can be overridden by the **viewerOnlyForSingle** variable in the FormPop query string. The **viewerOnlyForSingle** variable has no effect when **AutoDisplayOneDocument** is set to **true**.

FolderPop Vars

FolderPop-specific settings are located in the **Hyland.Web.FolderPop** element of the Web Server's Web.config file. The only required setting is a data source. You can either configure one in the Web Server's Web.config file or pass it along the query string. The following settings are located in the **Hyland.Web.FolderPop** element of the Web Server's Web.config file.

username - Enter the user name to use with default login with FolderPop, if you want to use a single user account for access. When **enableDefaultLogin** is set to **true**, users can automatically log on to FolderPop using the credentials provided in the **username** and **password** settings.

password - Enter the password to use with default login with FolderPop, if you want to use a single user account for access. When **enableDefaultLogin** is set to **true**, users can automatically log on to FolderPop using the credentials provided in the **username** and **password** settings.

datasource - Enter the name of the data source to use with FolderPop. This is a required value.

domain - Enter the domain to log on to if you are using Active Directory authentication.

embedded - Set this to **true** when you are embedding FolderPop results in a custom Web page and you want the FolderPop results to be displayed in a frame or iframe within the same browser window. When set to **false**, FolderPop results are opened in a new window.

- If **embedded** is set to **true** and results are not embedded in another Web page, then the address bar and browser toolbars will be displayed when a user accesses the FolderPop URL.
- If FolderPop results will not be embedded in Web pages, set **embedded** to **false**. The address bar and toolbars will be hidden when FolderPop results are displayed.

enableDefaultLogin - Set to **true** to have FolderPop use the **username** and **password** credentials specified in the **Hyland.Web.FolderPop** element. When set to **false**, it either attempts other authentication methods (if they are configured) or prompts the user for credentials.

enableHTTPLogin - Set this to **true** to pass login credentials to the server on the query string or to post them through an HTML form. Set this to **false** if FolderPop should either attempt other authentication methods (if they are configured) or prompt the user for credentials.

Note: For information about passing values using the query string, see the topic Modifying a FolderPop URL in the FolderPop help files or module reference guide.

enableAutoLogin - Set this to **true** to use domain credentials to log on to FolderPop automatically. When this is set to **false**, FolderPop either attempts other authentication methods (if they are configured) or prompts the user for credentials. See the **Legacy Authentication Methods** module reference guide for more information about Active Directory authentication.

Set **enableAutoLogin** to **true** if you are using Integration for Single Sign-On. If OnBase is configured for Active Directory or LDAP authentication, but you want to use Single Sign-On with FolderPop, set both **forceSSOAutoLoginOverDomain** and the Hyland.Web.FolderPop **enableAutoLogin** setting to **true**. For more information about Integration for Single Sign-On, see the **Legacy Authentication Methods** module reference guide.

enableHTTPDataSource - Set this to **true** to pass the data source on the query string or posted through an HTML form. Set to **false** to use the data source in the Web Server's Web.config file.

enableChecksum - If set to **true**, a checksum value will be added to the URL query string. To enable checksums, you are also required to enter a checksum key value in the FolderPop **checksum** setting, which is used to create the checksum value in the URL. When a user attempts to retrieve a document using the URL, FolderPop compares the checksum in the query string to the expected checksum. If the values match, the document is displayed. If the values do not match, the user is presented with an error. This is to prevent users from modifying query strings and accessing documents they should not access. If set to **false**, no checksum is created.

Note: When **enableChecksum** is set to **true**, users can only access the FolderPop URL Creator if they belong to a User Group that has the **Web Server** product right, or they make the request to access the FolderPop URL Creator from the Windows server that is also hosting the Web Server.

checksum - Enter the unique string value used as a key for external, dynamic checksum creation. This string value should not be well known. The **checksum** setting applies only when FolderPop's **enableChecksum** setting is set to **true** and an external automated process is being used to dynamically generate FolderPop links.

Note: Configuration of this setting is required for checksum creation and validation.

If an external process will generate the FolderPop URLs and you want to use checksums, a separate virtual directory for FolderPop should be configured.

enableCoreQueryAPILicense - This option requires OnBase to be licensed for Core Query API (Retrievals Per Hour). Set this option to **true** if you want users to consume Core Query API licenses when using FolderPop. Core Query API licenses help prevent the unnecessary consumption of Concurrent Client licenses. When this option is set to **true**, a Core Query API license is consumed as soon as a user logs on to FolderPop and is released immediately after the user logs off. When the **enableCoreQueryAPILicense** option is set to **false**, a Concurrent Client license is used.

Note: Core Query API licenses are only available for external users.

Office Documents Setting

The **openOfficeDocumentsInSeparateWindow** setting controls whether Microsoft Office documents (Word, Excel, and PowerPoint) are opened in a separate window using their native applications. This setting is set to **true** by default.

When **openOfficeDocumentsInSeparateWindow** is **true**, Office documents are opened externally in their native applications instead of within the browser window. The documents are opened externally regardless of the **Browse in same window** setting for the documents' file types in Windows Folder Options.

Note: When **openOfficeDocumentsInSeparateWindow** is **true**, the **File Download** prompt is displayed when Web Client users attempt to open Office documents, even if the **Confirm open after download** setting is disabled for the file type in Windows Folder Options. For more information about Folder Options, refer to your operating system's help files.

When **openOfficeDocumentsInSeparateWindow** is **false**, the Web Client attempts to open Office documents within the browser window. This is only available in the ActiveX Web Client. The documents may be opened either in the browser or externally, depending on the workstation's operating system settings, the version of Office installed, the version of the Office document being opened, and whether any OnBase Office integrations are installed. Documents created using different versions of Office may open differently. To ensure Office documents always are opened externally, set **openOfficeDocumentsInSeparateWindow** to **true**.

RTF Documents Setting

The **OpenRTFasMSWord** setting applies only to the HTML Web Client. When set to **true**, it allows RTF documents to be opened from the Web Client in Microsoft Word, provided that Microsoft Word is installed on the workstation. If **OpenRTFasMSWord** is **false**, then RTF documents are opened in the program associated with the RTF extension on the client operating system.

To allow RTF documents to be opened within the browser using Microsoft Word, ensure the following conditions are met:

- **openOfficeDocumentsInSeparateWindow** is set to **false**.
- **OpenRTFasMSWord** is set to **true**.
- Microsoft Word is installed on the client workstation.
- The fix provided by Microsoft KB article 927009 is applied to the client workstation.

Thumbnail Hit List Viewer

The thumbnail viewer, which is available for the ActiveX and HTML Web Clients, lets users preview multiple text or image documents in the Document Search Results list by displaying thumbnails of the first page of each document. This viewer displays the thumbnails in a new window, allowing users to quickly review multiple documents in the list. Users can zoom in on thumbnails by resting their mouse pointers on them. When the right document is found, it can be opened with a single click.



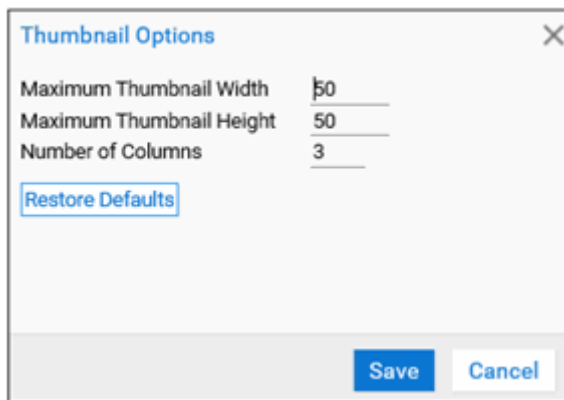
Access to the thumbnail viewer is controlled by the **Thumbnail Hitlist Results Viewer** privilege in OnBase Configuration. Users with this privilege can open the thumbnail viewer by selecting documents in the Document Search Results list and choosing **View Thumbnails** from the right-click menu. See the Configuration help files for information about assigning privileges.

The Web Server's Web.config contains several settings that control the thumbnail viewer's appearance and its ability to be customized.

ThumbnailHitListAllowCaching - Set to **true** to allow thumbnail images to be cached on the Web Server. Enable caching to prevent the Web Server from making multiple requests to the disk groups (either directly or through the Application Server) for the same images. A user's thumbnail viewer cache is stored temporarily during the user's session and is emptied when the user exits the Web Client. Set to **false** to disable thumbnail caching and to ensure that thumbnails always reflect recent changes to the documents.

ThumbnailHitListShowPreviews - Set to **true** to allow users to zoom in on thumbnails by placing their mouse pointers over them. Thumbnails are enlarged to the maximum height or width configured for previews. Set to **false** to disable thumbnail previews.

ThumbnailHitListUserConfigurable - Set to **true** to let users override the values you specify for the next five settings (number of columns, maximum thumbnail height/width, and maximum preview height/width). When this option is set to **true**, the **Options** button is available from the thumbnail viewer, allowing users to customize the viewer's appearance using the dialog box shown below. When this option is set to **false**, the **Options** button is unavailable, and the thumbnail viewer will use the values you provide for the following settings.

A screenshot of a 'Thumbnail Options' dialog box. The dialog has a title bar with the text 'Thumbnail Options' and a close button (X). Inside, there are three labels with corresponding input fields: 'Maximum Thumbnail Width' with a value of '50', 'Maximum Thumbnail Height' with a value of '50', and 'Number of Columns' with a value of '3'. Below these fields is a button labeled 'Restore Defaults'. At the bottom right of the dialog are two buttons: 'Save' and 'Cancel'.

Note: The maximum thumbnail height and width settings are not used by documents that have thumbnail image renditions available. For faster loading, the thumbnail viewer displays these renditions without resizing them. Thumbnail image renditions are created by Document Import Processes and scan queues that have the **Create Image Thumbnails On Commit** option enabled.

ThumbnailHitListColumns - Enter the maximum number of columns you want the thumbnail viewer to use when displaying thumbnails. Valid values range from **1** through **7**.

ThumbnailHitListThumbnailMaxWidth - In pixels, enter the maximum width for thumbnails. Valid values range from **20** through **500**.

ThumbnailHitListThumbnailMaxHeight - In pixels, enter the maximum height for thumbnails. Valid values range from **20** through **500**.

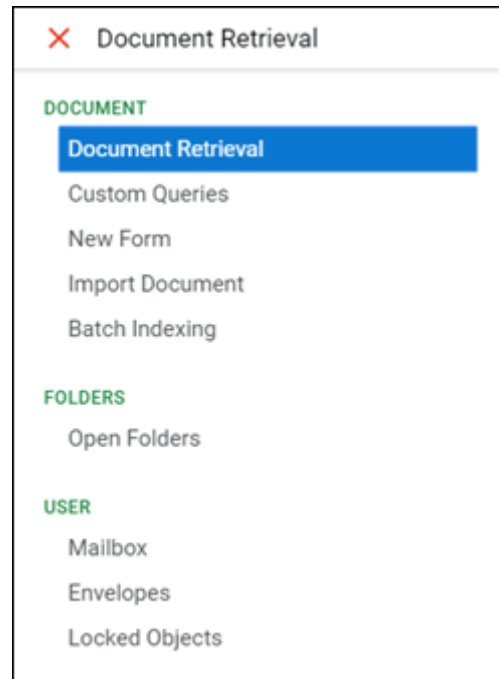
ThumbnailHitListPreviewMaxWidth - In pixels, enter the maximum width for thumbnail previews. Valid values range from **100** through **1000**. The minimum preview width allowed by the Web Client is twice the maximum thumbnail width.

ThumbnailHitListPreviewMaxHeight - In pixels, enter the maximum height for thumbnail previews. Valid values range from **100** through **1000**. The minimum preview height allowed by the Web Client is twice the maximum thumbnail height.

Main Menu Panel Configuration

The Main Menu panel controls the options available in the Web Client.

- The Section Heading options are controlled by **ContextInfo** elements.
- The Selection options available under each Section Heading are controlled by **ControlBar** elements.



Many contexts and control bars (which represent Selection options) are turned on by default. To enable or disable a context or control bar, you need to set the `<enabled>` text to **true** or **false**. To enable it, you would set it to true. For example, `<enabled>true</enabled>`.

Note: If you enable a context or control bar, you can control the view based on User Groups & Rights. If no control bars are enabled under a context, then the context will not be available. For descriptions of available settings, see [Navigation Panel Context Settings on page 285](#).

The following is an example configuration for the Document context:

```
<ContextInfo>
  <name>Document</name>
  <displayName>Document</displayName>
  <displayOrder>0</displayOrder>
  <icon>NavPanel/RetrieveUp.gif</icon>
  <enabled>True</enabled>
<!--Turns Retrieve Context Button on-off-->
</ContextInfo>
```

Navigation Panel Context Settings

Document - Enables or disables the **Document** context selection in the drop-down list.

RetrieveDocument - Enables or disables the **Document Retrieval** option in the **Document** context.

RetrieveDocumentByHandle - Enables or disables the **Retrieve by Document Handle** option in the **Document** context.

RetrieveSpecificDocument - Enables or disables the **Retrieve Specific Document** option in the **Document** context.

CustomQuery - Enables or disables the **Custom Queries** option in the **Document** context.

NewForm - Enables or disables the **New Form** option in the **Document** context.

DocumentTemplates - Enables or disables the **Document Templates** option in the **Document** context. One of the OnBase Office Business Applications (OBAs) is required, depending on your version of Microsoft Office.

Upload - Enables or disables the **Import Document** option in the **Document** context.

Scan - Enables or disables the **Scan a Document** option in the **Document** context.

FullTextIndexingService - Enables or disables the **Full-Text Search** option in the **Document** context.

IndexScannedBatch - Enables or disables the **Indexing** option in the **Document** context.

VersionControl - Enables or disables the **Documents Checked Out** option in the **Document** context.

Briefcase - Enables or disables the **Briefcase** option in the **Document** context.

Workflow - Enables or disables the **Workflow** context.

WorkView - Enables or disables the **WorkView** context.

KnowledgeTransfer - Enables or disables the **Knowledge Transfer** context.

Collaboration - Enables or disables the **Collaboration** context.

AllWorkspaces - Enables or disables the **My Workspaces** option in the **Collaboration** context.

FindWorkspace - Enables or disables the **Workspace Retrieval** option in the **Collaboration** context.

StatusView - Enables or disables the **StatusView** context.

MyViews - Enables or disables the **My Views** option in the **StatusView** context.

StatusViewAdmin - Enables or disables the **Administration** option in the **StatusView** context.

StatusViewPrivs - Enables or disables the **Privileges** option in the **StatusView** context.

Folders - Enables or disables the **Folders** context.

User - Enables or disables the **User** context.

Mailbox - Enables or disables the **Mailbox** option in the **User** context.

Envelope - Enables or disables the **Envelopes** option in the **User** context.

Password - Enables or disables the **Password** option in the **User** context.

Options - Enables or disables the **Options** option in the **User** context.

BriefcaseOptions - Enables or disables the **Briefcase Options** option in the **User** context.

Admin - Enables or disables the **Admin** context.

Users - Enables or disables the **Users** option in the **Admin** context.

Reporting Dashboards - Enables or disables the **Reporting Dashboards** option in the Document context.

Help - Enables or disables the **Help** context.

Context Security Checks and Licensing

If you enable a control bar, a user may access the context based upon User Groups & Rights. User security is still checked for each of these contexts. For example, if the Envelope control bar is enabled, but the user does not have the Envelopes privilege, the user will not be able to see the control bar.

Note: Licensing also determines the availability of control bars. If a control bar is turned on, but the system is not licensed for the corresponding feature, then the control bar is not available in the Web Client. Context options are typically used when a system is licensed for a product, but the system administrator does not want to show the feature for business reasons.

See the following table for details. In addition to the product rights listed, all Web Client users must have the **Web Client** product right.:

Functionality (Web)	Security Check / Other	Privileges*	Product Rights*
		*Parentheses indicate privileges' categories in OnBase Configuration dialog boxes.	
Retrieve Documents	Access to any Document Types	Retrieve Dialog (Client Features)	
Retrieve by Document Handle	Access to any Document Types		Retrieve by Document Handle / File Name (Administrative Privileges)
Custom Query	Access to any custom queries	Retrieve / View (Documents)	
Create a New Form	Access to Electronic Forms	Create (Documents)	HTML Forms (Registered Processing Products)

Functionality (Web)	Security Check / Other	Privileges*	Product Rights*
		*Parentheses indicate privileges' categories in OnBase Configuration dialog boxes.	
Document Templates	Access to Document Templates / OnBase OBA installed	Create (Documents) Import (Client Features)	
Upload a Document		Create (Documents) Import (Client Features)	
Scan a Document	License: Web Scanning	Create (Documents)	Scan (Registered Processing Products)
Full-Text—Index Server	License: Full-Text / Server	Full-Text Search (Client Based Products)	Full-Text Indexing (Registered Processing Products)
Indexing		Index Scanned Documents (Scan/Index Batches)	
Documents Checked Out		Create / View Revisions (Documents)	
Workflow	License: Workflow / Server	Workflow or Workflow Restricted (Client-Based Products)	
WorkView	License: WorkView / Server	WorkView (Client-Based Products)	
Knowledge Transfer	License: Document Knowledge Transfer		
Collaboration	License: Collaboration		
StatusView	License: StatusView		
Folders		Retrieve / View (Folders)	
User / Mailbox		Internal Mail (Documents)	
User / Envelopes		Envelopes (Client Features)	

Functionality (Web)	Security Check / Other	Privileges*	Product Rights*
		*Parentheses indicate privileges' categories in OnBase Configuration dialog boxes.	
User / Change Password	User Settings: Disable Change Password is off		
User / Options		User / Workstation Options (Client Features)	
Admin	Configuration Rights: User Account Admin, User Update Admin, or Password Admin (User / User Groups) OR Product Right: User Management ^a		
Reporting Dashboards	License: Reporting Dashboards		

a. In the Admin context, available options vary depending on which of these rights you are assigned. For more information, see [Required Administrative Rights on page 136](#).

Custom Contexts

You can also create contexts that contain custom control bars (menu items) in the Web Client. To change the display name of a custom context or control bar, change the **<displayName>** parameter.

The display names of built-in control bars and contexts, such as the following, cannot be changed:

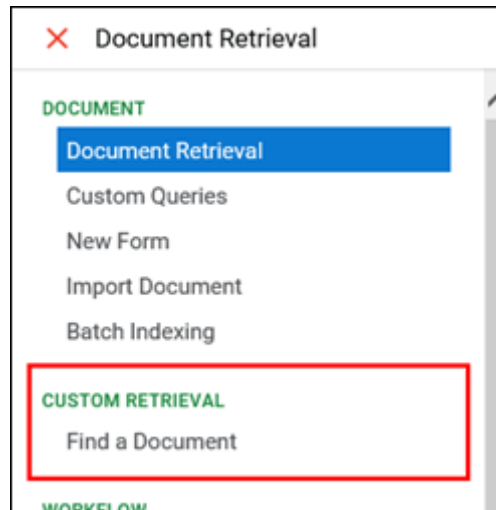
- Document context
- Workflow context
- WorkView context

Note: When customizing contexts in non-English locales, the web.config file must be saved with UTF-8 encoding. See [Web.config Encoding on page 312](#) for more information.

```

<ContextInfo>
  <name><![CDATA[CustomContextName]]></name>
  <displayName><![CDATA[Custom Retrieval]]></displayName>
  <displayOrder>0</displayOrder>
  <icon><![CDATA[NavPanel/CustomRetrieval.gif]]></icon>
  <enabled>True</enabled>
</ContextInfo>

```



Auto-Display Options

The server can be configured to display certain functions instead of the standard Document Retrieval. For example, you can configure the server so that users see a certain Custom Query by default, or have it open directly to Workflow. This is controlled by a set of keys in the Web Server's Web.config file. The entry under the **Navigation Panel Configuration** section, and looks like this:

```

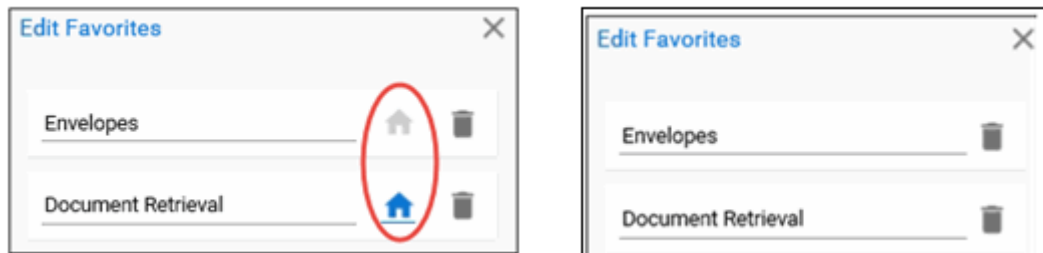
<DefaultContextInfo>
  <defaultContext>Document</defaultContext>
  <defaultControlBar>CustomQuery</defaultControlBar>
  <defaultContextID>145</defaultContextID>
</DefaultContextInfo>

```

The **defaultContext** option controls from which context the control bar is opened. The options are the available contextinfo items, including **Document**, **Workflow**, and **WorkView**. The **defaultControlBar** selects which mode is displayed, depending on the context. The **defaultContextID** is the ID of the specific context you want opened, as assigned by OnBase. This number can be obtained by looking at the configuration settings in the Configuration module. In this example, the context is Document, and the ControlBar is Custom Query. This will open the configured Custom Query whose ID number is 145.

Default Contexts & Home Pages

If a default context is specified in the Web Server's Web.config file, then the **Set as Home Page** button is removed from the list of favorites, and users cannot designate a home page.



If any users have already selected a home page, then the default context overrides this selection.

Custom Validation

Custom validation provides the ability to process, validate, and format Keyword values a user enters in the Keyword Panel. When triggered, a custom data validation handler can modify the value entered by a user. If the value is invalid and should not be submitted to OnBase, the handler can replace the value with an empty string to prevent it from staying on the Keyword Panel. The system may also display a dialog box to obtain user input before returning the updated keyword value to OnBase.

Custom validation is set up in the Web Server's Web.config through the configuration of custom data validation handlers.

Custom vs. Standard Validation

Standard validation ensures a Keyword value is of the expected data type and format (e.g., US currency, German floating point number). It occurs for all Keyword values when the user attempts to submit them from the Keyword Panel. Standard validation occurs regardless of whether custom validation is configured.

Custom validation can be used for more than data type and format validation and occurs as soon as the user tabs away from a Keyword Type field in the Keyword Panel. The CustomValidation element in the Web Server's Web.config includes examples of how custom validation may be used.

Restrictions and Limitations

Custom validation is triggered only after a value is manually entered by the end user. It is not triggered when displaying Keyword values that were previously on a document or when adding Keywords values that are part of an AutoFill Keyword Set.

To trigger custom validation, the end user must press **Tab** after typing the value. If the Keyword Type field is the last field in the Keyword Panel, the user must press **Shift + Tab**.

Custom data validation handlers must be configured for each Keyword Type that requires custom validation.

Validator names specified in the Web Server's Web.config are case-sensitive. The locations of script files and pages are not case-sensitive.

Configuration

The Web Server's Web.config allows you to set up custom validation at the application level for the entire virtual directory and at the page level for individual pages that use the Keyword Panel. If a Keyword Type is defined at both the application and the page level, the page level definition takes precedence on that page only.

To set up custom validation, you must provide the Keyword Type's ID, the validation function, and the location of the script file that contains the function. These parameters are defined in the CustomValidation element in the Web Server's Web.config. Note that the locations of script files and pages are relative to the root directory.

For more information about validation functions, see [Validation Functions on page 292](#).

Identifying Application and Pages Elements

Application-level custom validation is configured within the application element:

```
<application scriptLocation="">
  <keywords></keywords>
</application>
```

Page-level custom validation is configured for individual pages within the pages element:

```
<pages>
  <page location="/SamplePage.aspx" scriptLocation="">
    <keywords></keywords>
  </page>
</pages>
```

Procedure for Specifying Validation Functions

The following procedure describes how to configure custom validation for either the application or specific pages.

1. Between the quotation marks of the scriptLocation attribute, enter the relative path to the script file that contains the validation function.
2. Between the keywords tags, create a keyword element specifying the Keyword Type ID and the validation function to run on values entered for the Keyword Type. For example:

```
<keywords>
  <keyword id="123" validator="[validationfunction]">
</keywords>
```

Where [validationfunction] is the name of the function in the script file. Perform this step for each Keyword Type you want to validate on the page.

Validation Functions

The Keyword Panel uses a JavaScript function with a specific signature to process a Keyword value. The function should accept a single input parameter representing the value the user entered into the Keyword Type field and return either a null or string value. A null value is used to indicate that the user's input should not be changed. If a string value is returned, the Keyword value will be set equal to the returned value.

Sample Function

The following function could be used as a keyword validator:

```
function PrependBranchCode(originalNumber)
{
    if(originalNumber.length < 5)
    {
        return "1234" + originalNumber;
    }
    else
    {
        return null;
    }
}
```

In this example, the function prepends the branch code **1234** to the original number only if it has fewer than 5 digits; the function returns null if the number is longer. This function is a simple example of how validation can be used to determine whether a Keyword value should be modified. A more sophisticated function could display dialog box prompting the user to choose a branch code to prepend, for example. Essentially, the capabilities of a validation function are limited only by those of JavaScript.

Note: For information about writing JavaScript functions, consult a JavaScript reference site such as the Microsoft Developer Network (<http://msdn2.microsoft.com>).

Hyland.Logging

A **Hyland.Logging** section is available in the .config files of .NET-based applications, such as the OnBase Application Server or Web Server. This section controls diagnostics logging for those applications.

Enabling Event Viewer Logging

Events can be logged to the Hyland log in the Windows Event Viewer on the current server. The following steps describe how to ensure that Event Viewer logging is enabled.

1. Ensure the **WindowsEventLogging** element exists in the application's .config file.
2. If necessary, modify the **sourcename** attribute. When events are logged to the Hyland log, they display this value as their source. Ensure the value differs from the **sourcename** configured for any other OnBase application on this server.

The default source name for the OnBase Application Server is **Hyland Application Server**. The default source name for the OnBase Web Server is **ASP.NET Web Client**.

Diagnostics Profiles

The Diagnostics Service writes messages to specific profiles, which correspond to specific products or categories. The data logged to each profile corresponds to the tab of the same name in the Diagnostics Console.

Available profiles vary per application. Depending on the application, one or more of the following profiles can be used:

Profile	Description
asp.net	ASP.NET messages.
cache	Cache messages, which are logged when the Application Server attempts to add or retrieve information from the item cache.
configuration	OnBase Studio messages.
db	Database messages.
error	Errors. To save errors to a log file, you must still follow the normal procedures for enabling log file creation.
file	Disk Group access messages.
fulltext	Full Text Indexing Service messages. This profile is available only for the Hyland Full Text Indexing Service.
hl7	HL7 version 3 service messages.

Profile	Description
ldap	Active Directory and LDAP messages.
locking	Locking messages, which are logged when the Application Server attempts to lock an item in the system.
report.services	Report Services messages.
scriptexception	Allows client-side script exceptions to be reported through the Web Server to the Diagnostics Console. This profile is available in the Web Server's web.config, and it should always be included.
service	Service messages. This profile is not available for the Web Server.
trace	Trace messages. See Setting the Tracing Level on page 298 for information about configuring trace logging.
vbscript	VBScript execution messages in Workflow. <hr/> Note: This profile is not available for the Web Server. <hr/>
warnings	Warning messages, which the Application Server logs for events that do not trigger an error but may indicate an invalid setting. For example, this profile may display information about incorrectly configured E-Form fields.
wcf	Transfer Batch Handler Service messages.
web.service	Web service messages. <hr/> Note: This profile is not available for the Web Server. <hr/>
workflow	Workflow script execution and trace messages.

Enabling Diagnostics Logging

In order for an application to send diagnostics messages to the Diagnostics Service and Diagnostics Console, a logging route must be configured in the **Hyland.Logging** section of the application's .config file.

By default, all logging profiles are logged to the configured route. You can configure the route to include or exclude specific profiles.

Use the **include-profiles** key in a route to enable logging only for specific profiles. List the included profile names in a comma-separated, case-sensitive list in the **value** attribute of the key. For example:

```
<add key="include-profiles" value="example1,example2" />
```

Note: Any profiles not listed in the **include-profiles** key will not be logged.

Use the **exclude-profiles** key in a route to disable logging for specific profiles. List the excluded profile names in a comma-separated, case-sensitive list in the **value** attribute of the key. For example:

```
<add key="exclude-profiles" value="example1,example2" />
```

Note: Any profiles not listed in the **exclude-profiles** key will be logged. Also, the **include-profile** key overrides the **exclude-profiles** key, so if a profile is listed in both keys, it will be logged.

Truncating Log Length

Long string values can be configured for automatic truncation in logs. To configure this option:

1. Find the **Hyland.Logging** section of the application's .config file.
2. Under this section, prior to the **Route** subsection, find the following line:

```
<Hyland.Logging TruncateLogValues="NUMBER">
```


If the line is not already present, add it before the **<Routes>** subsection.
3. Replace **NUMBER** with the number of characters to truncate strings after, in quotation marks. The default value for this is **1024**.
4. Save the file and restart the application.

Setting the Logging Level

To receive logging messages, a logging level must be specified for a logging route in the **Hyland.Logging** section of the application's .config file. To set the logging level:

1. Find the logging route you want to configure in the **Hyland.Logging** section.
2. Within the **Route** section for the route, ensure the following line is included:

```
<add key="minimum-level" value="Trace" />
```

This enables detailed messaging to the diagnostics route.

Note: Depending on the application, this line might be included by default but commented out. Remove the **<!--** and **-->** from the line to uncomment the line.

3. Change **value="Trace"** to **value="Debug"**.

Note: The value **Trace** logs the most detailed messages possible. These messages may contain sensitive information. Due to this, **Trace** should not be used in any production environment.

4. To refine the severity of messages being received by the diagnostics route, you can edit the **key** and **value** attributes in the following manners:
 - The **key** value can be set to **minimum-level**, which limits the lowest-severity log level that is received. You can add an additional line that includes **maximum-level**, which limits the highest-severity log level that is received.
 - The **value** can be set to any of the following log level severities, listed from most severe to least severe.

Note: Log level names in the **value** attribute are case sensitive.

Log Level	Description
Critical	Logs that describe an unrecoverable application, system crash, or catastrophic failure that requires immediate attention.
Error	Logs that highlight when the current flow of execution is stopped due to a failure. These logs indicate a failure in the current activity, but not an application-wide failure.
Warning	Logs that highlight an abnormal or unexpected event in the application flow but do not otherwise cause the application to stop.
Information	Logs that track the general flow of the application.
Debug	Logs that are used for interactive investigation during development.
Trace	Logs that contain the most detailed messages and may include sensitive data. These logs should never be enabled in a production environment.
None	A logging category that should not write any logging messages.

For example, the **Hyland.Logging** section of the .config file could be edited to:

```
<add key="minimum-level" value="Debug" />
<add key="maximum-level" value="Critical" />
```

This example specifies that the logging route only receives logging messages with a severity level of **Debug** or above, and it receives no messages with a higher severity level than **Critical**.

Note: The default severity level of a route is a minimum of Information and a maximum of Critical. The route uses these severity levels if it does not include a **minimum-level** or **maximum-level** line specified in the .config file.

5. Save the file and restart the application.

Setting the Tracing Level

Some applications let you control the amount of information logged to the **trace** profile using the **hylandTracing** switch, which is in the application's configuration file. Set the value to **0** for no information. Set the value to **1**, **2**, **3**, or **4** for minimal, normal, detailed, or verbose messages, respectively.

Creating Log Files

Routes can be configured to write logs to separate external .json files. These files can later be opened for viewing in the Diagnostics Console or in a text editor such as Notepad.

To configure logs to be written to files in the .config file of the application:

1. Open the .config file.
2. Locate the **Hyland.Logging** section of the file.
3. In Route sub-section for the diagnostics route you want to configure, enter the following tag:

```
<add key="File" value="FILEPATH"/>
```

For **FILEPATH**, enter the full file path for the log file, including the name of the file you want the log to be saved as. This file must be a .json file. For example, `<add key="File" value="C:\Users\jsmith\Desktop\log.json">` would write the logs to a log.json in that directory.

4. Save the file and restart the application.

Disabling IP Address Masking

In the Diagnostics Console, the IP address of the workstation is displayed in certain tabs. By default, the source IP address is obfuscated so that it cannot be identified. To display the full source IP address of the workstation, a tag must be entered into the diagnostics route in the **Hyland.Logging** section of the .config file of the .NET-based application being used by the workstation.

To enter the tag into the .config file of the application:

1. Open the .config file.
2. Locate the **Hyland.Logging** section of the file.
3. In Route sub-section for the diagnostics route you want to configure, enter the following tag:

```
<add key="DisableIPAddressMasking" value="true"/>
```

4. Save the file and restart the application.

Configuring for Third Party Diagnostic Programs

Hyland.Logging can be configured to send information to several different third party diagnostic programs, such as Splunk or ELK. Routes must be specifically configured for each of these options. For more information on these configuration steps, see:

- [Configuring Hyland.Logging for Splunk on page 299](#)
- [Configuring Hyland.Logging for ELK on page 299](#)

Configuring Hyland.Logging for Splunk

Hyland.Logging can be configured to send information to Splunk as well as the Diagnostics Console by modifying the .config file of the server. To configure Hyland.Logging to send information to Splunk:

1. Open the .config file.
2. Locate the **Hyland.Logging** section of the file.
3. In the **Routes** sub-section, add the following new route:

```
<Route name="Logging_Local_Splunk" >
  <add key="Splunk" value="http://localhost:SplunkPort"/>
  <add key="SplunkToken" value="SplunkTokenNumber"/>
  <add key="DisableIPAddressMasking" value="false" />
</Route>
```
4. Replace the **localhost** value with the address of the host if not local.
5. Replace the **SplunkPort** value with the port used by Splunk.
6. Replace the **SplunkTokenNumber** value with the Splunk token.
7. Add any additional keys for routing levels or profiles to this route as desired.
8. In the **AuditRoutes** sub-section, add the following new route:

```
<Route name="Audit_Local_Splunk" >
  <add key="Splunk" value="http://localhost:SplunkPort"/>
  <add key="SplunkToken" value="SplunkTokenNumber"/>
  <add key="DisableIPAddressMasking" value="false" />
</Route>
```
9. Replace the **localhost** value with the address of the host if not local.
10. Replace the **SplunkPort** value with the port used by Splunk.
11. Replace the **SplunkTokenNumber** value with the Splunk token.
12. Add any additional keys for routing levels or profiles to this route as desired.
13. Save the file and restart the application.

Configuring Hyland.Logging for ELK

Hyland.Logging can be configured to send information to ELK as well as the Diagnostics Console by modifying the .config file of the server. To configure Hyland.Logging to send information to ELK:

1. Open the .config file.
2. Locate the **Hyland.Logging** section of the file.
3. In the **Routes** sub-section, add the following new route:

```
<Route name="Logging_LOCAL_ELK">
  <add key="Http" value="http://<LOGSTASH_HOST_MACHINE>:PORT"/>
  <add key="DisableIPAddressMasking" value="false" />
  <add key="CompactHttpFormat"/>
</Route>
```
4. Replace the **<LOGSTASH_HOST_MACHINE>** value with the address of the Logstash Host Machine.

5. Replace the **PORT** value with the port used by Logstash.
6. Add any additional keys for routing levels or profiles to this route as desired.
7. In the AuditRoutes sub-section, add the following new route:

```
<Route name="Audit_CLOUD_ELK">  
  <add key="Http" value="http://<LOGSTASH_HOST_MACHINE>:PORT" />  
  <add key="DisableIPAddressMasking" value="false" />  
  <add key="CompactHttpFormat" />  
</Route>
```
8. Replace the **<LOGSTASH_HOST_MACHINE>** value with the address of the Logstash Host Machine.
9. Replace the **PORT** value with the port used by Logstash.
10. Add any additional keys for routing levels or profiles to this route as desired.
11. Save the file and restart the application.

Configuring Image Quality and Compression Settings

The compression quality of color images (and where those images are decompressed) can affect the performance of your OnBase solution.

By default, the Application Server defers the decompression of JPEG-compressed TIFFs to the client workstation with the image quality set to 100%. This allows each client workstation to be responsible for its resource usage. It also prevents the Application Server from streaming large, decompressed color images to client workstations.

Two settings are available to modify this behavior: **RawImagesAllowed** and **CompressionQuality**. These settings can help improve speed and memory usage for displaying color images in the OnBase Web Client. Adjust these settings in the Application Server's Web.config file if users viewing many color images are encountering performance issues.

Note: Because these settings affect only images that are JPEG-compressed, the **Use JPEG compressed TIFF as default color image format** setting must be selected in OnBase Configuration. This setting is located on the **Document** tab under **Users | Global Client Settings**.

RawImagesAllowed

RawImagesAllowed controls where images are decompressed. This setting's default value is **true**, which means images are decompressed on the client workstation if possible. When set to **false**, images are decompressed on the server.

- Change this setting to **false** to reduce memory usage on the client side, but be aware that it also incurs additional overhead on the Application Server.
- Consider reducing the **CompressionQuality** to reduce the size of files streamed to client workstations.

If **RawImagesAllowed** is set to **false** and the Application Server has insufficient resources to display the image at the specified **CompressionQuality**, the Application Server will attempt to display the image at a reduced quality. When this quality reduction occurs, the document viewer informs the user by presenting the following message: "Image quality reduced due to available resources." If the image cannot be displayed at a reduced quality, the image fails to load. This feature has not been implemented in Unity-based clients.

CompressionQuality

CompressionQuality controls the compression quality of color images and can be used to reduce memory usage when viewed. The default setting is **70** (measured in percent).

- Lower this value when **RawImagesAllowed** is set to **false**. This reduces the size of files that are streamed to client workstations, which can improve performance.
- Test viewing samples of typical color images to determine whether the image quality is sufficient. Often the difference caused by lower compression quality is minimal and noticeable only when images are compared side-by-side with images compressed at 100% quality.

Configuring the ASP.NET Version of LoginFormProc

LoginFormProc presents users with a custom HTML form that they can complete and submit to OnBase as an E-Form.

When configured correctly, LoginFormProc allows users to submit forms using the following Web browsers:

- Apple Safari®
- Google Chrome™
- Microsoft Internet Explorer®
- Mozilla Firefox®

LoginFormProc does not allow you to retrieve documents from OnBase. Another Web Server component, DocPop, is the preferred method for viewing OnBase documents externally. For more information about DocPop and how to use it to retrieve documents from OnBase, see the DocPop reference guide.

LoginFormProc does not allow you to update existing E-Forms or Unity Forms. To update existing E-Forms and Unity Forms, FormPop should be used. For information about configuring FormPop, see [FormPop on page 306](#).

Configuration

The login settings for LoginFormProc are set in the Web Server's Web.config. All forms submitted through LoginFormProc are created in OnBase by the user account you specify in Web.config, as described in the following section, [LoginFormProc Settings](#).

LoginFormProc Settings

Several settings in the Web Server's Web.config file need to be configured for LoginFormProc. These settings are located within the **Hyland.Web.LoginFormProc** element.

username - Specify the user name to be used for creating forms. This account must not be a service account.

password - Specify the password for the supplied user for creating forms.

datasource - Specify the name of the data source to use for creating forms. You must provide a data source for LoginFormProc to work.

prompt - Set to **enable** if you want LoginFormProc to prompt users to create another form. Set to **disable** if LoginFormProc should not prompt users. When prompting is enabled, the HTML form must contain the **OBWeb_Redirect** field, which specifies the path to the form.

Encrypting LoginFormProc Web.config Settings

You can use the Web Application Management Console to encrypt all settings in the **Hyland.Web.LoginFormProc** element. When encrypted, information such as the LoginFormProc **username** and **password** values cannot be viewed within the Web Server's Web.config file.

Encryption is enabled by the **Encrypt Login Form Proc** setting in the Web Application Management Console. When this setting is applied and saved, information within the **Hyland.Web.LoginFormProc** element is replaced with an **EncryptedData** element, which contains the encrypted settings.

For information about using the console to modify and encrypt LoginFormProc settings, refer to the Web Application Management Console module reference guide.

Features

LoginFormProc allows a user to perform several tasks, which are described in the following sections:

1. [Submitting a new form to the database on page 303](#)
2. [Opening a read-only copy of the submitted form on page 304](#)
3. [Redirecting the user to the custom form on page 304](#)
4. [Setting the Language Parameter on page 305.](#)

Note: Values containing HTML or Script code cannot be submitted through LoginFormProc. For example, if a user enters a value of **<text>** and clicks **Submit**, an error is displayed and the form is not submitted. This behavior is by design to prevent a malicious attack on the server. A possible workaround is to use Workflow and scripting. Create a life cycle to capture the incoming E-Form, and create a new form converting text using scripts.

Submitting a new form to the database

Required fields on the custom HTML form:

- **OBDocumentType**
This field contains the Document Type number, not the Document Type name.
- E-Form fields
- **OBBtn_Save || OBBtn_Yes**

The action parameter on the form must include the path to the Web server that will be uploading the form. For example:

```
<form method="post" action="http://[server name]/appnet/loginformproc.aspx?>
```

New forms are submitted to the database using an **OBBtn_Save** (or **OBBtn_Yes**) button that saves information (E-Form fields) to the database. A new E-Form is created in the given Document Type (whose number is specified in the **OBDocumentType** input field), and any keyword values on the form are saved to the database. This button must be **type=submit**.

Either **OBBtn_Save** or **OBBtn_Yes** can be used to submit the form; both function exactly the same.

For example, if the E-Form has **Custom Alpha 250**, **Custom Numeric 9** and **Custom Currency** as keywords and you want users to provide values for them in the new E-Form, then you must include an HTML Input field for each keyword. These fields allow users to enter keyword values, which will be saved in the new E-Form once it is submitted.

```
<INPUT type="hidden" name="OBDocumentType" value="###" />
<p> Custom Alpha 250 <input type="text" name="OBKey__155_1" size="20"></p>
<p> Custom Numeric 9<input type="text" name="OBKey__125_1" size="20"></p>
<p> Custom Currency <input type="text" name="OBKey__128_1" size="20"></p>
<INPUT type="submit" value="Submit" name="OBBtn_Save" />
```

Opening a read-only copy of the submitted form

After a user submits a new E-Form, LoginFormProc can display read-only copy of the E-Form to show the user the form was properly submitted.

This feature requires the following field on the custom HTML form:

- **OBWeb_ReturnReadOnlyCopy**

When this input is set to **true**, a read-only copy of the submitted form is displayed after the user submits the form. When this input is set to **false**, the read-only copy is not displayed.

For example:

```
<INPUT type="hidden" name="OBWeb_ReturnReadOnlyCopy" value="true" />
```

Note: When **OBWeb_ReturnReadOnlyCopy** is set to **true**, the redirection settings configured for **OBWeb_Redirect** are overridden. After submitting a form, the user will not be prompted to create a new form.

Redirecting the user to the custom form

Required fields on the custom HTML form:

- **OBWeb_Redirect**

After submitting a new E-Form, the user is prompted to create another new E-Form. Upon choosing **OK**, the user is redirected to the same custom HTML form. For this redirection to work, the value property on the **OBWeb_Redirect** hidden input field must be set to the URL of the custom HTML form.

For example:

```
<INPUT type="hidden" name="OBWeb_Redirect" value="http://servername/appnet/
file.htm">
```

The path to **OBWeb_Redirect** must be provided in the following format: **value="http://[server name]/[virtual directory]/[file.htm]"**.

If the user chooses **Cancel** when prompted to create a new form, then a different target URL must be provided. The **OBWeb_FinalTargetPage** hidden input field is available for this purpose. This field defines the page to which the user is directed, and it takes the same form as the **OBWeb_Redirect** input field. The user is directed to this location under the following conditions:

- The Hyland.Web.LoginFormProc **prompt** setting is set to **disable** in the Web Server's Web.config.
- The Hyland.Web.LoginFormProc **prompt** setting is set to **enable** in the Web Server's Web.config, and the user selects **Cancel** when prompted to create a new form.

Note: When **OBWeb_ReturnReadOnlyCopy** is set to **true**, the redirection settings are overridden. After submitting a form, the user will not be prompted to create a new form.

Setting the Language Parameter

If a form is submitted indirectly by another application, then the form must contain a hidden input field to specify the language parameter. The field's name is **LanguageParam**, and its value specifies the ISO 2-letter code for language and region.

For example, the **LanguageParam** field for English-United States would be the following:

```
<INPUT type="hidden" name="LanguageParam" value="en-us" />
```

The **LanguageParam** parameter is required in certain situations. Forms submitted through Chrome (or an automated process, such as cURL) require the parameter to pass in the locale, but forms submitted directly to LoginFormProc from Internet Explorer, Safari, or Firefox do not require the parameter. If a form submitted through Internet Explorer, Safari, or Firefox contains this parameter, then the parameter takes precedence over the browser's locale.

In certain instances the HTML form is not submitted through LoginFormProc directly. For example, a third-party application may be used to process the data and then submit the post data to LoginFormProc. In this situation, the application is required to pass the **LanguageParam** in as part of the post data.

Licensing

LoginFormProc requires an E-Forms license.

With the Archival API server license, the concurrent license is released immediately without having to wait the 5 minute session timeout required with a standard concurrent license.

If the **LoginFormProc** user is currently logged on to another OnBase application when the form is submitted, the user's session is maintained. This is true regardless of whether the system is licensed for Archival API.

Overview

FormPop allows users to view and edit E-Forms and Unity Forms using a simplified Web Client viewer interface, without any extra OnBase functionality. This allows users outside of OnBase to follow web links to view and edit forms in OnBase.

FormPop does not allow users to create new forms by following a FormPop link.

For a list of browsers that are supported by FormPop, see **FormPop and PDFPop Browser Requirements** in the **Web Server** module reference guide.

Note: FormPop is only supported using the HTML Web Client. Links are always opened in the HTML Web Client regardless of how the Web Server is configured.

Usage

FormPop functionality is described in the following sections:

- [Retrieving Forms Using FormPop on page 306](#)
- [Editing Existing Forms Using FormPop on page 306](#)

For additional information on the functionality available with forms, see the **E-Forms** or **Unity Forms** help files or module reference guides.

Retrieving Forms Using FormPop

You can use FormPop to retrieve and edit forms in OnBase by clicking a link to the form from a Web site or email message. You can also use the DocPop URL Creator to generate a link and then modify the generated URL, as shown in the example below:

`http://WebServer/AppNet/docpop/docpop.aspx?doctypeid=139`

becomes:

`http://WebServer/AppNet/docpop/FormPop.aspx?doctypeid=139`

For information on using the DocPop URL Creator, see the **DocPop** module reference guide.

After accessing a FormPop link, a document select list or form is displayed.

Editing Existing Forms Using FormPop

After accessing a FormPop link, edit the necessary fields and save or submit the form.

Configuration

The configuration settings for using FormPop are set in the Web Server's Web.config file. For information on FormPop configuration settings, see [FormPop Vars on page 307](#).

For information specific to configuring E-Forms or Unity Forms, see the **E-Forms** or **Unity Forms** module reference guides.

For information about the variables available in a FormPop query string, see the **DocPop** module reference guide, which contains a comprehensive list of query string variables.

FormPop Vars

FormPop-specific settings are located in the **Hyland.Web.FormPop** element of the Web Server's Web.config file. The only required setting is a data source. You can either configure one in the Web Server's Web.config or pass it along the query string. FormPop results are displayed using the HTML Web Client.

The following settings are located in the **Hyland.Web.FormPop** element of the Web Server's Web.config file.

username - Enter the user name to use with default login with FormPop, if you want to use a single user account for access. When **enableDefaultLogin** is set to **true**, users can automatically log on to FormPop using the credentials provided in the **username** and **password** settings.

password - Enter the password to use with default login with FormPop, if you want to use a single user account for access. When **enableDefaultLogin** is set to **true**, users can automatically log on to FormPop using the credentials provided in the **username** and **password** settings.

datasource - Enter the name of the data source to use with FormPop. This is a required value.

domain - Enter the domain to log on to if you are using Active Directory authentication.

embedded - Set this to **true** when you are embedding FormPop results in a custom Web page and you want the FormPop results to be displayed in a frame or iframe within the same browser window. When set to **false**, FormPop results are opened in a new window.

- If **embedded** is set to **true** and results are not embedded in another Web page, then the address bar and browser toolbars will be displayed when a user accesses the FormPop URL.
- If FormPop results will not be embedded in Web pages, set **embedded** to **false**. The address bar and toolbars will be hidden when FormPop results are displayed.

enableDefaultLogin - Set this to **true** to have FormPop use the **username** and **password** credentials specified in the **Hyland.Web.DocPop** element. Set this to **false** to have FormPop either attempt other authentication methods (if they are configured) or prompt the user for credentials.

enableHTTPLogin - Set this to **true** to pass login credentials to the server on the query string or to post them through an HTML form. Set this to **false** if FormPop should either attempt other authentication methods (if they are configured) or prompt the user for credentials.

enableAutoLogin - Set this to **true** to use domain credentials to log on to FormPop automatically. When this is set to **false**, FormPop either attempts other authentication methods (if they are configured) or prompts the user for credentials. If you enable this setting, ensure that the Web Server is configured for Active Directory authentication. See the **Legacy Authentication Methods** module reference guide for more information about Active Directory authentication.

Set **enableAutoLogin** to **true** if you are using Integration for Single Sign-On. If OnBase is configured for Active Directory or LDAP authentication, but you want to use Single Sign-On with FormPop, set both **forceSSOAutoLoginOverDomain** and FormPop's **enableAutoLogin** setting to **true**. For more information about Integration for Single Sign-On, see the **Legacy Authentication Methods** module reference guide.

enableHTTPDataSource - Set this to **true** to pass the data source on the query string. Set to **false** to use the FormPop data source in the Web Server's Web.config.

enableChecksum - If set to **true**, a checksum value will be added to the URL query string. To enable checksums, you are also required to enter a checksum key value in the FormPop **checksum** setting, which is used to create the checksum value in the URL. When a user attempts to retrieve a document using the URL, FormPop compares the checksum in the query string to the expected checksum. If the values match, the document is displayed. If the values do not match, the user is presented with an error. This is to prevent users from modifying query strings and accessing documents they should not access. If set to **false**, no checksum is created.

checksum - Enter the unique string value used as a key for external, dynamic checksum creation. This string value should not be well known. The **checksum** setting applies only when **enableChecksum** is set to **true** and an external automated process is being used to dynamically generate FormPop links.

Note: Configuration of this setting is required for checksum creation and validation.

- The Web Server web.config file also has an **enableChecksum** setting within the **<Hyland.Web.DocPop>** node that must be set to **true**. You must also set the **checksum** setting to the appropriate value within that node.
- The Application Server web.config file also contains a Pop integration checksum setting: **ChecksumKey**. This setting is used for checksum generation when the docID is used from outside of the Web Client solution (for example, in Workflow notifications). If you use this feature, the **ChecksumKey** value in the Application Server web.config file must match the **checksum** value in the **Hyland.Web.FormPop** element of the Web Server web.config file. For more information about checksum generation, please refer to the Hyland SDK.
- If you are using the Workflow action **Med - Send HL7 Message**, the Hyland.Web.FormPop **checksum** value should be empty. If an external process will generate the FormPop URLs and you want to use checksums, then a separate virtual directory for FormPop should be configured.

enableCoreQueryAPILicense - This setting requires OnBase to be licensed for Core Query API (Retrievals Per Hour). Set this setting to **true** if you want users to consume Core Query API licenses when using FormPop. Core Query API licenses help prevent the unnecessary consumption of Concurrent Client licenses. When this setting is set to **true**, a Core Query API license is consumed as soon as a user logs on to FormPop and is released immediately after the user logs off. When the **enableCoreQueryAPILicense** setting is set to **false**, a Concurrent Client license is used.

Note: Core Query API licenses are only available for external users.

AutoDisplayOneDocument - Set this setting to **true** to always display only the viewer for FormPop queries that return a single result. When this setting is set to **false**, FormPop displays both the hit list and the viewer for queries that return a single result. This behavior can be overridden by the **viewerOnlyForSingle** variable in the FormPop query string. The **viewerOnlyForSingle** variable has no effect when **AutoDisplayOneDocument** is set to **true**.

Embedding FormPop Results in a Web Page

By default, if you are embedding content from the OnBase Web Server into a web page, the page and the embedded content must be on the same domain. If your solution requires embedding Web Server content into a different domain, you can configure the Web Server to allow this. For more information, see the section on X-Frame-Options in the **Web Server** module reference guide.

INTERNATIONALIZATION AND LOCALIZATION BEST PRACTICES

OnBase provides localization support for many locations. For an outline of requirements and best practices for setting up OnBase in an international environment, see the following topic, [Requirements and Best Practices](#). For a list of supported languages and local formats, see [Supported Translations and Formats on page 313](#).

Requirements and Best Practices

The following is an outline of requirements and best practices for setting up the OnBase system in an international environment.

1. The most important difference, and the one that has the largest potential impact is the database collation.
 - For Japanese installations, the database collation must be: Case Insensitive, Kana Sensitive, Accent Sensitive, and Width Insensitive
 - For other non-English installations, the database collation must be set to: Case Insensitive, Accent Sensitive, and Width Insensitive
2. In the **onbase32.ini** file, the **compressmode** must be set at **2** for all non-English installations.
3. For Chinese and Korean installations, the width of the Web Client's Navigation Panel should be increased. The width can be resized by clicking and dragging the handle on the vertical border of the Navigation Panel.
4. When working in OnBase in a non-English language, users should have that language's specific version of .NET installed on their workstations.
5. In the Configuration module, fonts need to be set to a typeface that works with the language of most of the documents. For Japanese, this should be MS Mincho or MS Gothic (preferred).
6. For printing in right-to-left (RTL) languages, a custom print format can be created in the Configuration module to print the columns or rows on a page from right to left.
7. The correct language DLL needs to be installed for the system.

The following languages are supported for the OnBase Web Client: Arabic, Bosnian, Chinese, Croatian, Czech, Danish, Dutch, English, Finnish, French, German, Indonesian, Italian, Japanese, Korean, Malay, Norwegian, Polish, Portuguese, Romanian, Russian, Serbian, Slovenian, Spanish, Swedish, Thai, and Turkish.
8. A native language operating system is preferred, but not required. The correct language files must be installed on the system.
9. On the Application Server, ensure the **Language for non-Unicode programs** is set to the correct language when storing data in an ANSI database.
10. Install the appropriate language packs and supplemental language support packages on any server used in your OnBase deployment. This step ensures the server recognizes the user locale code page and correctly validates submitted data.

11. In the Web Client, localizable data (currency, number formats, etc.) is displayed in the format of the client workstation's regional settings. The system and user locales must match in the Windows Regional and Language Options when storing data in an ANSI database. The system locale is selected as the **Language for non-Unicode programs** on the **Advanced** tab. The user locale is selected under **Standards and formats** on the **Regional Options** tab.

Please also note the following:

- A value's format will change to the client machine's locale, but the content will not change. So an amount entered in dollars, such as \$5.45, will be displayed in Spain as 5,45 €.
- The OnBase Web Server supports only default formats for a locale; customizations are not supported. The following statement explains how formats are customized in Windows Server.
 - Default formats are those displayed by default when you select a **Format** from the **Formats** tab in the Region and Language applet. If you select a different date or time format, or if you change any formats accessed through the **Additional Settings** button, the Web Server will not respect the change.
- When the HTML Web Client is accessed through Firefox, it detects the locale using different settings. See [Locale Detection with Firefox on page 319](#).
- Document Auto-Names will always be based on the server's locale settings, because Auto-Name strings are generated by the server at the point of archiving.
- There is no support for localized time formats (%I1) in the Auto-Name string.

Note: For general information about locales, including definitions and types, please visit the following URL: <http://www.microsoft.com/globaldev/drintl/faqs/locales.msp>

12. Client workstations accessing the Web Server should have Internet Explorer's Auto-Select encoding option selected. This option is available from the **View | Encoding** menu in Internet Explorer.
13. Ensure the Web Client's Navigation Panel is wide enough to properly display all labels. In some languages, words may be cut off or wrapped because the Navigation Panel is too narrow. To widen it, click and drag the handle on the vertical border of the Navigation Panel.
14. Error messages generated by OnBase contain a message ID that is displayed to the right of the caption in the message box. Use this ID whenever contacting support to ensure that they correctly understand which message is being generated.

Note Considerations

Japanese characters entered into a note while Japanese regional settings are enabled cannot then be viewed in an environment using English regional settings. You cannot enter Japanese characters into a note while English regional settings are enabled.

The SYSTEM locale always has to remain Japanese.

Users entering text using the IME in some languages may notice that the text disappears when it reaches the length restriction. This is a known limitation of the IME.

Web.config Encoding

The Web Server's Web.config must be saved with UTF-8 encoding. Encoding is specified in the **xml** element, which is the first line of the Web.config file. The **encoding** attribute must be set to **UTF-8**.

Transaction Log Translations

By default, actions logged to the OnBase Transaction Log through Core Services applications are translated according to the locale set on the Application Server machine. You can change this behavior so that actions performed in Core Services applications are logged in a specific language regardless of the Application Server locale.

In OnBase Configuration, set the **Transaction Log Locale** to the language in which you want actions to be logged. This setting is configured under **Utils | Core-Based Settings**. After the Application Server's cache is reset, all actions performed in Core Services applications are logged in the selected language. For more information about this setting, see the OnBase Configuration help files.

Help Files Setup for Multiple Languages

The OnBase Web Client can display different translations of the help files to users in different locales. It accomplishes this by storing the different translations within subfolders of the Web Server's virtual directory.

When a user accesses the help files from the Web Client, the Web Client first checks its **Help** directory for a subfolder named after the language code for the user's locale. If that subfolder does not exist, the Web Client checks for the **en** subfolder (for the English translation). Finally, the Web Client checks for the files in the root of the Help directory.

To make multiple translations of the help files available to users in different locales, do the following:

1. On the server, open the virtual directory for the OnBase Web Client (e.g., AppNet).
2. Open the **Help** folder.
3. Create a new folder. Name it using the two-letter code for the users' language (according to ISO 639-1).

For example, for English, the folder would be named **en**. For Spanish, it would be named **es**.

Refer to the following table for available translations and their corresponding language codes.

ISO Code ^a	Language
de	German
en	English

ISO Code ^a	Language
es	Spanish
fr	French
ja	Japanese
pt	Portuguese

a. Language codes according to ISO 639-1

4. Copy the translated help files to the new folder. These files can be obtained from your solution provider.
For example, the Spanish translation of the Web Client help would reside in ..\AppNet\Help\es\WebClient. The Workflow help would reside in ..\AppNet\Help\es\WFLOW.
The translated help files are now available to Web Client users.
5. Repeat this procedure for each required translation.

Supported Translations and Formats

The OnBase Web Server supports several translations and local formats, as described in the following topics:

- [Supported Translations on page 314](#)
- [Supported Formats on page 315](#)

Supported Translations

The OnBase Web Server has been translated into several languages. The following translations are supported:

Note: To use a non-English language, ensure the language is selected as the **Language for non-Unicode Programs** in the Regional and Language Options on the users' workstations. If an Asian language is not specified for this setting, users will not be able to use that language.

ISO Code ^a	Language ^b
bs	Bosnian
de	German
en	English
es	Spanish
fr	French
hr	Croatian
hu	Hungarian
it	Italian
ja	Japanese
ko	Korean
nl	Dutch
pt	Portuguese
ro	Romanian
sr	Serbian (Cyrillic) Note: Limited Web Client support in Safari.
tr	Turkish
vi	Vietnamese
zh zh-cn zh-sg	Chinese (Simplified)

ISO Code ^a	Language ^b
zh-hk zh-mo zh-tw	Chinese (Traditional)

a. Language codes according to ISO 639-1. Region codes (for Chinese) according to ISO 3166-1 alpha-2.

b. Most of the supported languages referenced above have been translated from English, while some are in the process of being translated. Please check with your account manager or solution provider regarding your specific localization needs.

Tip: The ISO codes can be entered for the **DefaultUILocale** setting in the Web Server's Web.config, if **OverrideUILanguage** is set to **true**. The **OverrideUILanguage** and **DefaultUILocale** settings are used to override the language selected under the client workstation's regional settings.

Supported Formats

The OnBase Web Server supports the formats listed in the following table. The table is sorted by ISO codes for language¹ and region², which are displayed in the left column. The right column displays the supported formats by language and region. This table is continued on the following pages.

Note: In the Web Client, localizable data (currency, number formats, etc.) is displayed in the format of the client workstation's regional settings. See number 11 under [Requirements and Best Practices](#) for more information.

ISO Code	Supported Format
bs-ba	Bosnian (Bosnia and Herzegovina)
cs-cz	Czech (Czech Republic)
da-dk	Danish (Denmark)
de-at	German (Austria)
de-ch	German (Switzerland)
de-de	German (Germany)
de-li	German (Liechtenstein)
de-lu	German (Luxembourg)

1. Language codes according to ISO 639-1

2. Region codes according to ISO 3166-1 alpha-2

ISO Code	Supported Format
el-gr	Greek (Greece)
en-au	English (Australian)
en-bz	English (Belize)
en-ca	English (Canada)
en-cb	English (Caribbean) <hr/> Note: English (Caribbean) locale is defaulted to English (United States) formatting. <hr/>
en-gb	English (Great Britain)
en-ie	English (Ireland)
en-in	English (India)
en-jm	English (Jamaica)
en-my	English (Malaysia)
en-nz	English (New Zealand)
en-ph	English (Philippines)
en-sg	English (Singapore)
en-tt	English (Trinidad)
en-us	English (United States)
en-za	English (South Africa)
en-zw	English (Zimbabwe)
es-ar	Spanish (Argentina)
es-bo	Spanish (Bolivia)
es-cl	Spanish (Chile)
es-co	Spanish (Colombia)
es-cr	Spanish (Costa Rica)
es-do	Spanish (Dominican Republic)
es-ec	Spanish (Ecuador)
es-es	Spanish (Spain)

ISO Code	Supported Format
es-gt	Spanish (Guatemala)
es-hn	Spanish (Honduras)
es-mx	Spanish (Mexico)
ex-ni	Spanish (Nicaragua)
es-pa	Spanish (Panama)
es-pe	Spanish (Peru)
es-pr	Spanish (Puerto Rico)
es-py	Spanish (Paraguay)
es-sv	Spanish (El Salvador)
es-us	Spanish (United States)
es-uy	Spanish (Uruguay)
es-ve	Spanish (Venezuela)
fi-fi	Finnish (Finland)
fr-be	French (Belgium)
fr-ca	French (Canada)
fr-ch	French (Switzerland)
fr-fr	French (France)
fr-lu	French (Luxembourg)
fr-mc	French (Monaco)
hr-hr	Croatian (Croatia)
hu-hu	Hungarian (Hungary)
id-id	Indonesian (Indonesia)
it-ch	Italian (Switzerland)
it-it	Italian (Italy)
ja-jp	Japanese (Japan)
ko-kr	Korean (Republic of Korea)
ms-my	Malay (Malaysia)

ISO Code	Supported Format
nb-no	Norwegian, Bokmål (Norway)
nl-be	Dutch (Belgium)
nl-nl	Dutch (Netherlands)
nn-no	Norwegian Nynorsk (Norway)
no-no	Norwegian (Norway)
pl-pl	Polish (Poland)
pt-br	Portuguese (Brazil)
pt-pt	Portuguese (Portugal)
ro-ro	Romanian (Romania)
ru-ru	Russian (Russia)
sk-sk	Slovak (Slovakia)
sl-sl	Slovenian (Slovenia)
sr-rs	Serbian (Serbia) <hr/> Note: Limited Web Client support in Safari. <hr/>
sv-fi	Swedish (Finland)
sv-se	Swedish (Sweden)
th-th	Thai (Thailand)
tr-tr	Turkish (Turkey)
vi-vn	Vietnamese (Vietnam)
zh-cn	Chinese (China)
zh-hk	Chinese (Hong Kong)
zh-mo	Chinese (Macao S.A.R.)
zh-sg	Chinese (Singapore)
zh-tw	Chinese (Taiwan)

Locale Detection with Firefox

When the OnBase Web Client is accessed using Firefox, it uses the browser's configured language to determine the user's locale. To access Firefox's language settings, select **Tools | Options**. Language setup is accessed under **Content**. Ensure the user's language is listed first in the order of preference.

MODULE-SPECIFIC WEB.CONFIG SETTINGS

The following sections describe Web Server Web.config settings that are specific to other OnBase modules.

AFP or PCL Caching from Centera or Tivoli Web.config Settings

The following settings in the Web.config file of the Application server apply when the Application server is retrieving AFP or PCL documents from a Centera or Tivoli device:

- **pmCacheLocation** is the location on the Application server where the cache files are stored.
- **pmCacheSize** is the high water mark for the cache, measured in megabytes. When this point is reached, cache files will be deleted to get below the **pmCacheSize**, starting with the oldest files.
- **pmCacheTimeout** is the amount of time in minutes that files will exist in the cache.

Application Client Connector Settings

The **UseFolderPopViewer** keys apply only to the Application Client Connector.

The **value** of the **UseFolderPopViewer** key is either **true** or **false**. If set to **true**, FolderPop is used to retrieve and display documents in the ACC Viewer. If set to **false**, the legacy document viewer is used to retrieve and display documents in the ACC Viewer. By default, the value is set to **true**.

Note: The FolderPop search results list always uses an HTML context menu, even if the **WebClientType** key is set to **activex**.

To change this key, locate the **<add key="UseFolderPopViewer"** key under the **<appSettings>** node and change the **value** attribute to **true** or **false**.

Application Enabler Web.config Settings

If you want to allow Application Enabler to work with the Web Client, you must set a specific setting on the server. In the Web.config file the following parameter must be set equal to **true**: **sv_AppEnablerIntegration**

If you want Application Enabler to automatically launch when the user enters an Application Enabler supported feature, you must set the following parameter to **true**:

sv_LaunchAppEnabler

The following is an example from a Web.config file configured for using with Application Enabler:

```
<!-- AppEnabler Vars -->
<add key="sv_AppEnableIntegration" value="true" />
<!-- Enable/disable AppEnabler integration -->
<add key="sv_LaunchAppEnabler" value="true" />
```

Collaboration Web.config Settings

The Collaboration module uses the Web Server's Web.config file to control specific settings:

- Collaboration Context button
- My Workspaces Control Bar
- Workspace Retrieval Control Bar

To activate any of the above items, ensure that the **enabled** switch is set to **true**. See example below:

```
<NavigationPanel>

<Context>

<ContextInfo>
<name><![CDATA[Collaboration]]></name>
<displayName><![CDATA[Collaboration]]></displayName>
<displayOrder>4</displayOrder>
<icon><![CDATA[NavPanel/CollaborationUp.gif]]></icon>
<enabled>true</enabled> <!--Turns Collaboration Context Button on-off-->
</ContextInfo>

<ControlBar>
<name><![CDATA[AllWorkspaces]]></name>
<displayName><![CDATA[My Workspaces]]></displayName>
<path><![CDATA[./Collaboration/AllWorkspaces.aspx]]></path>
<icon><![CDATA[AllWorkspaces.gif]]></icon>
<enabled>true</enabled> <!--Turns AllWorkspaces Control Bar on-off-->
</ControlBar>

<ControlBar>
<name><![CDATA[FindWorkspace]]></name>
<displayName><![CDATA[Workspace Retrieval]]></displayName>
<path><![CDATA[./Collaboration/FindWorkspace.aspx]]></path>
<icon><![CDATA[SearchWorkspaces.gif]]></icon>
```



```
<enabled>true</enabled> <!--Turns FindWorkspace Control Bar on-off-->
</ControlBar>
</Context>
```

DKT

Enabling DKT

The Document Knowledge Transfer module uses the Web Server's Web.config file to activate the Knowledge Transfer context. Set **enabled** to **true** to ensure the **Knowledge Transfer** is available from the Web Client's Context drop-down list. See the example below:

```
<ContextInfo>
<name><![CDATA[KnowledgeTransfer]]></name>
<displayName><![CDATA[Knowledge Transfer]]></displayName>
<displayOrder>3</displayOrder>
<icon><![CDATA[NavPanel/KnowledgeTransferUp.gif]]></icon>
<enabled>true</enabled> <!--Turns DKT Context Button on-off-->
</ContextInfo>
```

Prompting Users About Unread Documents

The **PromptWithUnreadDKTDocs** setting allows you to prompt users about unread DKT documents that have been assigned a deadline date after logging in to the Web Client. If the value is set to **true**, users will be prompted. If the value is set to **false**, users will not be prompted.

EDMS Web.config Settings

To use the EDM Briefcase from the OnBase Web Client, the Briefcase must be enabled in the Web Server's Web.config. These settings are configured in the Web Server's Web.config file.

Enabling the EDM Briefcase

To enable EDM Briefcase, ensure **EnableBriefcaseEDM** is set to **true** in Web.config. If **EnableBriefcaseEDM** is set to **true**, but a user does not have the EDM Briefcase installed on the client workstation, an error is displayed when the user attempts to check out the document. Before enabling the EDM Briefcase, ensure all users who will be checking out documents have the EDM Briefcase installed on their workstations.

Note: If **EnableBriefcaseEDM** is set to **false**, users with rights to check out documents can save OLE documents locally using the **Check Out** right-click option from the Document Search Results list. To check the document in, the user must access the **Documents Checked Out** pane (enabled through the **VersionControl** Control Bar setting) and check the document in from the location where the document was stored on the file system.

Configuring Settings

For the **Briefcase** option to be available from the Document context, the **Briefcase** setting must be enabled:

```
<name><![CDATA[Briefcase]]></name>
<displayName><![CDATA[Briefcase]]></displayName>
<path><![CDATA[Briefcase.aspx]]></path>
<icon><![CDATA[Briefcase_Small.gif]]></icon>
<enabled>true</enabled> <!--Turns VersionControl
Control Bar on-off-->
```

For the **Briefcase Options** option to be available from the User context, the **BriefcaseOptions** setting must be enabled:

```
<name><![CDATA[BriefcaseOptions]]></name>
<displayName><![CDATA[Briefcase Options]]></displayName>
<path><![CDATA[BriefcaseOptions.aspx]]></path>
<icon><![CDATA[versioncontrol.gif]]></icon>
<enabled>true</enabled> <!--Turns Options Control Bar on-off-->
```

For the **Documents Checked Out** option to be available from the Document context, the **VersionControl** setting must be enabled:

```
<name><![CDATA[VersionControl]]></name>
```

```
<displayName><![CDATA[Version Control]]></displayName>
<path><![CDATA[VersionControl.aspx]]></path>
<icon><![CDATA[versioncontrol.gif]]></icon>
<enabled>true</enabled><!--Turns VersionControl Control Bar on-off-->
```

For the **Document Templates** option to be available from the Document context, the **DocumentTemplates** setting must be enabled:

```
<name><![CDATA[DocumentTemplates]]></name>
<displayName><![CDATA[Document Templates]]></displayName>
<path><![CDATA[DocumentTemplates.aspx]]></path>
<icon><![CDATA[Document_Template.gif]]></icon>
<enabled>true</enabled><!--Turns Document Templates Control Bar on-off-->
```

Integration for Esri Web.config Settings

To allow users to access the Integration for Esri Web Client mapping functionality from the Web Client, at least one of the following options must be enabled within the Web Server's web.config file: the **View Map** button or the **Open Map Viewer** menu option.

To activate either of these items in the Web Client, you must ensure that the relevant **<enabled>** element is set to **True**. See the following sections for more information:

- [Enabling the View Map Button on page 324](#)
- [Enabling the Open Map Viewer Option on page 325](#)

Enabling the View Map Button

For the **View Map** button to be available in the top-right corner of the Web Client, the **<enabled>** element of the **Maps** setting must be set to **True**. To do so, follow these steps:

1. Open the Web Server web.config file using a text editor such as Notepad.
2. Locate the **Maps** setting. For example:

```
<ContextInfo>
  <name><![CDATA[Maps]]></name>
  <displayName><![CDATA[Maps]]></displayName>
  <displayOrder>3</displayOrder>
  <icon><![CDATA[]]></icon>
  <enabled>True</enabled>
</ContextInfo>
```

3. Set the **<enabled>** element to **True**.
4. Save and close the web.config file.
5. Restart IIS.

Enabling the Open Map Viewer Option

For the **Open Map Viewer** option to be available from the main menu of the Web Client, the **<enabled>** element of the **OpenMapView** setting must be enabled. To do so, follow these steps:

1. Open the Web Server web.config file using a text editor such as Notepad.
2. Locate the **OpenMapView** setting. For example:

```
<ControlBar>
  <name><![CDATA[OpenMapView]]></name>
  <displayName><![CDATA[Open Map Viewer]]></displayName>
  <path><![CDATA[blank.aspx]]></path>
  <icon><![CDATA[]]></icon>
  <enabled>True</enabled>
</ControlBar>
```

3. Set the **<enabled>** element to **True**.
4. Save and close the web.config file.
5. Restart IIS.

StatusView Web.config Settings

Once the Web Server is installed, its Web.config file requires no modification for StatusView; the StatusView context and modes are enabled by default. To check whether StatusView is enabled, see the following topic.

Ensuring StatusView is Enabled

The following steps outline the Web Server Web.config settings you can check to ensure StatusView is enabled:

1. Ensure the following setting is set to true to make the Web Server context available from the OnBase Web Client:

```
<ContextInfo>
  <name><![CDATA[StatusView]]></name>
  <displayName><![CDATA[StatusView]]></displayName>
  <displayOrder>5</displayOrder>
  <icon><![CDATA[NavPanel/StatusView_16x16.png]]></icon>
  <enabled>True</enabled>
</ContextInfo>
```

2. Ensure the following setting is set to true to enable the **My Layouts** option:

```
<ControlBar>
  <name><![CDATA[MyLayouts]]></name>
  <displayName><![CDATA[MyLayouts]]></displayName>
  <path><![CDATA[./StatusView/MyLayouts.aspx]]></path>
  <icon><![CDATA[NavPanel/My_Views_16x16.png]]></icon>
```

```
<enabled>True</enabled>  
</ControlBar>
```

Accommodating Very Large Folder & Workflow Solutions

When you save the configuration for folder or Workflow portlets, you may encounter one of the following errors:

- Operation is not valid due to the current status of the object.
- Message: Error during serialization or deserialization using the JSON JavaScriptSerializer. The length of the string exceeds the value set on the maxJsonLength property. Parameter name: input.

These errors typically occur if the folder or Workflow portlet configuration dialog box contains a very large number of folders or queues.

As a best practice, if your system has a very large number of folders and queues, perform portlet configuration using an account with privileges to fewer folders or queues. Doing so should prevent the errors and also make it easier to find the folders or queues you want to display in the portlet.

If using a different user account is not an option, then increase the **aspnet:MaxJsonDeserializerMembers** setting in the Web Server's Web.config file.

- If you are configuring a folder portlet, ensure the setting's value exceeds the total number of folders in your system.
- If you are configuring a Workflow portlet, ensure the setting's value exceeds the total number of Workflow life cycles and queues in your system.

If you expect your folder or Workflow solution to continue to grow, then you may need to increase the value further to accommodate the expected growth.

Web Parts for Microsoft SharePoint Settings

If you are using the Silverlight Web Parts with OnBase Web Parts for Microsoft SharePoint, you must modify the Web Server's Web.config file to accommodate your authentication scheme.

See the following topics for more information:

- [Basic Authentication on page 327](#)
- [Active Directory Authentication on page 327](#)

For complete information about installing and configuring Web Parts, see the Web Parts for Microsoft SharePoint module reference guide.

Basic Authentication

To use the Silverlight Web Parts with basic authentication, you must configure the OnBase Web Server as described in the following steps.

Note: When basic authentication is used, the account specified in the OnBase Web Server's Web.config file is used to interact with OnBase. Any rights and document permissions assigned to this account are reflected within the Silverlight Web Parts. In addition, the Document History for documents accessed through the Silverlight Web Parts will display this user regardless of the number of users who worked on the document. If auditing and user privileges are a concern, then Active Directory authentication should be used.

1. Open Web.config from the Web Server's virtual directory, which is named **AppNet** in a default installation.
2. Locate the Silverlight Web Parts App Settings.

```
<!-- Silverlight Web Parts App Settings -->
<add key="SLDefaultUsername" value="" />
<add key="SLDefaultPassword" value="" />
</appSettings>
```

3. Provide values for **SLDefaultUsername** and **SLDefaultPassword** using the OnBase account you configured.
 - a. Replace the **SLDefaultUsername** value with the account's user name.
 - b. Replace the **SLDefaultPassword** value with the account's password.
4. Locate the following element:
<httpTransport authenticationScheme="Negotiate"/>
5. Change the **authenticationScheme** from **Negotiate** to **Anonymous**. The element should now match the following:
<httpTransport authenticationScheme="Anonymous"/>
6. Save and close the Web.config file.

Active Directory Authentication

If OnBase and the Web Server are configured for Active Directory authentication, then you must enable NTLM authentication in the OnBase Web Server's web.config file.

1. Open Web.config from the Web Server's virtual directory, which is named **AppNet** in a default installation.
2. Locate the following element:
<httpTransport authenticationScheme="Negotiate"/>

3. Change the **authenticationScheme** from **Negotiate** to **Ntlm**.

Note: This value is case sensitive. Be sure to use a capital **N** followed by **tlm** in lowercase.

The element should now match the following:

<httpTransport authenticationScheme="Ntlm"/>

4. Save and close the Web.config file.

Virtual Print Driver Web.config Settings

To enable the Virtual Print Driver in the OnBase Web Client, open the Web Server's web.config file. Under **appSettings**, set the following to **true**:

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

When enabled, this setting allows users to archive documents to OnBase using the Virtual Print Driver and the OnBase Web Client, provided that the following are true:

- OnBase is licensed for the Virtual Print Driver.
- The Virtual Print Driver is installed on the user's workstation.
- The user has the **Create** privilege for at least one Document Type.
- The user is using the ActiveX Web Client.

Note: This functionality is not available in the HTML Web Client.

Workflow Web.config Settings

There are several Web Server web.config settings that influence the Workflow module.

If you want to open a specific queue within Workflow by default, set **defaultContext** to **Workflow**, leave the **defaultControlBar** blank, and set **defaultContextID** to the queue number. The queue number is displayed in the Studio when a queue is selected during configuration.

DefaultContextInfo — `<DefaultContextInfo>`

```
<defaultContext>Workflow</defaultContext>
```

```
<defaultControlBar>Lifecycles</defaultControlBar>
```

```
<defaultContextID>253</defaultContextID>
```

```
</DefaultContextInfo>
```

When you login to the Web Client, the Workflow queue with ID 253, should be opened by default.

If there is no queue with that ID, the Workflow will still be opened by default, but no queue should be opened.

Note: If an **Auto-Open Queue** is specified in the OnBase Client's **Workstation Options** dialog box, it will override the queue specified to open by default in the web.config file.

Note: When Workflow is opened by default, when you click the **Back** button, the Retrieval context is available when you click the **Retrieve** button.

showQueueCounts — Queue counts do not display by default. In **web.config** the **showQueueCounts** is set to false by default. This means that in Workflow, once the life cycle is expanded, there is no count of how many documents are in each queue.

If the **showQueueCounts** is set to true, the core runs a query to count the documents in the Workflow queues and displays this number.

WorkflowMaxResults — This option specifies the maximum number of results displayed in a Workflow filter results list. The default value is 2000.

ShowCombinedInbox — This option controls whether or not the Combined Inbox is available. The Combined Inbox is enabled by default. Set **ShowCombinedInbox** to **false** to disable the Combined Inbox.

WorkflowLayout — This setting allows the layout of Workflow to be specified.

When the value of this setting equals "**selectable**", a **Workflow Layout Options** button is displayed in the Web Client that allows users to define the layout of Workflow. Within the Web Client, users can select from **Horizontal Layout**, **Vertical Layout**, or **Separate Viewer Layout**.

When the value of this setting equals "**horizontal**", users will receive the layout that has the document viewer horizontally spanning the Workflow interface.

When the value of this setting equals "**vertical**", users will receive the layout that has the document viewer vertically spanning the Workflow interface.

When the value of this setting equals "**separateviewer**", users will receive the layout that has the document viewer in a separate window from the Workflow interface.

QueueAnnotationMap — You can configure a specific default annotation for a specific queue. When you configure this, the **Toggle Annotation** button is toggled on by default in the client and the annotation type defined is selected by default when a document is accessed from the queue specified. To define this, the following setting must be added to the web.config file within the **<appSettings>** node; this setting is not in the web.config file by default:

```
<add key="QueueAnnotationMap" value="<queue ID#>=<Annotation Type ID#>, ..." />
```

Specify the ID number for the queue you want to associate with a specific annotation type where <queue ID#> is. Do not enclose the value in carets (<>). Specify the ID number for the annotation you want to associate with the specified queue where <Annotation Type ID#> is. Do not enclose the value in carets (<>).

Viewer Vars

WORKFLOWMENU — When workflowMenu is set to **true**, the Workflow right-click option is available from the open document right-click menu.

WORKFLOW RELATED DOCUMENTS — The **DisplayRelatedDocuments** setting controls tab focus. If this is set to **always**, the focus will always be on the **Work Folder** tab upon document selection in a queue. If this is set to **never**, the focus will always be in the **Documents** tab upon document selection in a queue. If this is set to **document**, the focus will be on the **Work Folder** tab when related documents exist for the selected document in a queue. Otherwise, focus will remain on the **Documents** tab.

WINDOW SIZE — The **WorkflowUserInteractionHeight** setting controls the size of the top half of the Workflow window. This setting is measured in pixels. The minimum value is 150. The default value is 375.

WorkView Settings in the Web.config File

The Web Server's web.config file controls various features in the Web Client. Within this file is a WorkView section that controls WorkView specific functionality. The following is an example of this section:

```
<!-- WorkView Vars -->
<add key="WVMaxResults" value="1000"/>
<add key="WVFilterCount" value="false"/>
<add key="displayCreatedEForms" value="true"/>

<ContextInfo>
<name><![CDATA[WorkView]]></name>
<displayName><![CDATA[WorkView]]></displayName>
<displayOrder>2</displayOrder>
<path><![CDATA[NavPanel/WorkViewUp.gif]]></path>
<enabled>true</enabled>
<!--Turns WorkView Context Button on-off-->
</ContextInfo>
```

The **WVMaxResults** setting allows you to specify the maximum number of objects displayed for unconstrained filter results initiated from a filter bar.

The **WVFilterCount** setting allows you to turn on or turn off the counts displayed for filters. Filters that have user entry constraints configured do not have filter counts displayed regardless of this setting. If true, counts will be displayed in the filter bar displays. Filter counts shown reflect the number of objects filters return based on filter configuration. If false, counts will not be displayed. By default, counts are turned off.

Caution: If the **WVFilterCount** setting is enabled, it may negatively impact performance.

The **displayCreateEForms** setting allows you to specify that the **View EForm Before Creating** option is selected by default when users create E-Forms from within a **WorkView** object.

The **<ContextInfo>** element named **WorkView** controls the display of the **WorkView** toolbar button. If the **<enabled>** value is equal to **true**, the button is displayed. If the **<enabled>** value is equal to **false**, the button will not be displayed.

Setting the Maximum Display Results

You can specify the maximum number of results displayed at one time in filter results. This is specified in the server's **web.config** file. Within this file, you will find the following entry:

```
<!-- Web Server Vars -->
<add key="WVMaxResults" value="1000" />
```

Set the value to equal the maximum number of results that you want displayed at one time.

Setting WorkView to Open By Default

If users have no need to access the retrieval functionality in the Web Client, **WorkView** can be configured to open by default upon login. To do so, the following needs to be set in the **Web.config** file of the Web Server.

```
<DefaultContextInfo>
  <defaultContext>WorkView</defaultContext>
  <defaultControlBar>OpenWorkView</defaultControlBar>
  <defaultContextID>(valid Application ID)</defaultContextID>
</DefaultContextInfo>
```

The **defaultContext** setting should be set with the **WorkView** value.

The **defaultControlBar** setting should be set with the **OpenWorkView** value.

The **defaultContextID** should be set to the application ID of the application that should be selected by default. If no application ID is specified, **WorkView** will open with no application selected by default.

The following best practice recommendations were assembled by a team of OnBase subject matter experts. They represent the accumulation of years of experience installing and configuring OnBase solutions.

The following recommendations are general in nature, and are applicable to most OnBase solutions and network environments. Depending on your solution design and your organization's needs, not all of the best practice recommendations listed below may apply to, or be recommended for, your OnBase solution.

Carefully consider the impact of making any changes, including those listed below, to your OnBase solution prior to implementing them in a production environment.

Recommendations are organized in the following categories:

General on page 332 — This topic contains general guidelines that apply to all Web Server deployments, including recommendations for configuring the Web Server hardware and software environment and for troubleshooting the Web Server.

High-Security Deployments on page 339 — This topic provides guidelines specific to high-security deployments.

Load-Balanced Deployments on page 339 — This topic provides guidelines specific to load-balanced deployments.

General

The following are general guidelines for all Web Server deployments. Read these guidelines before installing and configuring the Web Server.

- [Installation Recommendations on page 332](#)
- [Antivirus/Backup/Indexing Software Configuration on page 333](#)
- [IIS and ASP.NET Configuration for Web Server Autologin on page 333](#)
- [Application Pool Configuration on page 337](#)
- [Overlays on page 338](#)
- [Troubleshooting on page 338](#)

Installation Recommendations

When preparing to install the Web Server, keep the following recommendations in mind.

1. Install the OnBase Web Server on a clean installation of an operating system.
2. When installing the Web Server and Application Server on separate machines, install the Application Server on the machine with the greater processing power. When users access documents through the Web Server, the majority of the processing is performed by the Application Server.

3. A Gigabit Ethernet connection to the file server and minimal latency connection to the database server are recommended.
4. Name the new subdirectory where you are installing the Web Server the same name that you plan to name your Web application/virtual directory.
5. Assign a unique application pool to each separate Web application/virtual directory you plan to operate. More information about application pool configuration is provided under [Application Pool Configuration on page 337](#).
6. Do not assign the Local System account as the identity account. This account has elevated privileges and can pose a significant security risk.
7. To ensure the security of highly sensitive information being transmitted through the Internet, use an HTTPS binding encryption.
8. If you install the Web Server manually, set the maximum log size for the OnBase Log in the Event Viewer to **16384** and select **Overwrite events as needed**. If you use the Server Side Components Installer to install the Web Server, these settings are automatically configured by the installer.
9. Use a separate client workstation during installation for all Web Client testing of the Web Server installation. If you encounter a server configuration issue during testing, attempt to recreate the issue using the browser on the server machine to display a more detailed description of the error.
10. If you are running your OnBase solution in a virtual environment, thoroughly test your solution prior to putting it into production.

Antivirus/Backup/Indexing Software Configuration

When configuring the Web Server's software environment, ensure antivirus, backup, and indexing software applications are configured correctly.

1. Antivirus software running on a Web server or client workstation may have adverse effects on system performance. To prevent performance issues on servers running McAfee VirusScan, disable ScriptScan on these servers. To prevent decreased performance on clients running VirusScan Enterprise 8.0i, upgrade to VirusScan Enterprise 8.5i. This upgrade resolves an issue related to decreased performance.
2. Disable antivirus, backup, and indexing software from scanning the server's virtual directories as well as the ASP.NET Temporary Files folder. Consult your antivirus, backup, or indexing service software's documentation for other recommended settings for Web servers.

For more information about antivirus software configuration, see "Impact of Running Antivirus Software on the OnBase Web Server" in the Web Server module reference guide.

IIS and ASP.NET Configuration for Web Server Autologin

The following topics describe the recommended IIS security and ASP.NET settings for the Web Server and Application Server when either interactive or non-interactive autologin is used. These recommendations are appropriate for all browser-based applications that use the OnBase Web Server.

ASP.NET impersonation is recommended for the Application Server, but it is not a requirement. If impersonation is not used, ensure the Application Server's identity account satisfies the criteria specified. The App Pool Identity and Local Service accounts would not satisfy these criteria for the Application Server.

These notes are organized under the following topics:

- [Overview on page 334](#)
- [Interactive Autologin on page 334](#)
- [Non-Interactive Autologin on page 335](#)
- [Other Important Notes on page 337](#)

Overview

The following table provides an overview of authentication settings for the Web Server and Application Server.

	Standard OnBase Authentication	Non-Interactive Autologin (NT/LDAP)	Interactive Autologin (NT/LDAP)
Web Server Virtual Directory	Anonymous Access	Integrated Windows authentication	Anonymous Access
Web Server Web.config	No impersonation needed	No impersonation needed	No impersonation needed
App Server Virtual Directory	Anonymous Access	Anonymous Access	Anonymous Access
App Server Web.config	Enable impersonation with a domain account that has modify privileges to the disk groups.	Enable impersonation with a domain account that has modify privileges to the disk groups and can query Active Directory.	Enable impersonation with a domain account that has modify privileges to the disk groups and can authenticate users against Active Directory.

Interactive Autologin

Interactive autologin prompts the user for credentials before granting the user access to OnBase. Interactive autologin presents stronger security because of this extra check.

The following topics outline recommended IIS security and ASP.NET settings for interactive autologin. An explanation of why each setting was chosen follows each table.

Web Server

The following table displays recommended Web Server IIS security and ASP.NET settings for interactive autologin.

Component	Recommended Setting
IIS	Anonymous Access
Application Pool Identity	App Pool Identity
Impersonation	N/A

Explanation:

- Integrated Windows authentication is not needed because the user is interactively providing credentials, allowing Anonymous Access to be the appropriate security setting.
- The App Pool Identity account without impersonation is appropriate because the ASP.NET worker process does not need elevated domain privileges.

Application Server

The following table displays recommended Application Server IIS security and ASP.NET settings for interactive autologin.

Component	Recommended Setting
IIS	Anonymous Access
Application Pool Identity	App Pool Identity
Impersonation	Domain user account with the Read Group Membership permission

Explanation:

- Anonymous Access is appropriate because the request is coming from the Web Server and not directly from the user.
- The identity or impersonation account needs the Account Operator role so that it can authenticate the user. It must also have permissions to the OnBase disk groups to retrieve content.

Non-Interactive Autologin

Non-interactive autologin obtains the username and domain from the browser using integrated Windows authentication, allowing the user to log on to OnBase without entering credentials.

The following topics outline recommended IIS and ASP.NET security settings for non-interactive autologin. An explanation of why each setting was chosen follows each table.

Web Server

The following table displays recommended Web Server IIS security and ASP.NET settings for non-interactive autologin.

Component	Recommended Setting
IIS	Integrated Windows authentication
Application Pool Identity	App Pool Identity
Impersonation	N/A

Explanation:

- Integrated Windows authentication is necessary to obtain the username and domain from the browser. Users must have NTFS **Read** permissions to read the Web Server content directory.
- The App Pool Identity account without impersonation is appropriate because the ASP.NET worker process does not need elevated domain privileges.

Application Server

The following table displays recommended Application Server IIS security and ASP.NET settings for non-interactive autologin.

Component	Recommended Setting
IIS	Anonymous Access
Application Pool Identity	App Pool Identity
Impersonation	Domain user account that has domain querying rights.

Explanation:

- Anonymous Access is appropriate because the request is coming from the Web Server and not directly from the user.
- The identity or impersonation account needs domain querying rights to look up the user's group in Active Directory.

Note: If you are using a module that directly communicates with the Application Server (e.g., Disconnected Scanning), then Anonymous Access may not be the appropriate setting for non-interactive Active Directory authentication.

Other Important Notes

When configuring IIS security and ASP.NET settings for your solution, also consider the following notes and recommendations:

1. Place a firewall between the Web Server and Application Server to ensure that the Application Server can only receive requests from a specific Web Server.
2. When Anonymous Access is used, the Anonymous Access account configured in IIS is still restricted by its NTFS permissions. Anonymous Access means that the user initiating the request is not being validated by IIS, but the Anonymous Access account is still key to everything.
3. If there is no need to authenticate the user who is accessing the Application Server, then there is no need to use integrated Windows authentication on the Application Server. If integrated Windows authentication is used on the Application Server, then the user account running the ASP.NET worker process on the Web Server will be authenticated for each request. The recommended way to restrict access to the Application Server is with a properly configured firewall.
4. In non-interactive authentication, the Web Server is not attempting to validate the user. This task is performed by the Application Server, which is why the domain account used for impersonation needs extra privileges.
5. IIS must be configured to use at least one authentication method. If no authentication method is selected, then the web application won't work.

Application Pool Configuration

The following tips provide best practices for application pool configuration in IIS.

From the application pool's **Advanced Settings** dialog box, ensure the following settings are applied:

Setting	Value
.NET CLR Version	v4.0
Enable 32-Bit Applications	False
Managed Pipeline Mode	Integrated
Queue Length	65535
Start Mode	AlwaysRunning
Limit Interval	0

Setting	Value
Identity	Set Network Service as the predefined security account, or use another account with least domain privileges. It is recommended that you use the Network Service account combined with impersonation. For high-security deployments, follow Microsoft best practices. Information about creating a custom least-privileged service account is available at: http://msdn.microsoft.com/en-us/library/ms998297.aspx .
Idle Time-out (minutes)	0
Ping Enabled	False
[Rapid-Fail Protection] Enabled	False
Regular Time Interval (minutes)	0

Overlays

The following are recommendations for configuring overlays that do not significantly inhibit your system's performance. System performance can be improved by:

- Using black and white overlays instead of color overlays. If color is required, you should save the image with the smallest color depth possible.
- Decreasing the file size of your overlays (for example, decrease the image's DPI and resolution).
- Storing overlay images using compression.

Note: Compressed images are decompressed when being viewed as an overlay on a document. The image's file size is significantly larger when decompressed.

Troubleshooting

The following are general recommendations for troubleshooting the Web Server. For information about specific issues and their solutions, see [Troubleshooting on page 159](#).

1. Prior to contacting support, connect to the **[dmsVirtualRoot]\Diagnostics\diagnostics.aspx** page from the problematic client workstation to run an extensive diagnostics test. For more information about the Web diagnostics page, see [Web Diagnostics Page on page 198](#).
2. For **HTTP 404 - File not found** errors, use the test.gif file in the **[dmsVirtualRoot]\Diagnostics** directory to see whether the Web site is working. If you can't access test.gif, then the Web site is not working.

3. If users cannot log on and the Web Server is using a domain account for impersonation or identity, check the validity of the domain account. It may be locked (e.g., because the password was changed).
4. Check the OnBase Log and the Application and System logs in the Windows Event Viewer for more detailed event messages.

High-Security Deployments

The following recommendations apply to Web Server deployments in high-security environments.

1. Install the Web Server and Application Server on separate machines and place a firewall between them. This configuration helps protect the OnBase database and disk groups from unauthorized access.
2. Read “Building Secure ASP.NET Applications: Authentication, Authorization, and Secure Communication” for information to help you plan a secure deployment. This article is available at <http://msdn.microsoft.com/en-us/library/aa302415.aspx>.
3. Follow Microsoft best practices for high-security deployments. To follow Microsoft best practices, you may need to install the Web Server manually.
For manual installation steps, see the Web Server Manual Installation Checklist in the Web Server module reference guide.
4. Only the group containing the worker process account should have access to the directory where the OnBase Web Server is installed.

Load-Balanced Deployments

The following recommendations apply to Web Server deployments that use load balancing.

1. Load balancing can be configured using either hardware load-balancing devices or software solutions, like Microsoft’s Network Load Balancing service. Hardware load-balancing devices are recommended. The load-balancing system must be capable of maintaining client affinity (or persistence) for a specific Web Server, and hardware devices typically offer more flexible client affinity options.
2. When a load balancer is placed in front of the Web Server, ensure the **dmsVirtualRoot** in the Web Server Web.config uses the load balancer’s address rather than the server’s.
3. Network and disk I/O hardware should be optimized for performance and redundancy. Two network ports can reduce server bottlenecks by using a segmented network for external and internal requests, where external requests are sent to the Web clients and internal requests are sent to the file and database servers.

Overview

The Feature Matrix lists options and features available throughout the OnBase platforms and shows which client supports each feature. The Feature Matrix outlines features available in the following OnBase platforms:

- OnBase Client
- ActiveX Web Client
- HTML Web Client, which uses no ActiveX controls and is supported across multiple platforms
- Unity Client

For more information about each Web Client type, see the Web Client Types topic in the Web Server module reference guide.

License-Specific Considerations

License-specific options and features are only listed if the module is able to be accessed in more than one platform. For example, because Workflow can be accessed in the OnBase Client, Web Client, and Unity Client, Workflow options are listed.

Module-specific interfaces are not listed in this guide. For example, Workflow options that appear in license-neutral areas (e.g., the Document Viewer and Document Select List) are displayed, but features found within the Workflow interface are not displayed. See the next section for a list of contexts covered in this guide.

For more information on which modules are available in which OnBase platforms, see the Platform Availability Guide.

Other Considerations

When using this guide, be aware that listed features may differ in how they are labeled and located within each platform. For example, while the menu option **Send To | Mail Recipient (with Advanced Options)** is listed as available in all platforms, it is only labeled as such in the OnBase Client. In the Unity Client, advanced options are displayed by default when you attempt to email a document within the Unity Client. In the Web Client, advanced options are available after selecting **Send To | Mail Recipient**.

If you have questions on where a feature is accessed within a specific platform, refer to the appropriate module reference guide and search for the desired functionality.

Categories of Features

Features are broken down into the following categories. If you are viewing this document as a PDF, click a category to quickly navigate to it.

- [Search & Retrieval on page 342](#)
- [Document Select List on page 345](#)
- [Viewer—Standard—Image Document on page 351](#)
- [Viewer—Text Document Specific on page 367](#)
- [Viewer—PCL Document Specific on page 370](#)
- [Viewer—AFP/RSS Document Specific on page 370](#)
- [Viewer—OLE Document Specific on page 371](#)
- [Viewer—HTML/E-Form/Unity Form Document Specific on page 373](#)
- [Viewer—Import/Scan/Index on page 375](#)
- [Print Options on page 378](#)
- [Content Management on page 380](#)
- [User Options on page 387](#)
- [Administration on page 391](#)

Search & Retrieval

The following table lists document search and retrieval features and where they are supported.

Search & Retrieval X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Custom Viewer Support—Configured custom viewers using the OnBase File Service ActiveX control.	N/A	X	N/A	N/A
Keyword Panel Search: Cascading Data Sets	X	X	X	X
Keyword Panel Search: Combined AND / OR / TO Queries —“TO” used for numerics, dates, and currency	X	X	X	X
Keyword Panel Search: Drop-down Keyword Data Sets	X	X	X	X
Keyword Panel Search: Keyword Types—Alphanumeric, Alpha Single Table, Currency, Date, Date/Time, Floating Point, Numeric 9, Numeric 20, and Specific Currency.	X	X	X	X
Keyword Panel Search: Query Operators (<, <=, >, >=, ")	X	X	X	X
Keyword Panel Search: Repeat Keywords—using additional instances of Keywords Types by pressing F6	X	X	X	X
Keyword Panel Search: Required Keyword Settings	X	X	X	X
Retrieve: Date Range	X	X	X	X
Retrieve: Document Type	X	X	X	X
Retrieve: Document Type Group	X	X	X	X

Search & Retrieval X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Retrieve: Double-click to select all Document Types in the selected Document Type Group	X	X	X	N/A
Retrieve: Keywords—Support for standard Keyword Types, Keyword Type Groups, and Multi-Instance Keyword Type Groups.	X	X	X	X
Search: Button Disablement—Until search is complete.	N/A	X	X	N/A
Search: Configurable Date Search Default Format	X	X	X	X
Search: Custom Query Retrievals	X	X	X	X
Search: External Text Search	X	X	X	X
Search: External Text Search History	X	N/A	N/A	N/A
Search: External Text Search Options—Case Sensitive	X	X	X	X
Search: External Text Search Options—Column Search	X	N/A	N/A	X
Search: External Text Search Options—Create Report (advanced external text search reports)	X	X	X	N/A
Search: External Text Search Options—Distributed	X	N/A	N/A	N/A
Search: External Text Search Options—Find First	X	X	X	N/A
Search: External Text Search Options—Currency	X	N/A	N/A	N/A
Search: External Text Search Options—Formatted Number	X	X	X	X
Search: External Text Search Options—Number	X	X	X	X

Search & Retrieval X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Search: External Text Search Options—Text	X	X	X	X
Search: External Text Search Options—Whole Word Match	N/A	X	X	N/A
Search: External Text Search Options—Wild Card Search	X	X	X	X
Search: External Text Search User Results (history)	X	N/A	N/A	N/A
Search: External Text Search—Display a “No Documents Found” message when no documents are found.	X	X	X	X
Search: External Text Search—Of non-default OCR'd text renditions	X	X	X	N/A
Search: External Text Search—Open result in new window	X	X	X	N/A
Search: External Text Search—Searching of notes/annotations	X	X	X	X
Search: Full-Text Indexing Search Field	X	X	X	X
Search: Recent Query History—From current session	X	X	X	X
Search: Retrieve by Document Handle	X	X	X	X
Search: Server-side Full-Text Search	X	X	X	X
Search: Unrestricted Query Warning Settings	X	X	X	X

Document Select List

The following table lists features and options available when selecting documents in the Document Search Results list and other document select lists.

Document Select List X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Briefcase Add Document as Reference	X	X	N/A	N/A
Menu: Briefcase Check In Document	X	N/A	N/A	N/A
Menu: Briefcase Check-Out Comments	X	N/A	N/A	N/A
Menu: Briefcase Check Out Document	X	X	N/A	N/A
Menu: Briefcase Undo Checkout	X	N/A	N/A	N/A
Menu: Check Out—When EDM Briefcase is disabled	N/A	X	X	N/A
Menu: Clear Selected	X	N/A	N/A	N/A
Menu: Collaboration Add to Workspace	X	X	X	N/A
Menu: Collaboration Attach to Current Post	X	N/A	N/A	N/A
Menu: Collaboration Create New Discussion	X	X	X	X
Menu: Collaboration View All Posts	X	X	X	X
Menu: Compose Document	X	N/A	X	X
Menu: Compound Structure	X	N/A	N/A	N/A

Document Select List X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Create Keyword List	X	N/A	N/A	N/A
Menu: Create List Report	X	X	X	X
Menu: Data Mining	N/A	X	X	N/A
Menu: Data Mining Extract	X	N/A	N/A	N/A
Menu: Data Mining Mine Report	X	N/A	N/A	N/A
Menu: Data Mining Print	X	N/A	N/A	N/A
Menu: Data Mining View	X	N/A	N/A	N/A
Menu: Delete Document	X	X	X	X
Menu: Digital Signatures Sign Document (certificate-based signatures)	X	X	N/A	N/A
Menu: Digital Signatures Verify Document (certificate-based signatures)	X	X	N/A	N/A
Menu: Digital Signatures View Signatures (certificate-based signatures)	N/A	X	N/A	N/A
Menu: Display Disposition Status	N/A	X	X	N/A
Menu: Distribute Document	X	N/A	N/A	N/A
Menu: Document History	X	X	X	X

Document Select List X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Document History—Filter Items	X	X	N/A	X
Menu: Document History—Generate Report	X	N/A	N/A	N/A
Menu: Document Properties	X	X	X	X
Menu: Document Retention Exclude from Document Retention	X	X	X	N/A
Menu: Document Retention Remove Exclusion from Document Retention	X	X	X	N/A
Menu: Document Retention Re-Index	X	X	X	N/A
Menu: Document Retention Delete	X	X	X	N/A
Menu: Export All	X	N/A	N/A	N/A
Menu: Export to DIP File	X	N/A	N/A	N/A
Menu: Generate CSV File	X	X	X	X
Menu: Hosted Signing Package Status	X	N/A	N/A	X <i>DocuSign only</i>
Menu: Hosted Signing Upload for Signing	X	N/A	N/A	X <i>DocuSign only</i>
Menu: Keywords—view/edit/add— Supports read-only Keyword values that are locked by another user	X	X	X	X
Menu: Knowledge Transfer Add to Reading Group (Available in Unity as Send To Reading Group)	X	X	X	X

Document Select List X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Locate Document	X	N/A	N/A	N/A
Menu: Notes—Add/view/edit/delete—Opens Notes pane or dialog box	N/A	X	X	X
Menu: Open in New Window	N/A	X	X	X
Menu: Perform Automated Redaction	X	N/A	N/A	N/A
Menu: Perform Document Advanced Capture	X	N/A	N/A	N/A
Menu: Perform Document Full-Page OCR	X	N/A	N/A	X
Menu: Print—Opens Print pane or dialog box (see Print section for specific features)	X	X	N/A	X
Menu: Print Print All	X	N/A	N/A	N/A
Menu: Properties	X	X	X	X
Menu: Re-Index	X	X	X	X
Menu: Refresh	X	N/A	N/A	N/A
Menu: Render Statement	X	N/A	N/A	N/A
Menu: Revisions/Renditions	X	X	X	X
Menu: Ribbon	N/A	N/A	N/A	X
Menu: Run Script	X	N/A	N/A	N/A

Document Select List X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Send To Create DocPop Link [Available in Unity as Send To Mail Recipient (as Link)]	N/A	X	X	X
Menu: Send To Create New Document	X	X	X	X
Menu: Send To Create New ROI Request	X	N/A	N/A	N/A
Menu: Send To Document Editor (Available in Unity as Send To Document Separation)	X	N/A	N/A	X
Menu: Send To Envelope	X	X	X	X
Menu: Send To File—Advanced Options	N/A	X	X	N/A
Menu: Send To File—Save file to local drive	X	X	X	X
Menu: Send To Folder	N/A	X	X	N/A
Menu: Send To Internal User (Internal Mail)	X	X	X	X
Menu: Send To Mail Recipient (as Attachment) <hr/> Note: HTML Web Client support requires a configured web email service. <hr/>	X	X	X	X
Menu: Send To Mail Recipient (as Zip File) <hr/> Note: HTML Web Client support requires a configured web email service. <hr/>	X	X	X	N/A

Document Select List X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Send To Mail Recipient (with Advanced Options)	X	X	N/A	X
Menu: Send To Secure Package	X	N/A	N/A	N/A
Menu: Send To Zip File	X	N/A	N/A	N/A
Menu: Show Folder Locations	X	N/A	N/A	X
Menu: Task Pane	N/A	N/A	N/A	X
Menu: View Redacted Images	X	N/A	N/A	X
Menu: View Selected	X	N/A	N/A	N/A
Menu: View Thumbnails (Preview documents in the Thumbnail Hit List Viewer)	N/A	X	X	N/A
Menu: Workflow Approval Status	N/A	N/A	N/A	X
Menu: Workflow Execute Workflow	X	X	X	X
Menu: Workflow Open Workflow	N/A	X	X	X
Menu: Workflow System Tasks	X	X	X	X
Menu: Workflow Workflow Queues	X	X	X	X
Menu: WorkView Create Object	X	N/A	N/A	X
Menu: WorkView Execute Filter	X	N/A	N/A	X
Options: Results Per Page Settings	N/A	X	N/A	N/A

Document Select List X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Options: Show Previous/Next Results	N/A	N/A	N/A	N/A
Options: Toolbar Buttons—No Text/Show Text Labels	N/A	X	N/A	N/A
Printing: Send documents to server print queues	X	X	X	X
Select List: Grouping and sorting	N/A	X	X	X
Select List: Large Query Results Sets Handler	X	X	X	N/A
Select List: Respects Formatting Tags in Document Auto-Names	X	X	X	X
Select List: Select Multiple Documents—Shift-click and Ctrl-click	X	X	X	X

Viewer—Standard—Image Document

The following table lists features and options available from the document viewer. These features are usually available for image documents, and they may also be available for file types described later in this document. Some features don't apply to other file types.

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Automatically Adds the Web Server to Pop-Up Blocker Whitelists—For Internet Explorer and Google Toolbar pop-up blockers	N/A	X	N/A	N/A
Document Information Panel - Keywords, Notes, and Cross-References	N/A	N/A	N/A	X

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Briefcase Add Document as Reference	X	X	N/A	N/A
Menu: Briefcase Check-Out Comments	X	N/A	N/A	N/A
Menu: Briefcase Check Out Document	X	X	N/A	N/A
Menu: Briefcase Undo Checkout	X	N/A	N/A	N/A
Menu: Collaboration Add to Workspace	X	X	X	N/A
Menu: Collaboration Attach to Current Post	X	N/A	N/A	N/A
Menu: Collaboration Create New Discussion	X	X	X	X
Menu: Collaboration View All Posts	X	X	X	X
Menu: Cross-References	X	X	N/A	X
Menu: Delete Document	X	X	X	X
Menu: Delete/Re-Order Pages	X	N/A	N/A	N/A
Menu: Digital Signatures Sign Document (certificate-based signatures)	X	X	N/A	N/A
Menu: Digital Signatures Verify Document (certificate-based signatures)	X	X	N/A	N/A
Menu: Digital Signatures View Signatures (certificate-based signatures)	X	X	N/A	N/A

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Display Normal	X	X	N/A	N/A
Menu: Display Preserve Black	X	N/A	N/A	N/A
Menu: Display Scale to Gray	X	X	N/A	N/A
Menu: Display Disposition Status	N/A	X	X	N/A
Menu: Distribute Document	X	N/A	N/A	N/A
Menu: Document History	X	X	X	X
Menu: Document History—Filter Items	X	X	N/A	X
Menu: Document History—Generate Report	X	N/A	N/A	N/A
Menu: Document Properties	X	X	X	X
Menu: Electronic Signature Stamp Signature	X	N/A	N/A	N/A
Menu: Electronic Signature Verify Document	X	N/A	N/A	N/A
Menu: Image Zooming Reset Zoomed Area	X	N/A	N/A	N/A
Menu: Image Zooming Save Zoomed Area	X	N/A	N/A	N/A
Menu: Keywords—View/edit/add—Supports read-only Keyword values that are locked by another user	X	X	X	X
Menu: Knowledge Transfer Add To Reading Group	X	X	X	X
Menu: Navigate First Page	N/A	X	N/A	X

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Navigate Go To Page	X	X	X	X
Menu: Navigate Last Page	N/A	X	N/A	X
Menu: Navigate Next Page	N/A	X	N/A	X
Menu: Navigate Previous Page	N/A	X	N/A	X
Menu: Navigate Set Page Number	X	N/A	N/A	N/A
Menu: Next Document	X	X	X	X
Menu: Notes Add Note	X	X	X	X
Menu: Notes Delete Note	X	X	X	X
Menu: Notes View Notes	X	X	X	X
Menu: Open Markup Toolbar	X	N/A	N/A	N/A
Menu: Overlay	X	N/A	N/A	N/A
Menu: Perform Automated Redaction	X	N/A	N/A	N/A
Menu: Perform Document Advanced Capture	X	N/A	N/A	N/A
Menu: Perform Document Full-Page OCR	X	N/A	N/A	X
Menu: Previous Document	X	X	X	X
Menu: Print	X	X	X	X

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Process Custom	X	N/A	N/A	N/A
Menu: Process Flip Horizontally	X	X	N/A	X
Menu: Process Flip Vertically	X	X	N/A	X
Menu: Process Invert	X	X	X	N/A
Menu: Process Rotate 180	X	N/A	N/A	N/A
Menu: Process Rotate All Pages 180	N/A	N/A	X	N/A
Menu: Process Rotate Left	X	X	N/A	X
Menu: Process Rotate Right	X	X	N/A	X
Menu: Process Save Rotation	X	X	N/A	X
Menu: Re-Index	X	X	X	X
Menu: Re-Index Split (Document Separation)	X	N/A	N/A	X
Menu: Redaction Bitmap Capture from Signature Pad	X	X	X	X
Menu: Redaction Bitmap Create redacted image	X	X	N/A	X
Menu: Redaction Bitmap Delete all redaction bitmaps	X	N/A	N/A	N/A
Menu: Redaction Bitmap Delete redaction bitmap	X	N/A	N/A	N/A

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Redaction Bitmap Insert redaction bitmap	X	N/A	N/A	N/A
Menu: Redacted Image Create Redacted Image	X	N/A	N/A	X
Menu: Redacted Image View Redacted Images	X	N/A	N/A	X
Menu: Render Statement	X	N/A	N/A	N/A
Menu: Reset	X	N/A	N/A	N/A
Menu: Revisions/Renditions	X	X	X	X
Menu: Save Markups In Black and White	N/A	X	N/A	X
Menu: Save Markups In Color	N/A	X	N/A	X
Menu: Scale Actual Size	X	X	N/A	X
Menu: Scale Fit Height	N/A	X	N/A	N/A
Menu: Scale Fit in Window	X	X	N/A	X
Menu: Scale Fit Width	X	X	N/A	X
Menu: Scale True Size	X	N/A	N/A	N/A
Menu: Scale Zoom In	X	X	N/A	X
Menu: Scale Zoom Out	X	X	N/A	X
Menu: Scan More Pages	X	N/A	N/A	N/A

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Send To Clipboard	X	X	N/A	N/A
Menu: Send To Create DocPop Link [Available in Unity as Send To Mail Recipient (as Link)]	N/A	X	X	X
Menu: Send To Create DocPop Link to Page	N/A	X	X	N/A
Menu: Send To Create New Document	X	X	N/A	X
Menu: Send To Document Separation	N/A	N/A	N/A	X
Menu: Send To Envelope	X	X	X	X
Menu: Send To File—Advanced Options	X	X	X	N/A
Menu: Send To File—Save file to local drive as native format, PDF, Text, or TIFF	X	X	X	X
Menu: Send To Internal User (Internal Mail)	X	X	X	X
Menu: Send To Mail Recipient (as Attachment)—Supports client-side Outlook and GroupWise (MAPI 1.1 compliant) and respective address book integration. Note: HTML Web Client support requires a configured web email service.	X	X	X	X
Menu: Send To Mail Recipient (with Advanced Options)	X	X	N/A	N/A
Menu: Show Folder Locations	X	X	X	X

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Toolbars Annotations / Markups	X	X	N/A	X
Menu: Toolbars Notes List	N/A	X	N/A	X
Menu: Toolbars Pages (Page Thumbnails)	X	X	N/A	X
Menu: Toolbars Viewer Control	N/A	X	N/A	N/A
Menu: Workflow Approval Status	N/A	N/A	N/A	X
Menu: Workflow Execute Workflow	X	X	X	X
Menu: Workflow Open Workflow	N/A	X	X	X
Menu: Workflow Workflow Queues	X	X	X	X
Menu: Workflow System Tasks	X	X	X	X
Menu: WorkView Create Object	X	X	X	X
Menu: WorkView Execute Filter	X	X	X	X
Notes: User Group Rights Checking for Note Types	X	X	X	X
Printing: Send documents to server print queues	X	X	X	X
Status Bar—Displays check-out information	X	N/A	N/A	N/A
Status Bar—Displays disk group information	X	N/A	N/A	N/A
Status Bar—Displays note/annotation count	X	X	X	X

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Status Bar—Displays page count	X	X	X	X
Status Bar—Displays thread/discussion count	X	X	X	X
Thumbnails: Auto-Hide	N/A	X	N/A	X
Thumbnails: Copy pages across viewer windows	X	X	N/A	X
Thumbnails: Toolbars Annotations	X	X	N/A	N/A
Thumbnails: Toolbars Notes	N/A	X	N/A	N/A
Thumbnails: Toolbars Pages	N/A	X	N/A	N/A
Toolbar: Add Note	X	X	N/A	X
Toolbar: Append to Envelope	X	N/A	N/A	N/A
Toolbar: Auto-Hide	N/A	X	N/A	N/A
Toolbar: Briefcase	X	N/A	N/A	X
Toolbar: Cascade Windows	X	N/A	N/A	N/A
Toolbar: Change Font	X	N/A	N/A	N/A
Toolbar: Close All	X	N/A	N/A	N/A
Toolbar: Collaboration Workspaces	X	N/A	N/A	N/A
Toolbar: Copy Page to Clipboard	X	N/A	N/A	N/A

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Toolbar: Copy to Clipboard	X	N/A	N/A	N/A
Toolbar: Create From Existing Document	X	N/A	N/A	X
Toolbar: Create Highlight	X	X	X	X
Toolbar: Create New Envelope	X	N/A	N/A	X
Toolbar: Create New Form	X	N/A	N/A	X
Toolbar: Create New OLE Document	X	N/A	N/A	N/A
Toolbar: Create New ROI Request	X	N/A	N/A	N/A
Toolbar: Cross-References	X	N/A	N/A	X
Toolbar: Delete Selected Items	X	N/A	N/A	X
Toolbar: Display Scale to Gray	N/A	N/A	X	N/A
Toolbar: First Page	N/A	X	X	X
Toolbar: Flip Image Horizontal	X	N/A	N/A	X
Toolbar: Flip Vertical	X	N/A	N/A	X
Toolbar: Go to Line	X	N/A	N/A	N/A
Toolbar: Go to Page	X	X	N/A	X
Toolbar: Host Session	X	N/A	N/A	N/A

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Toolbar: Import Documents	X	N/A	N/A	X
Toolbar: Invert Image	X	N/A	N/A	N/A
Toolbar: Last Page	N/A	X	X	X
Toolbar: Mail Document (External)	X	N/A	N/A	X
Toolbar: Mail Document (Internal)	X	N/A	N/A	X
Toolbar: Mail Selected Text as Attachment	X	N/A	N/A	N/A
Toolbar: Next Document	X	X	X	X
Toolbar: Next Page	X	X	X	X
Toolbar: Open About Box	X	N/A	N/A	X
Toolbar: Open Custom Queries	X	N/A	N/A	X
Toolbar: Open Document Template	X	N/A	N/A	X
Toolbar: Open Envelope	X	N/A	N/A	X
Toolbar: Open File Cabinets	X	N/A	N/A	X
Toolbar: Open Help	X	X	X	X
Toolbar: Open Help Index	X	N/A	N/A	N/A
Toolbar: Open Help Search	X	N/A	N/A	N/A

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Toolbar: Open Print Queue	X	N/A	N/A	N/A
Toolbar: Open Trash Can	X	N/A	N/A	N/A
Toolbar: Open User Options	X	N/A	N/A	X
Toolbar: Open Workstation Options	X	N/A	N/A	N/A
Toolbar: Options—Enable Thumbnail Zoom	N/A	X	N/A	N/A
Toolbar: Options—Enable Thumbnail Zoom—Zoom Height	N/A	X	N/A	N/A
Toolbar: Options—Enable Thumbnail Zoom—Zoom Width	N/A	X	N/A	N/A
Toolbar: Options—Maximum Thumbnail Height	N/A	X	N/A	N/A
Toolbar: Options—Maximum Thumbnail Width	N/A	X	N/A	N/A
Toolbar: Options—Show Note Icons and Annotations When Open	X	X	N/A	X
Toolbar: Options—Always Show Note Icons and Annotations	N/A	X	N/A	X
Toolbar: Overlay	X	X	X	X
Toolbar: Previous Document	X	X	X	X
Toolbar: Previous Page	X	X	X	X
Toolbar: Print	X	X	X	X
Toolbar: Reading Group Viewer	X	N/A	N/A	X

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Toolbar: Refresh the Current Window	X	N/A	N/A	N/A
Toolbar: Re-Index	X	N/A	N/A	X
Toolbar: Retrieve Documents	X	N/A	N/A	X
Toolbar: Rotate Clockwise/Counterclockwise	X	X	X	X
Toolbar: Rotate Image 180 degrees	X	N/A	N/A	N/A
Toolbar: Run All Cross-References	X	N/A	N/A	X
Toolbar: Run VB1	X	N/A	N/A	N/A
Toolbar: Run VB2	X	N/A	N/A	N/A
Toolbar: Run VB3	X	N/A	N/A	N/A
Toolbar: Save Redactions	N/A	X	N/A	X
Toolbar: Save Rotation	X	N/A	N/A	X
Toolbar: Save to File	X	X	N/A	X
Toolbar: Scale to Gray	N/A	X	X	N/A
Toolbar: Scan/Index	X	N/A	N/A	X
Toolbar: Send Mail	X	N/A	N/A	X
Toolbar: Show Alternate Rendition—For documents that allow multiple renditions.	N/A	X	X	N/A

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Toolbar: Signature Pad	X	N/A	N/A	X
Toolbar: Sign Document	X	N/A	N/A	N/A
Toolbar: Tile Vertically	X	N/A	N/A	N/A
Toolbar: Tile Horizontally	X	N/A	N/A	N/A
Toolbar: Toggle Annotation	N/A	X	X	N/A
Toolbar: Toggle Redaction	N/A	X	N/A	N/A
Toolbar: Toggle Thumbnails	X	N/A	N/A	X
Toolbar: View Cross-References	X	N/A	N/A	X
Toolbar: View Document History	X	N/A	N/A	X
Toolbar: View Document Information	X	N/A	N/A	X
Toolbar: View Notes	X	X	N/A	X
Toolbar: View or Modify Keywords	X	N/A	N/A	X
Toolbar: Zoom In	X	X	X	X
Toolbar: Zoom Out	X	X	X	X
Toolbar: Zoom—Actual Size	X	X	X	X
Toolbar: Zoom—By Percentage—25%, 50%, 75%, 100%, 200%	N/A	X	N/A	X

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Toolbar: Zoom—Fit Height	N/A	X	X	N/A
Toolbar: Zoom—Fit in Window	X	X	X	X
Toolbar: Zoom—Fit Width	X	X	X	X
Toolbar: Zoom—True Size	X	X	N/A	N/A
Toolbar: Workflow	X	N/A	N/A	X
Toolbar: WorkView	X	N/A	N/A	N/A
Viewer: Actual Size	X	X	X	X
Viewer: Annotations—View/create/edit/delete	X	X	X	X
Viewer: Auto-Display Keywords	X	X	X	X
Viewer: Auto-Scroll (scrolling by resting the mouse pointer near the corner or edge of an image)	N/A	X	N/A	N/A
Viewer: Color Overlays	X	X	X	X
Viewer: Display Multi-Page Overlays	X	X	X	X
Viewer: Double-Click for Cross-References	X	X	X	X
Viewer: Highlights—Always on display status	N/A	X	N/A	N/A
Viewer: Highlights—Create/view/edit/delete	X	X	N/A	X
Viewer: Highlights—View as note tab	N/A	X	N/A	X

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Viewer: Multiple Page Thumbnails	X	X	X	X
Viewer: Notes—Auto-save on note text changes	X	X	X	X
Viewer: Notes—Color attribute in note's title bar	X	X	X	X
Viewer: Notes—Create/view/edit/delete	X	X	X	X
Viewer: Notes—"Hide Window" note attribute	X	X	X	N/A
Viewer: Notes—Right-click options (Delete Note, Privacy Options, Unobstruct)	X	X	N/A	X
Viewer: Notes—Show notes on all pages	X	X	X	X
Viewer: Notes—Support for auto-opening notes by type	X	X	X	X
Viewer: Notes—Support for changing a note's type after creation	X	X	X	N/A
Viewer: Notes—Title bar displays creation time	X	X	X	X
Viewer: Notes—Title bar displays creator's user name	X	X	X	X
Viewer: Overlay Cross-References	X	X	X	X
Viewer: Overlay Revisions	X	X	X	X
Viewer: Overlay—Use configuration settings on a per-Documents-Type basis	X	X	X	X
Viewer: Page Advancing Using Mouse Wheel	X	N/A	N/A	N/A
Viewer: Panning	X	X	X	X

Viewer—Standard—Image Document X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Viewer: Renditions—When renditionable	X	X	X	X
Viewer: Revisions—When revisable	X	X	X	X
Viewer: Rubber Band Zoom	X	X	N/A	X
Viewer: Select Area (CTRL-left-click-drag) Send To Clipboard	X	X	N/A	N/A
Viewer: Select Area (CTRL-left-click-drag) Send To Printer	X	X	N/A	N/A
Viewer: Text Locking	X	X	N/A	N/A
Viewer: Zoom Using Ctrl + Mouse Wheel	N/A	X	N/A	X

Viewer—Text Document Specific

The following table lists features and options specific to documents with a text report format.

Viewer—Text Document Specific X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Data Mining	N/A	X	X	N/A
Menu: Data Mining Extract	X	N/A	N/A	N/A
Menu: Data Mining Mine Report	X	N/A	N/A	N/A

Viewer—Text Document Specific X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Data Mining Print	X	N/A	N/A	N/A
Menu: Data Mining View	X	N/A	N/A	N/A
Toolbar: Internal Text Search—Enter alphanumeric search string	X	X	X	X
Toolbar: Internal Text Search—Find First	X	N/A	N/A	N/A
Toolbar: Internal Text Search—Find Next	X	X	X	X
Toolbar: Internal Text Search—Find Previous	X	X	X	X
Toolbar: Internal Text Search Options—Case Sensitive	X	X	N/A	X
Toolbar: Internal Text Search Options—Column Index (select option)	X	X	N/A	X
Toolbar: Internal Text Search Options—Column Search	X	X	X	X
Toolbar: Internal Text Search Options—Currency	X	N/A	N/A	N/A
Toolbar: Internal Text Search Options—End Column	X	X	X	X
Toolbar: Internal Text Search Options—Formatted Number	X	X	N/A	X
Toolbar: Internal Text Search Options—Generate Report	X	X	X	N/A
Toolbar: Internal Text Search Options—Number	X	X	N/A	X
Toolbar: Internal Text Search Options—Start Column	X	X	X	X
Toolbar: Internal Text Search Options—Start Search on Current Page	N/A	X	N/A	X

Viewer—Text Document Specific X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Toolbar: Internal Text Search Options—Text	X	X	N/A	X
Toolbar: Internal Text Search Options—Whole Word Match	N/A	X	N/A	X
Toolbar: Internal Text Search Options—Wild Card Search	X	X	N/A	X
Viewer: Auto-Display Keywords	X	X	N/A	X
Viewer: Creation of Page References upon Viewing	X	X	X	X
Viewer: Cross-References by Clicked Text Search	X	X	X	N/A
Viewer: Page References by Common Keyword Value	X	X	X	X
Viewer: Page References	X	X	X	X
Viewer: Toggle Image Overlays—Landscape	X	X	X	N/A
Viewer: Toggle Image Overlays—Portrait	X	X	X	N/A

Viewer—PCL Document Specific

The following table lists features and options specific to documents with PCL formats.

Viewer—PCL Document Specific X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Toolbar: Text Search	X	X	N/A	X
Viewer: Double-Click Cross-References (PCL to...)	X	X	X	X
Viewer: Overlay Support	X	X	X	X
Viewer: Positionable Note Bitmaps	X	X	X	X
Viewer: Viewing Documents	X	X	X	X

Viewer—AFP/RSS Document Specific

The following table lists features and options specific to documents with AFP and RSS formats.

Viewer—AFP/RSS Document Specific X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Toolbar: Text Search	X	X	N/A	X
Viewer: Double-Click Cross-References (AFP/RSS to...)	X	X	X	X
Viewer: Overlay Support	X	X	X	X

Viewer—AFP/RSS Document Specific X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Viewer: Positionable Note Bitmaps	X	X	X	X
Viewer: Support for Compatible DJDE File Viewing—Requires DJDE file compatibility testing by Hyland	X	X	X	N/A
Viewer: Viewing Documents	X	X	X	X

Viewer—OLE Document Specific

The following table lists features and options specific to OLE documents.

Viewer—OLE Document Specific X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Document Cross-References	X	X	X	X
Menu: Document History	N/A	X	X	X
Menu: Document Print	X	X	N/A	X
Menu: Document Properties	X	X	X	X
Menu: Document Revisions / Renditions	X	X	X	X
Menu: Document View in Native Application (Requires the Integrated Office Viewer)	X	X	X	X

Viewer—OLE Document Specific X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Menu: Edit Keywords	X	X	X	X
Menu: Edit Notes	X	X	X	X
Menu: Edit Re-Index	X	X	X	X
Menu: Next Document	X	X	X	X
Menu: Previous Document	X	X	X	X
Menu: Process Workflow Execute Workflow	X	X	X	X
Menu: Process Workflow Open Workflow	N/A	X	X	X
Menu: Process Workflow Workflow Queues	X	X	X	X
Menu: Process WorkView Create Object	X	X	X	X
Menu: Process WorkView Execute Filter	X	X	X	X
Toolbar: Status Bar—Displays note count	X	X	X	X
Toolbar: Status Bar—Displays revision count	X	X	X	X
Viewer: Auto-Display Keywords	X	N/A	N/A	X
Viewer: Viewing Documents	X	X	X	X

Viewer—HTML/E-Form/Unity Form Document Specific

The following table lists features and options specific to HTML documents, E-Forms, and Unity Forms.

Viewer—HTML/E-Form Document Specific X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
E-Forms: Create New Form	X	X	X	X
E-Forms: Create Unity Form	N/A	X	X	X
E-Forms: Create Virtual E-Form	X	X	X	X
E-Forms: Filter Field Available for Finding Forms	N/A	X	X	X
E-Forms: List of Available E-Forms in Alphabetical Order	X	X	X	X
Viewer: Auto-Display Keywords	N/A	N/A	N/A	X
Viewer: Edit and Resubmit E-Forms	X	X	X	X
Viewer: E-Forms—Execute cross-references	X	X	X	X
Viewer: E-Forms—Execute cross-references using xrefitemnum button	X	X	X	N/A
Viewer: E-Forms—Execute Custom Query links	X	X	X	N/A
Viewer: E-Forms—Execute OBBtn_SaveNoClose	X	X	X	X
Viewer: E-Forms—Trigger AutoFill Keyword Sets—Using ExpandKS button	X	X	X	X
Viewer: E-Forms—Update all input types—text box, radio button, scrolling text box, drop-down, check box, push buttons	X	X	X	X

Viewer—HTML/E-Form Document Specific X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Viewer: E-Forms—View date properties—obdocumentdate, obfromdate, obtodate, obproperty_documentdate, obproperty_datestored, obproperty_timestored	X	X	X	X
Viewer: E-Forms—View user and document properties—obproperty_username, obproperty_itemnum, obproperty_currentuserID, obproperty_currentusername, obproperty_currentuserrealname, obproperty_currentuserdisplayname	X	X	X	X
Viewer: Positionable Notes and Icons	X	X	X	N/A
Viewer: View E-Forms	X	X	X	X
Viewer: View Unity Forms	N/A	X	X	X

Viewer—Import/Scan/Index

The following table lists features and options available for creating E-Forms and for importing, scanning, and indexing documents.

Note: For a more detailed list of features and functions related to scanning, see the Scanning Feature Matrix, found in any of the following module reference guides: **Document Imaging**, **Disconnected Scanning**, **Express Scanning**, and **Front Office Scanning**.

Viewer—Import/Scan/Index/ X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Import/Re-Index: Set Document Date	X	X	X	X
Import/Scan/Re-Index: Clear Keyword Values Note: Scan is not supported in HTML Web Client	X	X	X	X
Import/Scan/Re-Index: Select Document Type Note: Scan is not supported in HTML Web Client	X	X	X	X
Import/Scan: Clear All	X	X	X	X
Import: New Document	X	X	X	X
Import: Open in Viewer	N/A	N/A	N/A	X
Import: Preview	N/A	N/A	N/A	X
Import: Security	X	X	X	X
Index: Append Pages to Existing Documents while Indexing	X	X	X	X

Viewer—Import/Scan/Index/ X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Index: Create New Document	X	X	X	X
Index: Delete Document	X	X	X	X
Index: Delete Page	X	X	X	X
Index: Image Segment Archiver	X	N/A	N/A	N/A
Index: Navigation—First Document	X	X	X	X
Index: Navigation—Last Document	X	X	X	X
Index: Navigation—Next Document	X	X	X	X
Index: Navigation—Previous Document	X	X	X	X
Index: Navigation—Skip Document	X	N/A	N/A	X
Index: Stop Indexing	X	X	X	X
Index: Support for Double-Blind Indexing	X	X	X	X
Index: Undo Indexing Action	N/A	X	X	X
Keyword Panel Index: Keyword Locking	X	X	X	X
Keyword Panel: Repeat Keywords—Using additional instances of Keyword Types by pressing F6	X	X	X	X
Keyword Panel: Retain Keyword Values after import	X	X	X	X
Keyword Panel: Support for AutoFill Keyword Sets	X	X	X	X

Viewer—Import/Scan/Index/ X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Keyword Panel: Support for Cascading Data Sets	X	X	X	X
Keyword Panel: Support for Drop-down Keyword Data Sets	X	X	X	X
Keyword Panel: Support for Indexing All Keyword Type Groups and Multi-instance Keyword Type Groups	X	X	X	X
Keyword Panel: Support for Indexing All Keyword Types—Alphanumeric, alpha single table, currency, date, date/time, floating point, numeric (9), numeric (20), and specific currency	X	X	X	X
Keyword Panel: Support for Invisible Keywords	X	X	X	X
Keyword Panel: Support for Keyword Type Validation	X	X	X	X
Keyword Panel: Support for Required Keywords—based on Document Types	X	X	X	X
Keyword Panel: Support for Reverse AutoFill Keyword Sets	X	X	X	X
Re-Index: Re-Index Document to Another Document Type	X	X	X	X

Print Options

The following table lists OnBase printing features and options and where they are supported. The HTML Web Client (in standard mode) lets users print OnBase documents, but it does not support OnBase print options outside of page range options.

Print Options X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Color: Black & White	X	X	N/A	N/A
Color: Color	X	X	N/A	N/A
Default Settings: Automatically Print Using Default Settings	X	X	N/A	N/A
Default Settings: Set as Default	X	X	N/A	N/A
Digital Signatures: Print Digital Signature Information	X	N/A	N/A	N/A
Image Scaling: Best Fit	X	X	N/A	X
Image Scaling: One-to-One	X	X	N/A	X
Job Settings: Number of Copies	X	X	N/A	X
Job Settings: Single Print Job	X	X	N/A	X
Job Settings: Continuous Flow	X	X	N/A	N/A
Notes Printing: Annotation and/or Note Icon On Document	X	X	N/A	X
Notes Printing: Note Text On Document	X	X	N/A	X
Notes Printing: Note Text After Document	X	X	N/A	X

Print Options X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Orientation: Portrait	X	X	N/A	X
Orientation: Landscape	X	X	N/A	X
Orientation: Auto Orientation	X	X	N/A	N/A
Performance: Force Optimized PostScript Image Printing	X	N/A	N/A	N/A
Print Formats—including N-Up formats (images per page) with support for printing titles (above and below) and printing borders	X	X	N/A	X
Print Overlay: No Overlay	X	X	N/A	X
Print Overlay: Print Overlay	X	X	N/A	X
Print Overlay: Fax Compatible Overlay	X	X	N/A	X
Print Queues	X	X	N/A	X
Print Range: All	X	X	X	X
Print Range: Current Page	X	X	X	X
Print Range: Selected	X	N/A	N/A	N/A
Print Range: Pages	X	X	X	X
Revision Printing: Current Revision	X	X	N/A	X
Revision Printing: All Revisions	X	X	N/A	X
Revision Printing: Current Version	X	X	N/A	X

Print Options X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Revision Printing: All Versions	X	X	N/A	X

Content Management

The following table lists features and options for managing, organizing, and sending documents.

Content Management X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Document Templates: Create Documents from Templates	X	X	N/A	X
Documents Checked Out: Briefcase	X	X	N/A	X
Documents Checked Out: Briefcase Edit	X	X	N/A	X
Documents Checked Out: Check in selected document(s)	X	X	X	X
Documents Checked Out: Check out selected document(s)	X	N/A	N/A	N/A
Documents Checked Out: Get all revisions for selected document(s)	X	N/A	N/A	N/A
Documents Checked Out: Remove selected revision(s)	X	N/A	N/A	N/A
Documents Checked Out: Synchronize all documents	X	N/A	N/A	N/A
Documents Checked Out: Synchronize selected reference document(s)	X	N/A	N/A	N/A

Content Management X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Documents Checked Out: Undo checkout on selected document(s)	X	X	X	X
Envelopes: Create	X	X	X	X
Envelopes: Delete	X	X	X	X
Envelopes: Share Envelopes	X	X	X	N/A
Folders: Documents Menu—Briefcase Add Document as Reference	X	X	X	N/A
Folders: Documents Menu—Briefcase Check-Out Comments	X	N/A	N/A	N/A
Folders: Documents Menu—Briefcase Check In Document	X	N/A	N/A	N/A
Folders: Documents Menu—Briefcase Check Out Document	X	N/A	N/A	N/A
Folders: Documents Menu—Briefcase Undo Check Out	X	N/A	N/A	N/A
Folders: Documents Menu—Clear Selected	X	X	X	N/A
Folders: Documents Menu—Collaboration Add to Workspace	X	N/A	N/A	N/A
Folders: Documents Menu—Collaboration Attach to Current Post	X	N/A	N/A	N/A
Folders: Documents Menu—Collaboration Create New Discussion	X	N/A	N/A	N/A
Folders: Documents Menu—Collaboration View All Posts	X	N/A	N/A	N/A
Folders: Documents Menu—Compound Structure	X	N/A	N/A	N/A
Folders: Documents Menu—Copy To Folder	N/A	X	X	N/A

Content Management X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Folders: Documents Menu—Compose Document	N/A	N/A	X	N/A
Folders: Documents Menu—Create Keyword List	X	N/A	N/A	X
Folders: Documents Menu—Delete	X	X	X	X
Folders: Documents Menu—Digital Signatures Sign Document	X	N/A	N/A	N/A
Folders: Documents Menu—Digital Signatures Verify Document	X	N/A	N/A	N/A
Folders: Documents Menu—Distribute Document	X	N/A	N/A	N/A
Folders: Documents Menu—Document Retention Delete	X	N/A	N/A	N/A
Folders: Documents Menu—Document Retention Exclude from Document Retention	X	N/A	N/A	N/A
Folders: Documents Menu—Document Retention Re-Index	X	N/A	N/A	N/A
Folders: Documents Menu—Document Retention Remove Exclusion from Document Retention	X	N/A	N/A	N/A
Folders: Documents Menu—Filter Documents	X	X	X	X
Folders: Documents Menu—History	X	N/A	N/A	X
Folders: Documents Menu—Keywords	X	X	X	X
Folders: Documents Menu—Knowledge Transfer Add to Reading Group	X	N/A	N/A	X
Folders: Documents Menu—Locate Document	X	N/A	N/A	N/A

Content Management X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Folders: Documents Menu—Move To Folder	N/A	X	X	N/A
Folders: Documents Menu—Open in New Window	X	X	X	N/A
Folders: Documents Menu—Perform Document Advanced Capture	X	N/A	N/A	N/A
Folders: Documents Menu—Perform Document Full-Page OCR	N/A	N/A	N/A	X
Folders: Documents Menu—Print Selected	X	N/A	N/A	X
Folders: Documents Menu—Properties	X	N/A	N/A	X
Folders: Documents Menu—Re-Index	X	N/A	N/A	X
Folders: Documents Menu—Reconcile Crippled Statement	X	N/A	N/A	N/A
Folders: Documents Menu—Refresh	X	X	X	N/A
Folders: Documents Menu—Remove from Folder	X	X	X	X
Folders: Documents Menu—Render Statement	X	N/A	N/A	N/A
Folders: Documents Menu—Revisions/Renditions	X	X	X	X
Folders: Documents Menu—Run Script	X	N/A	N/A	N/A
Folders: Documents Menu—Send To Create New Document	X	N/A	N/A	X
Folders: Documents Menu—Send To Create New ROI Request	X	N/A	N/A	N/A
Folders: Documents Menu—Send To Document Editor (Document Separation)	X	N/A	N/A	X

Content Management X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Folders: Documents Menu—Send To Envelope	X	X	X	X
Folders: Documents Menu—Send To File	X	X	X	X
Folders: Documents Menu—Send To Mail Internal User	X	X	X	X
Folders: Documents Menu—Send To Mail Mail Recipient (as Attachment)	X	N/A	N/A	X
Folders: Documents Menu—Send To Mail Mail Recipient (with Advanced Options)	X	N/A	N/A	X
Folders: Documents Menu—Template	X	X	X	X
Folders: Documents Menu—View Redacted Images	X	N/A	N/A	X
Folders: Documents Menu—Workflow Execute Workflow	X	X	X	X
Folders: Documents Menu—Workflow Workflow Queues	X	X	X	X
Folders: Documents Menu—WorkView Create Object	X	N/A	N/A	X
Folders: Documents Menu—WorkView Execute Filter	X	N/A	N/A	X
Folders: Folder Notes—Create/view/edit/delete	X	X	X	X
Folders: Menu—Cancel Rimage Export	X	N/A	N/A	N/A
Folders: Menu—Clear Selected	X	X	X	N/A
Folders: Menu—Delete	X	X	X	X
Folders: Menu—Display Disposition Status	X	X	X	X

Content Management X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Folders: Menu—Export Folder	X	N/A	N/A	N/A
Folders: Menu—Export Folder to Rimage	X	N/A	N/A	N/A
Folders: Menu—Find Folder	X	X	X	X
Folders: Menu—Folder Contents options	X	N/A	N/A	X
Folders: Menu—History	X	X	X	X
Folders: Menu—Keywords	X	X	X	X
Folders: Menu—New Folder	X	X	X	X
Folders: Menu—Open in New Window	N/A	X	X	N/A
Folders: Menu—Place Hold	X	X	X	X
Folders: Menu—Post Event	X	X	X	X
Folders: Menu—Print	X	X	X	N/A
Folders: Menu—Properties	X	N/A	N/A	X
Folders: Menu—Refresh	X	X	X	X
Folders: Menu—Remove From List	X	N/A	N/A	N/A
Folders: Menu—Send To Create FolderPop Link	N/A	X	X	N/A
Folders: Menu—View Holds	X	X	X	X

Content Management X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Folders: Menu—View Selected	X	X	X	N/A
Folders: Retrieve	X	X	X	X
Folders: View Child	X	X	X	X
Folders: View File Cabinet	X	X	X	X
Integrated Audio	N/A	X	X	X
Integrated Video	N/A	X	X	X
Mailbox: Delete Mail	X	X	X	X
Mailbox: Delete Selected	X	X	X	X
Mailbox: Forward	X	X	X	X
Mailbox: Navigation—First Message	N/A	X	X	N/A
Mailbox: Navigation—Last Message	N/A	X	X	N/A
Mailbox: Navigation—Previous Message	N/A	X	X	N/A
Mailbox: Read Receipt Requested	X	X	X	X
Mailbox: Refresh	X	X	X	X
Mailbox: Reply Without Attachments	X	X	X	X
Mailbox: Reply With Attachments	X	N/A	N/A	X

Content Management X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Mailbox: Select User Groups/Users from Address Book	X	X	X	X
Mailbox: Send Mail	X	X	X	X
Mailbox: View Inbox	X	X	X	X
Mailbox: View Selected	X	X	X	X

User Options

The following table lists user-specific options and where they are available.

User Options X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Change Password	X	X	X	X
Change User Calendar	X	N/A	N/A	N/A
Document: Display Options—Disable Vertical Scroll Bar	X	N/A	N/A	N/A
Document: Display Options—Hide Notes	X	N/A	N/A	N/A
Document: Display Options—Hide Page Markers	X	N/A	N/A	N/A
Document: Display Options—Show Text Guideline	X	N/A	N/A	N/A

User Options X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Document: Display Options—Use Same Guideline	X	N/A	N/A	N/A
Document: Document Search—Display all documents if number of results is less than or equal to #	X	N/A	N/A	N/A
Document: Document Search—Launch Item View on Document Search	X	N/A	N/A	N/A
Document: EDM Briefcase Options—Archive New Documents	X	X	N/A	N/A
Document: EDM Briefcase Options—Check In Documents	X	X	N/A	N/A
Document: EDM Briefcase Options—Synchronize Documents	X	X	N/A	N/A
Document: Full-Text Search—Show Alternate Document View	X	N/A	N/A	N/A
Document: Image Thumbnail—Rotate Auto-Save	X	X	N/A	X
Document: Image Thumbnail—Show Thumbnails Horizontal	X	N/A	N/A	N/A
Document: Image Thumbnail—Show Thumbnails Vertical	X	N/A	N/A	N/A
Document: Image Thumbnail—Show Thumbnails, adjust height and width	X	N/A	N/A	N/A
Document: Selected Text Options—Add End Of Line	X	N/A	N/A	N/A
Document: Selected Text Options—Change Space to Tab	X	N/A	N/A	N/A
Document: Selected Text Options—Preserve From Feeds	X	N/A	N/A	N/A
Document: Text Display—Normal	X	N/A	N/A	N/A
Document: Text Display—Green Bar	X	N/A	N/A	N/A

User Options X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Document: Text Display—Overlay	X	N/A	N/A	N/A
Document: Text Search—Local	X	N/A	N/A	N/A
Document: Text Search—Distributed	X	N/A	N/A	N/A
Document: Text Search—Text Search Toolbar	X	N/A	N/A	N/A
Document: Text Select Mode—Line	X	N/A	N/A	N/A
Document: Text Select Mode—Column	X	N/A	N/A	N/A
Document: Text Select Mode—Block	X	N/A	N/A	N/A
Document Storage Default Date: Last weekday, last business day, yesterday, today, first of the month, last of the month, specific day	X	N/A	N/A	N/A
General: Default Print Format	X	N/A	N/A	N/A
General: Document List Refresh—Disable document list refresh	X	N/A	N/A	N/A
General: Document List Refresh—Document List Refresh Rate # Seconds	X	N/A	N/A	N/A
General: Exit—Verify Exit	X	N/A	N/A	X
General: General—Classic File Cabinets Window	X	N/A	N/A	N/A
General: General—Classic Retrieval Window	X	N/A	N/A	N/A
General: General—Disable List Bitmaps	X	N/A	N/A	N/A
General: General—Display Toolbar	X	N/A	N/A	N/A

User Options X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
General: General—Keyword Operators	X	N/A	N/A	N/A
General: General—Keyword Select List	X	N/A	N/A	N/A
General: General—Large Toolbar	X	N/A	N/A	N/A
General: General—Notify on New Mail	X	N/A	N/A	X
General: General—Status Bar	X	N/A	N/A	N/A
General: Terminal Emulation—Bypass Configuration	X	N/A	N/A	N/A
General: Terminal Emulation—Verify Window Exit	X	N/A	N/A	N/A
Menu: Favorites	N/A	X	X	X
Menu: Home Page	N/A	X	X	X
Retrieval Default Date: Last weekday, last business day, yesterday, today, first of the month, last of the month, specific day, last month, current month, current week, month-to-date, year-to-date, last # days/weeks/months	X	X	X	X
Startup: Launch on Startup—Mail, Trash Can, Local Print Queue, Custom Query List, Retrieval Dialog, Open File Cabinets, Workflow, Reading Group Viewer	X	N/A	N/A	N/A
Workflow Combined View: Show Combined View at Startup	X	N/A	N/A	N/A
Workstation Options	X	N/A	N/A	N/A

Administration

The following table lists administrative features and options and where they are available.

Administration X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
AutoFill Keyword Sets: Importer	X	N/A	N/A	N/A
AutoFill Keyword Sets: Manager	X	N/A	N/A	N/A
Configure Document Composition: Form Letters	X	N/A	N/A	N/A
Distribution Recipients: Edit recipient information	X	X	X	N/A
Distribution Recipients: View recipients	X	X	X	N/A
Document Distribution: Customer Importer	X	N/A	N/A	N/A
Document Distribution: Customer Information	X	N/A	N/A	N/A
Document Distribution: Delivery Template	X	N/A	N/A	N/A
Document Distribution: Distribution Queue	X	N/A	N/A	N/A
Document Distribution: Distribution Sites	X	N/A	N/A	N/A
Document Distribution: Server Configuration	X	N/A	N/A	N/A
Document Retention: Excluded Items	X	N/A	N/A	N/A
Document Retention: Process	X	N/A	N/A	N/A
Export Manager: Auto-Publishing Queue	X	N/A	N/A	N/A

Administration X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Export Manager: Auto-Publishing Scheduler	X	N/A	N/A	N/A
Export Manager: Auto-Publishing Sites	X	N/A	N/A	N/A
Export Manager: Export Documents	X	N/A	N/A	N/A
Export Manager: View Envelope Exports	X	N/A	N/A	N/A
Export Manager: View Folder Exports	X	N/A	N/A	N/A
Extractor for Data Warehouse	X	N/A	N/A	N/A
Import Manager	X	N/A	N/A	N/A
IMS Lockbox Processing Report	X	N/A	N/A	N/A
Knowledge Transfer: Add Document	X	N/A	N/A	X
Knowledge Transfer: Administrative Assistant	X	N/A	N/A	X
Knowledge Transfer: Document Administration	X	N/A	N/A	X
Knowledge Transfer: Reading Group Administration	X	N/A	N/A	X
Knowledge Transfer: User Administration	X	N/A	N/A	X
License Usage Report	X	N/A	N/A	N/A
Lockbox Batch Print Monitor	X	N/A	N/A	N/A
Platter Management	X	N/A	N/A	N/A

Administration X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Print Distribution: Print	X	N/A	N/A	N/A
Print Distribution: Schedule	X	N/A	N/A	N/A
Records Management: Administration	X	N/A	N/A	X
Records Management: Create Report	X	N/A	N/A	N/A
Release of Information Reports: Generate Report(s)	X	N/A	N/A	N/A
Scanning Reports: Generate Report(s)	X	N/A	N/A	N/A
Scanning Reports: Purge Scanning Log	X	N/A	N/A	N/A
Signature Administration: Ceremony Server Signature Locations	X	N/A	N/A	N/A
Signature Administration: Configure Signature Locations	X	N/A	N/A	X
Signature Administration: DocuSign Signature Locations	X	N/A	N/A	N/A
Signature Administration: Hosted Signature Polling	X	N/A	N/A	N/A
Timing Test	X	N/A	N/A	N/A
Transaction Logs: Create Report	X	N/A	N/A	N/A
Transaction Logs: Purge Messages	X	N/A	N/A	N/A
Transaction Logs: View All Messages	X	N/A	N/A	N/A
Users: Configure—Named Web User	N/A	X	X	N/A

Administration X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Users: Configure—User name, real name, email address, password Note: The Unity Client only supports editing of the real name and email address of a user.	N/A	X	X	X
Users: Create User	N/A	X	X	X
Users: Delete	N/A	X	X	X
Users: Disconnect	N/A	X	X	N/A
Users: Lock	N/A	X	X	X
Users: Refresh	N/A	X	X	X
Users: Search/Filter	N/A	X	X	X
Users: Security Keywords—Add, edit, remove	N/A	X	X	X
Users: Show Active Users	X	X	X	N/A
Users: Show All Users	N/A	X	X	X
Users: Show Users Consuming Licenses	X	X	X	N/A
Users: Unlock	X	X	X	X
Users: User Groups—Assign, unassign	N/A	X	X	X
Users: Workstation Registration	X	N/A	N/A	N/A

Administration X = Feature is Available/Supported N/A = Feature is Not Available	OnBase Client	ActiveX Web Client	HTML Web Client	Unity Client
Utilities: Batch Lock Administration	X	N/A	N/A	N/A
Utilities: Commit Icons and Bitmaps	X	N/A	N/A	N/A
Utilities: Document Lock Administration	X	X	X	X
Utilities: Document Maintenance	X	N/A	N/A	N/A
Utilities: Edit INI File	X	N/A	N/A	N/A
Utilities: Folder Maintenance	X	N/A	N/A	N/A
Utilities: Launch Configuration Module	X	N/A	N/A	N/A
Utilities: Load Icons and Bitmaps	X	N/A	N/A	N/A
Utilities: System Statistics	X	N/A	N/A	N/A
Utilities: Windows Services	X	N/A	N/A	N/A
Web Diagnostics: General Diagnostics	N/A	X	X	N/A
Web Diagnostics: Logging Profiles	N/A	X	X	N/A
Workflow Log: Purge All Entries	X	N/A	N/A	N/A
Workflow Log: Restricted Purge	X	N/A	N/A	N/A