WebView Installation and Administration Guide

Cisco ICM/IPCC Enterprise & Hosted, Release 7.0(0)
June 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel:  408 526-4000
     800 553-NETS (6387)
Fax:  408 527-0883
CONTENTS

Preface ix
  Objective ix
  Audience ix
  Organization x
  Conventions xi
  Related Publications xii

Installation

CHAPTER 1
Understanding WebView 1-1
  About WebView 1-2
  WebView Components 1-2
    The Distributor Admin Workstation 1-4
    Databases on the Admin Workstation 1-4
    The WebView Server 1-5
    Internet Information Services (IIS) 1-6
    Third-Party Software 1-6
    WebView Software 1-7
    The WebView Client 1-7
    The Web Browser 1-7
  Sequence of Installing WebView Components 1-9
  The WebView Information Flow 1-10
  WebView Deployments for ICM/IPCC Enterprise 1-12
    Standard Deployment 1-12
    Large-Customer Deployment 1-12
    Migrating from a Standard to a Large-Customer Deployment 1-13
    Primary/Secondary AW Deployment 1-15
    Hosted Deployment 1-16
  Multi-language Installations 1-16
    Character Set and Databases 1-17
    Language Selection at Setup 1-18
    Localizing the Browser Language Setting 1-19
Contents

CHAPTER 5
The WebView Database  5-1
  About the WebView Database  5-2
  Location of the WebView Database  5-3
  WebView Database Deployment Models  5-4
    WebView Database in a Standard Deployment  5-4
    WebView Database in a Large-Customer Deployment  5-5
  Working with a Second (Failover) WebView Database  5-6
    Creating a Second (or Failover) WebView Database  5-7
    Redirecting the WebView Server to Another WebView Database  5-7
  WebView Database Tables  5-8
    The WebViewVersion Table  5-8
    The Print Jobs Table  5-9
    The Report Table  5-11
    The User Preferences Table  5-12

CHAPTER 6
Jaguar Administration and the Jaguar Watchdog  6-1
  Jaguar Administration  6-1
    Changing the Jaguar Admin Password  6-1
    Setting the Size of the Jaguar Log File  6-3
    Deleting Jaguar Log Files  6-3
    Troubleshooting Jaguar  6-4
  The Jaguar Watchdog  6-5
    Jaguar Watchdog Properties  6-5
    Executing a Batch File after Jaguar Restarts  6-6
    About Jaguar Watchdog Logging  6-7

CHAPTER 7
Time and Date in Reports  7-1
  Date and Time Formats in WebView Reports  7-1
  Time Zone Values for Report Viewing  7-1
    Central Controller Time Zone and Reporting Data  7-2
    Checking WebView AW Time Synchronization  7-2
  Time Zone Field  7-2
  Time and Time Zones Dependencies  7-3
  How Date Formats are Set  7-3
Dates and Date Ranges in Mixed-Language Installations  7-5
List of International Date Formats  7-6

CHAPTER 8
Template Maintenance  8-1
About Templates  8-1
How Templates are Organized  8-2
Cisco Templates and Custom Templates  8-2
Caching Templates and Items  8-3
Refreshing the Cache  8-3
Configuring Caching  8-3
How to Run PATCHPBL to Update or Fix Templates  8-6

CHAPTER 9
WebView Registry Settings and Property Files  9-1
Registry Settings  9-1
AllowAdminLogin  9-1
Event  9-2
Property Files  9-3
adminui.properties  9-3
jagconnection.properties  9-8
WebView.properties  9-9
wvLocale.properties  9-9

CHAPTER 10
WebView Security: Active Directory and Secure Socket Layer  10-1
About Active Directory  10-2
Domain Rights for the WebView Administrator  10-2
User Membership in the WebView Domain Local Security Group  10-2
WebView User Authentication Model  10-2
UserNames  10-3
About SSL  10-4
SSL Configuration at ICM Setup  10-4
Changes at User Log In  10-4
The SSL Encryption Utility  10-6

CHAPTER 11
Troubleshooting Tips  11-1
Logs  11-4
Third-Party Software  11-5
Browser Setting for Trusted Sites  11-5
Checking New Atlanta ServletExec  11-5
Debugging: Turning it On and Off for Third-Party Tools
EAServer/Jaguar Installation Fails
Error 2221: Determine Current User Security Type
Error After Changing the Jaguar Admin Password
Error: IIS Admin Service Configuration
Error: The Windows Scripting Host Must be Installed
Jaguar Server Connection Fails After Restart
Jaguar Service Verification
Removing Old Versions of EAServer/Jaguar
Third-Party Software Licenses
World Wide Publishing Service: Stopping it and Restarting WebView

Installation and Login
Java Code Displays After Login
Users Unable to Log in to WebView
  Are They Entering the Correct UserName?  
  Are They a Member of the WebView Group?  
  Are They Seeing HTTP Error 403.4?  
  Are They Using a Blank Password?  
  Has the IP Address Changed?  
  Has the Password Expired or the User Account Been Disabled?  
  Is Jaguar Working Correctly?  
WebView Database Messages at Login
WebView Supervisors Rights and Active Directory Account
WebView User Unable to Change Password

Job Scheduler
Job Scheduler Does Not Work
  Are Terminal Services Running on the Client?  
  Does the User Have Access to a Printer?  
  Does the User have Minimum Rights?  
  Is ActiveX Enabled?  
  Is Fast User Switching Disabled on the Client?  
  Is the User Logged in When the Job is Triggered?  
  Is the WebView Server added to the Trusted Sites List?  
Job Scheduler File Not Found Message
Job Scheduler Upgrade Does Not Migrate Jobs to New Server

Reports and Templates
3000 Row Limit
Agent Data Does Not Appear in Reports
Blank Dialer Port Status Real-Time Report
Blank Pages When Report is Rendered 11-19
Caltype Items in Reports 11-19
Date Formats are Incorrect or Historical Reports do not show for a Specified Time Period 11-19
Error on Attempting to Select a WebView Template 11-20
Error Retrieving Information from the Web Server 11-20
Errors Running Reports 11-20
Graphical Reports Do Not Print 11-20
Graphical Reports Do Not Work Correctly 11-21
Header Truncated in French Reports 11-21
Historical Reports Do Not Work Correctly 11-21
  Historical Reports Fail 11-21
  Historical Reports Saved with Fixed Date Do Not Work Correctly 11-22
  Historical Reports Slow the System 11-22
Pages do not Display Correctly 11-22
Private and Favorite Reports Not Displayed After Upgrading 11-24
Saved Reports Do Not Work 11-25
Time difference between ICM Record and WebView Report 11-25
Preface

This preface describes the objectives of, and the intended audience for, this guide. It also has general information on how to access Cisco product documentation and how to obtain assistance with Cisco products. It contains these sections:

- About This Guide, page ix
- Related Publications, page xii
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page xiii
- Obtaining Technical Assistance, page xv

About This Guide

This section is an overview of the purpose, audience, and organization of this guide.

Objective

This guide explains how to perform an initial (“fresh”) installation of the WebView product for Cisco ICM/IPCC Enterprise & Hosted Edition and how to administer and maintain WebView after the installation.

For instructions on upgrading WebView from a previous version, refer to the ICM Upgrade Guide for Cisco ICM/IPCC Enterprise & Hosted Editions.

For assistance in using WebView, refer to the WebView online help.

Audience

This guide is intended for System Administrators who are responsible for installing and setting up WebView Reporting as part of an ICM/IPCC Enterprise/Hosted solution.

It will also be helpful to Contact Center Administrators who need to understand and troubleshoot operational processes that are outside the scope of the WebView online help.

The Administrators must have:

- General knowledge of contact center operations and management
- General knowledge of the operations performed by reporting users who log in to WebView
Preface

- Specific information about the contact centers and carrier networks connected to Cisco ICM and/or IPCC Enterprise software
- A solid understanding of the hardware, software, browser, and operating system specified in the Hardware and System Software Specification for Cisco ICM/IPCC Enterprise & Hosted Editions, Releases 7.0(0) and 7.1(x)


Sections of this guide also pertain to System deployments of IPCC Enterprise, as follows:

- Part 1 of this guide describes installation. In the System IPCC Enterprise deployment, WebView and the third-party tools are installed automatically. Therefore most of the information in Part 1 does not pertain to System IPCC Enterprise deployments.
  
  The exceptions are noted in sections on creating users, (page 3-5), on uninstalling WebView (on page 3-8), on uninstalling the third-party software tools (on page 2-9), and on multi-language installations (on page 1-16).

- Part 2 of this guide explains administration, maintenance, and troubleshooting. Most information in Part 2 is relevant to System IPCC Enterprise deployments unless specifically noted as not applicable.

  Refer to the System IPCC Enterprise guide and online help for full information on that deployment.

Organization

This guide is organized in two parts. Part 1 has chapters that pertain to installation. Part 2 has chapters that document ongoing administrative and maintenance operations.

<table>
<thead>
<tr>
<th>Part 1: Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1, “Understanding WebView”</td>
</tr>
<tr>
<td>Chapter 2, “Installing the Third-Party Software”</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Part 2: Ongoing Administration and Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter</td>
</tr>
<tr>
<td>---------</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>11</td>
</tr>
</tbody>
</table>

**Conventions**

This guide uses the following conventions.

<table>
<thead>
<tr>
<th>Format</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong> type is used for menu, tab, field, and command names.</td>
<td>Click Next.</td>
</tr>
<tr>
<td><strong>Courier</strong> type is used for file names, directory paths, code, and user input.</td>
<td>Peripheral services templates are stored in the persvc subdirectory.</td>
</tr>
</tbody>
</table>
Related Publications

The following documentation also pertains to WebView Reporting.


Document how to install and configure the system.

Database Schema Handbook for Cisco ICM/IPCC Enterprise & Hosted Editions

Documents how the Cisco ICM/IPCC Enterprise software organizes the database tables from which WebView reports access data.

Reporting Guide for Cisco IPCC Enterprise & Hosted Editions

Covers how reporting data is generated and how to interpret reporting data in an IPCC Enterprise Environment. Does not contain information on reporting in a traditional ACD contact center environment.

Reporting Guide for Cisco Unified ICM Enterprise & Hosted

Covers how reporting data is generated and how to interpret reporting data in an ICM Enterprise Environment.

Template Design Guide Using InfoMaker for Cisco ICM/IPCC Enterprise & Hosted Editions

Describes how to use Sybase InfoMaker™ to create custom report templates. Provides instructions on how to access and launch custom templates from WebView. (InfoMaker is an optional, third-party application for customizing WebView templates.)

IPCC Gateway Deployment Guide

Explains the differences between Simplified IPCC Express reports and reports for ICM/IPCC Enterprise.
WebView online Help

This help describes how to use WebView and includes reference descriptions of all the templates.

IPCC Enterprise Template Reference Guide

This manual describes the Cisco IPCC Enterprise WebView report templates. This material is also available in the WebView online help.

System IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition

This manual explains the System deployment of IPCC Enterprise.

In addition, you might need to refer to documents that explain how to install, configure, administer, and upgrade ICM and IPCC Enterprise. All of these guides are available for download in PDF format when you follow the Customer Contact Software link at this URL:
http://www.cisco.com/univercd/home/home.htm

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, security guidelines, and also recommended aliases and general Cisco documents, see the monthly What's New in Cisco Product Documentation, which also lists all new and revised Cisco technical documentation, at:

Documentation Feedback

You can provide comments about this document by sending email to the following address:
ccbu_docfeedback@cisco.com
We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:
From this site, you will find information about how to do the following:
• Report security vulnerabilities in Cisco products
• Obtain assistance with security incidents that involve Cisco products
• Register to receive security information from Cisco
A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:
http://www.cisco.com/go/psirt
To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

**Reporting Security Problems in Cisco Products**

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- **For emergencies only** — security-alert@cisco.com
  - An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- **For nonemergencies** — psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip**

We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.x through 9.x.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:


The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

**Product Alerts and Field Notices**

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:


To register as a Cisco.com user, go to this URL:

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:


Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:


Note

Before you submit a request for service online or by phone, use the Cisco Product Identification Tool to locate your product serial number. You can access this tool from the Cisco Support website by clicking the Get Tools & Resources link, clicking the All Tools (A-Z) tab, and then choosing Cisco Product Identification Tool from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting show command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip

Displaying and Searching on Cisco.com

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing F5.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the Advanced Search link next to the Search box on the resulting page and then click the Technical Support & Documentation radio button.

To provide feedback about the Cisco.com website or a particular technical document, click Contacts & Feedback at the top of any Cisco.com web page.
Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe
The Cisco Product Quick Reference Guide is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

http://www.cisco.com/go/guide

Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

http://www.cisco.com/go/marketplace/

Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

http://www.ciscopress.com

Internet Protocol Journal is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

http://www.cisco.com/ipj

Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:


Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

http://www.cisco.com/discuss/networking

“What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

World-class networking training is available from Cisco. You can view current offerings at this URL:

P A R T  1

Installation
Understanding WebView

This chapter introduces the WebView application, the components required to operate WebView, the sequence of installing those components, and the deployment models that are supported for WebView. This chapter includes the following topics:

- **About WebView**, page 1-2
- **WebView Components**, page 1-2
  - The Distributor Admin Workstation, page 1-4
  - The WebView Server, page 1-5
  - The WebView Client, page 1-7
  - The Web Browser, page 1-7
- **Sequence of Installing WebView Components**, page 1-9
- **The WebView Information Flow**, page 1-10
- **WebView Deployments for ICM/IPCC Enterprise**, page 1-12
  - Standard Deployment, page 1-12
  - Large-Customer Deployment, page 1-12
  - Migrating from a Standard to a Large-Customer Deployment, page 1-13
  - Primary/Secondary AW Deployment, page 1-15
  - Hosted Deployment, page 1-16
- **Multi-language Installations**, page 1-16
About WebView

WebView is a web-based query and presentation reporting application that allows access to reporting data over the corporate intranet.

WebView reporting users are typically individuals who supervise a group of agents and who rely on WebView reports to monitor contact center statistics for date and agent activity at the enterprise level.

Users log in by entering the WebView URL from the browser on their client PCs or workstations (http://<webviewserver>/<instance>). (If SSL is enabled for the full session, they must log in using https.)

Once logged in, they can generate real-time and historical reports that display integrated information about various aspects of contact center operations.

- Real-time reports offer up-to-the-minute data collected now and in the last five- and thirty-minute intervals.
- Historical reports present contact center activity in selected half-hour or daily intervals.

Reports are represented in both tabular and graphical formats. Report data is determined by the category and scope of the template the user selects and also by the items and date range the user chooses when generating a report from the template.

WebView is installed with more than 200 Cisco-provided report templates.

Users who require additional templates to meet specific analysis needs have the option to purchase, install, and integrate InfoMaker 10.x software from Sybase to create custom templates. Custom templates are typically modified versions of out-of-the-box WebView templates, with columns added or deleted and SQL queries added or revised. Refer to the Template Design Guide Using InfoMaker for Cisco ICM/IPCC Enterprise & Hosted Editions for the procedure to install and use InfoMaker to create custom templates.

The data sources for WebView reports are the real-time database (AWDB) and the Historical Database Server (HDS), which are created on the primary distributor Admin Workstation.

Favorite reports, saved report definitions, as well as scheduled report jobs, are stored in the WebView database (WVDB). This database is also located on the distributor Admin Workstation.

For more on these databases, see Databases on the Admin Workstation, page 1-4.

WebView Components

Various components comprise the WebView architecture. This section explains these components, requirements for them, and the sequence in which they must be deployed. All components are on the same hardware platform.

In a standard deployment, shown in the illustration below, WebView and the The Distributor Admin Workstation co-resident on the same server. The reporting user connects from a client PC. InfoMaker (an optional component used for custom reporting), must be installed on a separate machine that can access the WebView server (for templates) and the Admin Workstation databases). InfoMaker cannot be installed on the WebView server or on a distributor AW where WebView is installed.
Figure 1-1 WebView Components, Standard Deployment

WebView Components

AW Processes

WebView server

IIS (Web Server)

Third Party sw

WebView Reporting sw and templates

SQL Server Databases

AWDB

HD3

WDB

WebView Client

Distributor AW/ WebView Server

InfOMaker (optional)
The Distributor Admin Workstation

An Administrative Workstation (AW) is a PC that provides tools and resources to monitor the activity of the system and to manage the Unified ICM software. An AW can be one of two types: a distributor AW or a client AW.

The databases for WebView reporting reside on a real-time distributor Admin Workstation.

Note
Although it is possible to install the distributor AW after you install WebView, WebView will not work until you have installed the AW that hosts the databases used for reporting. For this reason, it is best to set up the Admin Workstation before you install WebView. Please see Sequence of Installing WebView Components, page 1-9.

Requirements for the Admin Workstation

The Admin Workstation must conform to the guidelines in the Hardware and System Software Specification for Cisco ICM/IPCC Enterprise & Hosted Editions, Releases 7.0(0) and 7.1(x) (BOM).

In addition, confirm that the Admin Workstation meets the following criteria:

- Is installed as a real-time distributor Admin Workstation, rather than a client (non-distributor) Admin Workstation. For information on how to determine this, refer to the IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition.
- Has an AW Database, which is a data repository for real time data (forwarded by the Router), configuration data copied from the Central Database, and scripts (copied from the Central Database).
- Can have an HDS Database, if the HDS option is enabled at setup.
- Uses the Microsoft Windows time synchronization facility to synchronize the time on the ICM WebView AW computer with the time on the ICM Central Controller. For details, refer to the ICM Installation Guide for Cisco ICM Enterprise Edition.
- If the WebView server and the distributor Admin Workstation co-reside on the same machine, refer to System Requirements for the WebView Server, page 1-6 to ensure that the Admin Workstation also meets the WebView server requirements.

If you are not sure that your Admin Workstation meets these requirements, contact your Cisco ICM software representative.

Databases on the Admin Workstation

These are the databases associated with WebView:

- The AW database (AWDB) is automatically created and initialized when you install the distributor Administrative Workstation. This real-time database is refreshed continuously (every 15 seconds, by default) with reporting data written to it by the AW distributors, which receive data from the peripherals.

Real-time data is stored in four time increments on a number of real-time tables in the local Admin Workstation database and is distributed to the Client AWs. Old real-time data is constantly overwritten by new real-time data.

Real-time data is the content of real-time WebView template, which are designated by the words "Real Time" or "Rolling 5 Minute" in their titles.
The AW database is the single point of access for WebView reporting data and provides views into the HDS.

- **The Historical Database Server (HDS)** receives and stores historical data and call detail data, which are forwarded from the Logger in five-minute and half-hour intervals.

An Historical Data Server (HDS) is required if you plan to use WebView historical reports. This historical data is not accessed directly, but rather through views that exist in the local Admin Workstation database. To retrieve information for historical reports, WebView connects to the AW where the HDS resides.

The Historical Data Server (HDS) must reside on a Distributor Admin Workstation. It is enabled at setup and created using the ICMDBA tool.

You can configure the size of the HDS and the duration for which data is retained.

For a fresh installation, you first install the distributor AW without checking the Historical Data Server box. Then create the HDS with the ICMDBA utility, and run setup locally to enable the HDS for the AW.

Note that as a fault-tolerant strategy, two Distributor AWs are typically set up at a site as HDS machines, each with its own HDS database.

For more on the real-time AW database and the HDS, refer to the *ICM Administration Guide for Cisco ICM Enterprise Edition*.

- **The WebView database (WVDB)** is created and enabled as an option when you set up the Admin Workstation. It stores saved report definitions, favorites, and scheduled report jobs. One AW in the system must have a WebView database installed on it, and multiple WebView servers must point to that one, shared WebView database. For more on the WebView database, see *About the WebView Database, page 5-2*.

**Note**

In a standard deployment, all three databases can be located on the same distributor Admin Workstation machine.

It is possible to set up multiple distributor Admin Workstations and to separate the databases. For example, in a large-customer deployment, the HDS can be on a separate Admin Workstation. It is also possible to set up a second (failover) WebView database located on separate Admin Workstation.

In these deployments, the machine where WebView is located must have network connections to the machines where the databases reside.

**The WebView Server**

The WebView server is the machine on which the following components reside:

- Microsoft Internet Information Services (IIS)
- Third-Party software
- WebView reporting software

At one time, you had to install the WebView server on a distributor AW. This remains a standard deployment option. However, you now also have the option to set up one or more ‘standalone’ WebView servers on machine(s) separate from, on the same domain as, and pointing to, the primary distributor.
Admin Workstation. Refer to the Hardware and System Software Specification for Cisco ICM/IPCC Enterprise & Hosted Editions, Releases 7.0(0) and 7.1(x) for information on the maximum number of WebView servers that can be connected to a single distributor Admin Workstation.

You cannot mix and match: that is, you cannot have both an all-in-one WebView/Admin Workstation and a standalone WebView server pointing to an WebView/Admin Workstation.

Therefore, if you initially configure a standard deployment (with the WebView server and the distributor AW server on the same machine), and you subsequently require more than one WebView server, you must uninstall the WebView reporting software and the third-party software on the AW and reinstall those components on a new machine. See Installing the Third-Party Software, page 2-6.

**System Requirements for the WebView Server**

- The WebView server must conform to the guidelines of the Hardware and System Software Specification for Cisco ICM/IPCC Enterprise & Hosted Editions, Releases 7.0(0) and 7.1(x) (BOM).
- In addition, confirm that the WebView server has sufficient RAM and sufficient free disk space for the Third-Party Software applications. See About the Third-Party Software, page 2-1 for more on these space requirements.
- If the WebView server and the distributor Admin Workstation co-reside on the same machine, the machine must conform to the requirements for the Admin Workstation. Refer to Requirements for the Admin Workstation, page 1-4.
- If the WebView server and the distributor Admin Workstation are on separate machines, the WebView server must have network connection to the primary distributor Admin Workstation.
- It must also be on the same domain as the Admin Workstation.

If you are not sure that your WebView server meets these requirements, contact your Cisco ICM software representative.

**Internet Information Services (IIS)**

Microsoft Internet Information Services (IIS) must be in place on the WebView server machine before you install software from the Third-Party CD. IIS serves the web pages for WebView reports.

IIS is shipped with Windows Server 2003. It is not installed by default with Windows Server 2003, but you can install it through the Add/Remove Windows Components utility.

IIS is installed by default with Windows 2000.

**Third-Party Software**

The ICM Third-Party Tools CD contains applications that must be in place to support WebView.

You must install this software on the WebView server machine, and you must install it before you run ICM setup to install WebView.

WebView Software

WebView software is installed as an ICM component from ICM Setup tool. WebView setup creates and installs:

- Application-specific files
- Cisco reporting templates
- The Jaguar Watchdog service


The WebView Client

A WebView client is simply a Windows-based PC or workstation running a supported web browser.

The Web Browser

WebView requires that a supported browser be installed on each client PC that logs in to WebView. Refer to the Hardware and System Software Specification for Cisco ICM/IPCC Enterprise & Hosted Editions, Releases 7.0(0) and 7.1(x) for the browser that is currently supported.

Several modifications are required to enable the browser to perform optimally with WebView. These modifications must be enabled at each client browser.

- Add the WebView server(s) to Trusted Sites.
- Ensure browser cache updates.
- Ensure display of WebView server error messages.

Procedures to check these three settings are documented on the next two pages.

In addition, some users might also need to do the following:

- Change the language setting to display reports with the native date format. See Localizing the Browser Language Setting, page 1-19.

Add the WebView server(s) to Trusted Sites

**Step 1** In the browser, select Tools > Internet Options > Security.

**Step 2** Click Trusted Sites. Then click Sites...

**Step 3** Clear the checkbox for Require server verification (https) for all sites in this zone.

**Step 4** In the Trusted Sites dialog box, add each of your WebView servers. (http://webview server and https://webviewserver).

**Step 5** Click OK to apply the setting and close the Trusted Sites dialog box.

**Step 6** Click Custom Level on the Security tab and verify that the following are enabled:

- Download signed ActiveX controls
- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting
Step 7  Click Cancel, or click OK and confirm if you have changed any of these settings to enable them.

Step 8  Click OK again.

Ensure browser cache updates

Use the following procedure to make sure the cache is updated at each new view of a real-time report.

Step 1  In the Internet Explorer window, choose Tools > Internet Options.

Step 2  On the General Settings tab (Temporary Internet Files section) click Settings.

Step 3  In the Settings dialog box, enable Every visit to the page, then click OK.

Step 4  Click OK to close the Internet Options dialog box.

Ensure display of WebView server error messages

 Occasionally, you might see a blank page. This happens when the WebView Server sends an error message, but your browser is configured to mask the text message. Use the following procedure to ensure that you see an error message, and not a blank page.

Step 1  In the Internet Explorer window, choose Tools > Internet Options.

Step 2  Click the Advanced tab.

Step 3  Under Browsing, clear the checkbox for Show friendly HTTP error messages.

Step 4  Click Apply. Then click OK to close the Internet Options dialog box.
Sequence of Installing WebView Components

This is a high-level overview for the sequence of installing WebView and its components.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Review the deployment options and decide if you will install WebView to co-reside with the distributor Admin Workstation, or if you will install ‘standalone’ WebView server(s). See WebView Components, page 1-2 for an explanation of the deployment options.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Make sure that Microsoft Internet Information Services (IIS) is installed at the machine where you will deploy WebView.</td>
</tr>
</tbody>
</table>
| Step 3 | Run ICM Setup for the distributor AW that will host the databases that WebView uses. Setup is documented in the ICM Installation Guide for Cisco ICM Enterprise Edition. At the Real-time Distributor Properties dialog box for the distributor AW setup:  
  - Do not check ‘Second distributor for site’.  
  - Check WebView Database  
  - Do not check Historical Data Server.  
  For a fresh installation, you must first install the primary distributor AW without checking the Historical Data Server box. Then create the HDS with the ICMDBA utility, and run Setup locally to enable the HDS for the AW.  
  If you check the Historical Data Server box when you initially set up the distributor AW, and no HDS database has yet been installed, inappropriate values can be set that will not be reset by simply creating the database later. |
| Step 4 | After you complete ICM Setup, use the ICMDBA tool to create the HDS. Refer to the ICM Administration Guide for Cisco ICM Enterprise Edition for the procedure to do this. |
| Step 5 | Re-run ICM Setup for the real-time Administrator Workstation you created in Step 2. This time, check the Historical Data Server. |
| Step 6 | Install the third-party software on the WebView server. See Chapter 2. |
| Step 7 | Re-run ICM Setup on the WebView server and install WebView. See Chapter 3 of this guide. |
| Step 8 | Optionally, install Sybase InfoMaker on a separate machine (NOT on the same machine where you installed WebView). |
The WebView Information Flow

Figure 1-2  A diagram of the WebView system program-execution flow

Note  This illustration shows the WebView server and the distributor Admin Workstation on separate machines.

They can reside on the same machine.

These steps describe the flow illustrated in Figure 1-2.

Step 1  The client makes a request to access WebView.
Step 2  IIS displays WebView to the user.
Step 3  After several requests and responses (steps 1 and 2 repeated a few times), the client requests a report.
Step 4  NewAtlanta is called to compile the JSP page.
Step 5  The EAServer component is invoked to query the database.
Step 6  The query is sent, based on the template chosen.
Step 7  The data is returned to EAServer.
Step 8  Jaguar generates the HTML based on the chosen template.
Step 9  NewAtlanta uses the HTML to finish compiling the page.
Step 10 The report page is served back to user.
WebView Deployments for ICM/IPCC Enterprise

This section explains supported deployments for Cisco ICM/IPCC Enterprise WebView: standard, large-customer, and hosted. It also explains how to migrate from a standard to a large-customer deployment and how to work with primary/secondary AWs. These models are based on sizing/capacity specifications defined in the Hardware and System Software Specification for Cisco ICM/IPCC Enterprise & Hosted Editions, Releases 7.0(0) and 7.1(x).

Standard Deployment

For a standard deployment, WebView software co-resides with the reporting databases on an Admin Workstation/WebView server. That is, the same server hosts these components:
- The real-time distributor AW
- The real-time AW database, the HDS database, and the WebView database
- Third-party software required for WebView
- WebView reporting software, WebView templates, and IIS

You can have multiple standard (all-in-one) servers. In this case, only one has a WebView database, and all must point to that shared WebView database.

Large-Customer Deployment

In a large-customer deployment, WebView is installed on one or more ‘standalone’ server(s), separate from the distributor Admin Workstation.

The components installed to the WebView server(s) are IIS, the Third-Party software, the WebView software, and WebView templates.

Database-class servers are not required for these individual WebView servers, since the WebView database, the real-time distributor database, and the HDS (and Microsoft SQL Server) must reside on the distributor AW server.

All standalone WebView servers point to the databases on the AW.

Figure 1-3  WebView Standard Deployment
Use this model to accommodate sizing and capacity as defined in the *Hardware and System Software Specification for Cisco ICM/IPCC Enterprise & Hosted Editions, Releases 7.0(0) and 7.1(x).*

**Figure 1-4 WebView Large-Customer Deployment**

---

**Migrating from a Standard to a Large-Customer Deployment**

This section explains the procedure to follow if you initially configure a standard deployment (with WebView and the distributor AW co-resident on the same machine) and subsequently migrate to a large-customer deployment model (where the WebView server is installed on a separate machine).

Follow this procedure to change from a Standard (all-in-one) to a Large deployment:

**Step 1** If you have created and saved custom templates on the distributor Admin Workstation, copy all of the template libraries to the new machine where the standalone WebView server will reside. To do this:

a. On the distributor Admin Workstation, navigate to `<icmroot>\<inst>\aw\custom`.

b. Copy the entire folder and paste it in the new WebView server machine.

**Step 2** Stop the services for the third-party software as follows:

a. Click **Start > Programs > Administrative Tools > Services**.

b. Right-click each of the following services and select **Stop**:
   - Cisco ICM Jaguar Watchdog
   - Jaguar
You can delete the third-party applications from the distributor AW, but it is sufficient to stop their services.

See Uninstalling and Reinstalling the Third-Party Software, page 2-9 for instructions to remove the third-party applications.

**Step 3** Remove WebView from distributor AW machine. To do this:

a. Select **Start > Programs > ICM Admin Workstation > Setup**.

b. At the Cisco ICM Setup screen:
   - Select the Instance.
   - Select WebView.
   - Click **Delete**.

**Step 4** Run a fresh installation of the third-party applications on the new machine.

See Installing the Third-Party Software, page 2-6 for the procedure.

**Step 5** Run a fresh installation of WebView on the new machine.

Point the new instance of WebView to the machine locations for the HDS-enabled Admin Workstation distributor and the WebView database.

See Installing Cisco ICM/IPCC Enterprise WebView Software, page 3-3 for the complete procedure to install WebView.
Primary/Secondary AW Deployment

Some organizations set up both a primary and a secondary distributor Admin Workstation. Refer to the *ICM Installation Guide for Cisco ICM Enterprise Edition* for an explanation of why and how you do this.

If your organization deploys ICM/IPCC Enterprise with a primary and a secondary distributor Admin Workstation, please note the following:

**For ‘fresh’ Release 7.0 installations:**

- If WebView is on the same machine as the distributor Admin Workstation, then it must be installed on the primary AW.
- If WebView is installed on a separate machine, then it must point to databases (the AW database, the HDS, and the WebView database) on the primary Admin Workstation.

**For upgrades from Release 5.0 or 6.0 to Release 7.0:**

- If WebView is on the same machine as the primary Admin Workstation, simply upgrade to Release 7.0.
- If WebView is on the same machine as the secondary Admin Workstation, you must either:
  - Convert the secondary AW to a primary AW, change the site name, and then upgrade to Release 7.0.
  - Remove WebView from the secondary AW.
- If you prefer to install WebView on a separate machine, remove it from the AW and point it to databases (the AW database, the HDS, and the WebView database) on the primary Admin Workstation.

---

**Note**

There can be only one WebView database, and it needs to be on the primary AW.

**Note**

If you accidentally upgrade a secondary AW that has WebView installed on it, you must remove WebView from the secondary AW.
**Hosted Deployment**

Hosted environments allow service providers and large businesses to route calls to child instances that are dedicated to specific customers or business entities.

Each instance has dedicated real-time AW and HDS databases that contain reporting data for that instance. All instances share a single WebView server and a single WebView database.

As with all deployments, reporting users log in with a web browser on their local PC to connect to their WebView server instance.

WebView determines which database to connect to based on the URL in the browser (https://<webviewservename>/<instancename>). Users of one instance cannot log into another instance.

*Figure 1-5* shows the distributor AW/WebView server in a hosted environment with four reporting instances. This illustration shows WebView installed on the distributor Admin Workstation.

Refer to the *Hardware and System Software Specification for Cisco ICM/IPCC Enterprise & Hosted Editions, Releases 7.0(0) and 7.1(x)* for guidelines on how best to set a hosted deployment for your customer population.

*Figure 1-5  Hosted Reporting Deployment*

---

**Multi-language Installations**

With release 7.0(0), it is possible to install WebView on a server other than the distributor AW and, in that deployment, to select a language at WebView setup. In addition, it is possible to have WebView clients installed on machines with various Microsoft Windows language settings and browser language settings.

This section contains information to clarify certain language-related issues. Also see Chapter 7, “Time and Date in Reports” and Chapter 11, “Troubleshooting Tips” in this guide for information about language settings.
Character Set and Databases

The character set used in ICM 7.0(0) databases is determined by the collation designator of SQL2000 Server. ICM 7.0(0) supports the following Collation Designators only: Latin1, Japanese, Chinese_PRC, and Korean_Wansung.

ICM 7.0(0) supports ASCII characters only—except for the Agent Names, Description, and Reason Code fields. Validation rules do not apply to these three fields. This means that in a Japanese installation, users will see the WebView user interface in Japanese, Agent Names, Reason Codes, and Descriptions in Japanese, but all other reporting data will be presented using ASCII characters.

The correct fonts must be available for these fields to display correctly.

Data is stored in the AW and HDS databases in native character sets.

UK customers are no longer required to set “British English” as the default language for SQL groups created by ICM7.0, and pbodb100.ini is not required to be installed on a UK platform.
Language Selection at Setup

Language selection is a required parameter when you run ICM Setup to add the distributor AW and to add WebView.

If you install the AW and WebView on the same machine, the language for the component you add first (typically, the AW) sets the registry key for the other component.

In a standard deployment, if you set up the distributor AW first and select a language, the language list dropdown is greyed out when you set up WebView.

However, if you install WebView first and then install the AW, you can change the language. You will see a message indicating that your change of language will initiate a replacement of the WebView templates to the templates for the new language.

In a large-customer deployment, when you install the AW and WebView on separate machines, select the same language for each.

The languages you can select at installation are:

- Brazilian Portuguese
- Danish
- Dutch
- English (US)
- English (UK)
- French (Canada)
- French (France)
- German
- Italian
- Japanese
- Korean
- Russian
- Simplified Chinese
- Spanish
- Swedish
- Traditional Chinese

Language selection affects the user interface, online help, and template installation as follows. Date format is determined by the client browser's setting. See How Date Formats are Set, page 7-3 for more on this.
Localizing the Browser Language Setting

A WebView client is a Windows-based PC or workstation running the supported Internet Explorer web browser. The default language for the browser is set during the Windows installation, and in most cases, you never need to change it.

For two of the languages that WebView supports (English U.K. and French Canadian), there is an IE browser language but no Windows platform language.

If you selected to install the French Canadian or the English (U.K.) version of WebView, you might want to set the language of the IE browser to `fr-ca` or `en-gb`.

**Note**
There are reasons *not to* maintain different localized browser languages. See Dates and Date Ranges in Mixed-Language Installations, page 7-5 for details.

To change the language setting in the browser:

- **Step 1** From the browser, select **Tools > Internet Options**.
- **Step 2** In the General tab, click **Languages** to open the Language Preference dialog box.
- **Step 3** Click **Add**.
- **Step 4** Scroll to select **English (United Kingdom)** or **French (Canada)**.
- **Step 5** Click **OK** to return to the Language Preference dialog box.
- **Step 6** Use the **Move Up/Move Down** buttons to move the language you added to the top of the list.
- **Step 7** Click **OK** to close all Internet Option dialog boxes.
Installing the Third-Party Software

This chapter explains how to install software from the ICM Third-Party Tools CD.
It contains the following topics:

- About the Third-Party Software, page 2-1
- Installing the Third-Party Software, page 2-6
- After You Install the Third-Party Software, page 2-7
- Maintaining Third-Party Software, page 2-7
- Uninstalling and Reinstalling the Third-Party Software, page 2-9

Before you install the software from the ICM Third-Party Tools CD, be sure to read Chapter 1, “Understanding WebView.”

Chapter 1 contains topics that explain the requirements for the WebView server machine where you will install the Third-Party Software CD and your deployment model options (to install the third-party software on the distributor Admin Workstation or on one or more separate WebView servers)

About the Third-Party Software

If you administer an ICM/IPCC deployment, you have received a CD for the ICM Third-Party Tools. This CD contains applications that are necessary to support WebView Reporting.

*The Third-Party tools are installed on the WebView server machine.*

If you have a large-customer deployment in place (where WebView is installed on one or more separate machines) you install the Third-Party tools on the standalone WebView server machines only, and not on the distributor Admin Workstation.

*Note*  
If you administer a System IPCC Enterprise deployment, the third-party installer runs automatically from the DVD. You do not need to take an action to install the third-party tools.

Sequence of Third-Party Software Installation

The applications on the ICM Third-Party Tools CD must be:

- Installed on each WebView server machine where you will set up WebView reporting
- Installed before you run ICM Setup to install WebView
Administrator Rights for Third-Party Software Installation

You must be an administrator with local admin and setup rights on the machine where you intend to install the third-party software.
Chapter 2      Installing the Third-Party Software

Applications on the CD

The ICM Third-Party Tools CD includes the following applications:

- Sun JDK version 1.4.2
- New Atlanta ServletExec ISAPI version 5.0.0.18
  (This software compiles servlets and JSP pages.)
- Sybase EA Server version 5.1.0
  (This software contains the logic for generating reports and querying the database.)

**Note** Sybase EAServer is also referred to as Jaguar Server and as Enterprise Application Server.

- PowerBuilder Virtual Machine version 10.x.
  This application is not visible to reporting users. However, after the third-party software installation, it appears in Control Panel under Add/Remove Programs.

Note that these are the third-party software versions at the time this guide was prepared.

For complete and current information on the third-party software versions, see the *Hardware and System Software Specification for Cisco ICM/IPCC Enterprise & Hosted Editions, Releases 7.0(0) and 7.1(x) (BOM).*

About Sybase InfoMaker Software

Another third-party application, Sybase InfoMaker, is available for use with WebView Reporting to create and modify custom templates. Unlike the software on the ICM Third-Party Tools CD, InfoMaker is optional, must be purchased separately, and cannot be installed on the WebView server or the distributor Admin Workstation machines.

If you need to create custom templates, you must purchase InfoMaker from Sybase, Inc.

Refer to the *Template Design Guide Using InfoMaker for Cisco ICM/IPCC Enterprise & Hosted Editions* for instructions on installing InfoMaker.

**Note** InfoMaker must NOT be installed on the WebView server machine or on a distributor AW where WebView is installed. Certain DLL files that InfoMaker installs interfere with the software in the AW and the WebView server machine.

For information on installing InfoMaker, see the *Template Design Guide Using InfoMaker for Cisco ICM/IPCC Enterprise & Hosted Editions.*

Before You Install the Third-Party Software

This section has information on final checks to make before you begin the third-party software installation:
Ensure Adequate Disk Space and RAM

Make sure that you have sufficient space on the drive where you intend to install the third-party software. The installer software uses approximately 10 MB of RAM and 1 MB of space on the hard drive while running.

If the drive runs out of space in the middle of the installation, you must end the installation process and start over on a drive that has more space.

- Sun JDK requires 60 MB. By default, it is installed to `c:\j2sdk1.4.2_04`.
- New Atlanta Servlet Exec ISAPI requires 15 MB. By default, it is installed to `C:\Program Files\New Atlanta\ServletExec\ISAPI`.
- Sybase EAServer requires 450 MB. By default, it is installed to `C:\Program Files\Sybase\EAServer`.

Regardless of the drive where you install EAServer, the EAServer installation requires that the `TEMP` environment variable be set, and that the drive that contains that directory has at least 300 MB of free space. Additionally, the installation requires 500 MB of working space on the C:\ drive. After the installation, this space is no longer required.

Remove Older Versions of Jaguar Software

There is no upgrade path from some older Jaguar versions. If the machine where you intend to install the third-party tools has this software, you must manually remove it before you run the setup for third-party tools.

Step 1 Check to see if Jaguar 3.5 of Jaguar 3.6.1 software is installed on the machine where you intend to run the Cisco WebView Third-Party Software installation.

Step 2 If it is, see Removing Old Versions of EAServer/Jaguar, page 11-10 for directions to manually remove the software.

Check for New Atlanta Servlet Exec

The third-party software cannot be installed on the same machine as another application that depends on a specific configuration of New Atlanta ServletExec.

Although the third-party installation installs New Atlanta Servlet Exec with no configuration, the ICM Setup for WebView modifies the New Atlanta configuration to work with WebView.

If another application that depends on New Atlanta Servlet Exec is already installed on the machine, you cannot reliably share that machine with WebView. In particular, ICM WebView cannot be co-located with Cisco E-Mail Manager or Cisco Web Collaboration options, which require specific New Atlanta ServletExec configurations.

Suspend Cisco Security Agent

Step 1 Check to see if you have Cisco Security Agent running on your machine.

Step 2 If you are using Cisco Security Agent, suspend the CSA service before running the third-party software Setup.
Refer to *Cisco Security Agent Installation Guide for Cisco ICM/IPCC Enterprise & Hosted Editions* for more on the Cisco Security Agent.
Installing the Third-Party Software

The third-party software installation procedure can take from 30 to 50 minutes depending on the speed of the machine and the resources available on it.

The following is a summary of the installation procedure. See the README.txt file on the ICM Third-Party Tools CD for any further information.

---

**Step 1**
Insert the ICM Third-Party Tools CD and run the top-level Setup.exe program.

**Step 2**
Click Next at the Welcome screen and follow the instructions presented on the screens that follow it.

The Setup program displays a dialog box listing the third-party software that is required by WebView.

- Any software that *is not* already installed on your system is automatically checked (selected for installation) and is grayed out in this dialog box.
- Any software that *is* already installed on your system and has the same version as the version on the CD is not checked (selected for installation).

The Setup program does not reinstall software that is already installed on your system if its version number has not changed.

**Step 3**
Review the automatically selected software options.

**Note**
If you want to re-install any unselected options, you must cancel out and **manually uninstall** them before you continue with the Third-Party installation. **Do not install software ‘over itself’**.

**Step 4**
Click Next.

**Step 5**
At the prompt to choose the destination location for the files, select or enter the directory location. The default locations for a new installation are:

- For Sun JDK:  
  C:\j2sdk1.4.2_04

- For New Atlanta Servlet Exec:  
  C:\Program Files\New Atlanta\ServletExec\ISAPI

- For Sybase EAServer:  
  C:\Program Files\Sybase\EAServer

**Note**
Cisco Security Agent requires that you use the default directory when installing any software on a server. You can change the default disk drive if an option is available (for example, from C:\ to D:\), but you must use the default. If you do not, CSA will not allow the software to execute.

**Step 6**
Click Next to begin the installation.

Status messages appear during the installation.

At one point, warnings might appear in a console command-line window indicating defaults that the installation is choosing for unspecified parameters:

These messages are produced by the EAServer installation and are expected.

**Step 7**
When the installation is complete, you are prompted to reboot your computer now or at a later time. Make your selection and click Finish.

**Step 8**
Restart the server.
Chapter 2      Installing the Third-Party Software

After You Install the Third-Party Software

When you complete the third-party installation and reboot the computer, you are ready to install WebView from the ICM Setup utility. See Chapter 3, “Installing WebView” for the procedure to do this.

Maintaining Third-Party Software

Several chapters in this guide contain additional information about maintaining and administering the third-party software:

See Chapter 6, “Jaguar Administration and the Jaguar Watchdog,” for information on Jaguar. Chapter 11, “Troubleshooting Tips” also has a number of tips on managing the third-party software.

For example, see Third-Party Software Licenses for information on installing New Atlanta on a server that has more than four processors.

Changing the New Atlanta ServletExec password

By default, the New Atlanta ServletExec is installed with a blank Administrator password. You may need to reset your password if

- the access to the ServletExec Administration tool requires local access to this server
- your environment requires a higher level of security.

How to change the New Atlanta ServletExec password

Step 1  In the Start menu, select Programs > New Atlanta > ServletExec 5.0 ISAPI > ServletExec Admin. This opens the ServletExec Administration page.
Step 2  Enter "admin" as the login name and leave the password blank.
Step 3  From the left panel under Web Applications, select Users. A list of users appears on the right panel.
Step 4  Select Admin from the list of users.
Step 5  Enter a new password in the Administrator Password field and click Submit.
Step 6  Logout from the ServletExec Administration login page.
        Your password in reset. You can now login to the ServletExec Administration page with new password.
Uninstalling and Reinstalling the Third-Party Software

There are two methods for uninstalling the third-party software:

- You can uninstall it "manually" using the procedure documented below.
- You can run the WVThirdPartyUnInstaller.vbs tool. See Uninstalling the Third-Party Software Programatically, page 2-11.

Please note that whichever method you choose, you will uninstall the tools provided on the WebView third-party tools CD only. These tools are listed in Applications on the CD, page 2-3.

Note that the WebView Third-Party Uninstaller process does not uninstall:

- The Cisco SNMP Service, because SNMP Service is not a WebView third-party tool.
- The Jaguar Watchdog service, because that WebView tool is installed by ICM Setup and is not a third-party tool.

Uninstalling the Third-Party Software Manually

This section explains how to manually uninstall and remove the third-party applications.

You can uninstall most of the third-party applications using Windows Add/Remove Programs. You need to remove Jaguar manually.

Step 1
If you do not have a System deployment of IPCC Enterprise, skip this step and start with Step 2.
If you administer a System deployment of IPCC Enterprise, create a temporary directory and copy the following files to it:

- These directory trees:
  C:\Program Files\Sybase\EAServer\html\classes\webview
  C:\Program Files\Sybase\EAServer\html\classes\com\cisco
  C:\Program Files\Sybase\EAServer\Repository\Component\WebView
  C:\Program Files\New Atlanta\ServletExec ISAPI\ServletExec Data
  C:\Program Files\New Atlanta\ServletExec ISAPI\Servlets
  C:\Program Files\New Atlanta\ServletExec ISAPI\webapps

- These files:
  c:\Program Files\Sybase\EAServer\Repository\Server\Jaguar.props
  c:\Program Files\Sybase\EAServer\Repository\Package\webview.props

Step 2
Stop services as follows:

a. Click Start > Programs > Administrative Tools > Services.
b. Right-click each of the following services and select Stop:
   - Jaguar
   - Jaguar Watchdog
   - IIS Admin Services

Step 3
Remove these third-party tools by uninstalling them as follows:

a. Click Start > Settings > Control Panel > Add/Remove Programs.
b. Select and each of these programs and click Remove:
Uninstalling and Reinstalling the Third-Party Software

Chapter 2 Installing the Third-Party Software

Note

Respond to all operating system prompts, including the prompt to reboot, if it appears. If you do need to reboot, repeat Step 2 to stop services.

Step 4 Remove EAServer/Jaguar manually as follows:

a. Click Start > Programs > Accessories > Command Prompt and change directory to C:\Program Files\Sybase\EAServer\bin.

b. Enter this command to remove the Jaguar service: serverstart.bat -remove.

c. Close the Command Prompt.

d. From Windows Explorer, search for Sybase folders in these locations: C:\Program Files and C:\Documents and Settings. Delete all Sybase folders found in these directories.

e. Run Regedit and delete the Sybase key under HKEY_LOCAL_MACHINE\Software.

f. Delete environmental variables as follows:

   – Right-click My Computer and select Properties.

   – Under the Advanced tab, click Environment Variables.

   – Under the System variables section, locate and delete these variables: JAGUAR and JAGUAR_CLIENT_ROOT.

   – Also under the System variables section, edit the PATH and CLASSPATH to remove references to the Sybase folder.

If you do not have a System deployment of IPCC Enterprise, reinstall as follows:

• Re-install the Third-Party software from the Third-Party CD, as documented on page 2-6.

• Run ICM Setup in Upgrade All mode.

If you administer a System deployment of IPCC Enterprise, reinstall as follows:

• Stop Cisco Security Agent.

• Re-install the third party software from the System IPCC DVD. The installer is located in Support Files\ThirdPartyInstallers\WebViewThirdParty.

• Copy the directories and files you moved in Step 1 back to their original locations.

• On the drive where you installed System IPCC Enterprise, navigate to icm\bin\.

   – Run IPCCADinitializer.exe.

   – Run wvconfig.bat.

   If you had never changed the Jaguar Admin password, your reinstallation is complete.

• ONLY IF you had changed the Jaguar Admin password before you reinstalled the third-party tools, reset it using EAServer Manager. (Start > Programs > Sybase > EAServer 5.1.0 > EAServer Manager).

See Changing the Jaguar Admin Password, page 6-1 for details.
Reinstalling the Third-Party Software Manually

Reinstall the third-party software as follows:

- **For System IPCC**, the Third-Party software is installed automatically when you reinstall SIPCC from System IPCC Enterprise DVD.
  Follow the instructions in the *System IPCC Enterprise Installation and Configuration Guide*. This option is recommended if and only if you need to uninstall and reinstall SIPCC.

- **For IPCC/ICM**, run the ICM Third-Party Tool CD, following the instructions earlier in this chapter (Installing the Third-Party Software, page 2-6).

Uninstalling the Third-Party Software Programatically

The manual process for uninstalling the third-party tools is a complex procedure with high risks of failure.

Cisco now offers a tool that automates the uninstall/reinstall of WebView Third-Party software. The utility, named WVThirdPartyInstaller, is distributed with ICM, IPCC and SIPCC for versions 7.0(0) SR 3, 7.0(0) SR4, 7.1(x), 7.2(1), and any newer major, minor or maintenance release.

Using the utility reduces the risk of manual errors and eases the process of uninstalling WebView Third-Party software.

The location and filename of the tool is as follows: `icm\bin\WVThirdPartyUnInstaller.vbs`

- **Note** This tool runs on Windows 2003 only and should only be run under the supervision of the TAC.

To run this tool:

Open a Command Prompt and run following command with the appropriate arguments:

```
WVThirdPartyUnInstaller.vbs [/uninstall] [/postinstall] [/reinstall:]
```

- **/uninstall:** Uninstall all WebView Third-Party components
- **/postinstall:** (System IPCC Only) For System IPCC, certain files are backed up before the uninstallation process and then copied back into place after reinstallation.
  - If you are using System IPCC and use the uninstall argument just to uninstall, you must run this script again with the postinstall argument in order to put those files back into place.
- **/reinstall:** Perform all steps for uninstall and postinstall of the WebView Third-Party Installer. This option requires an additional argument to define the path to the WebView Third-Party Installer (if local or use the media might be applicable).
  - **For System IPCC:** `\Support Files\ThirdPartyInstallers\WebViewThirdParty`. No additional steps are required after the WebView third party software is installed.
  - **For IPCC/ICM:** You need to run IPCC/ICM setup from the IPCC/ICM media after the WebView third party software is installed.
Installing WebView

This chapter explains how to install Cisco ICM/IPCC Enterprise WebView software and how to set up users. It contains the following topics:

- About WebView Software, page 3-1
- Installing Cisco ICM/IPCC Enterprise WebView Software, page 3-3
- About WebView Users, page 3-5
- Creating WebView Users, page 3-5
- Logging into WebView, page 3-7
- Troubleshooting Your WebView Installation, page 3-8
- Uninstalling WebView, page 3-8

About WebView Software

WebView is selected and added as an instance component from the ICM Setup program, which you run from the ICM Software CD.


About WebView Installation

ICM Setup for WebView must be installed on the same machine where you have installed the third-party software.

Depending on your deployment model, this can be the same machine as the distributor Admin Workstation, or it can be on one or more separate machines.

WebView must be installed after you have:

- Set up a primary distributor AW with WebView Database checked but without enabling Historical Data Server (HDS).
- Created the HDS with the ICMDBA tool.
- Rerun ICM Setup to enable Historical Data Server.
  The HDS must be created and enabled if WebView is to report from it.
• Installed the third-party tools and rebooted.
Refer to Sequence of Installing WebView Components, page 1-9.

Administrator Rights for WebView Installation

The person who installs Cisco ICM/IPCC Enterprise WebView software product, either on the distributor Admin Workstation or on a separate server, must have local administrator and setup rights for the instance.

Cisco Security Agent and Installation

If the current version of CSA (CSA 4.5) is running, Setup displays a warning message and asks for permission to stop CSA.
If permission is granted, Setup stops CSA, and when installation is completed, automatically restarts CSA.
If you have CSA installed but it is not the current version, a message displays (whether or not CSA is running) telling you that you do not have the latest version.
Refer to the Cisco Security Agent Installation/Deployment Guide for ICM/IPCC Enterprise & Hosted Editions for more on CSA.
Installing Cisco ICM/IPCC Enterprise WebView Software

The WebView installation takes approximately 10 minutes, depending on the speed of the machine and the resources available on it.

**Step 1**
Insert the ICM Software CD. Locate and run the `Setup.exe` program at the top level of the directory. The Cisco ICM Setup dialog box opens.

**Step 2**
In the left column, select the ICM Instance to which you want to install WebView and click Add. The ICM Component Selection dialog box opens.

**Step 3**
Click WebView.
If ICM Setup detects that any of the required third-party tools (JDK, EAServer, or New Atlanta Servlet) are not installed on the server, you will see an error message, and the installation cannot proceed.
If all third-party tools are in place, you see the WebView Node Properties dialog box.

**Step 4**
At the WebView Node Properties dialog box:
- **Drive**: Accept the default drive (C), or enter a different drive letter.
- **Language**: This is enabled only if you have not already installed the distributor AW at this machine. Accept the default (English American) or select from the other options.
  See Language Selection at Setup, page 1-18 for further information.

**Note**
A System IPCC Enterprise deployment can be installed on an English platform only.

**Step 5**
Select Database Locations.
- **WebView Database Hostname**: Enter the machine name of the computer that holds the database WebView will use to store saved reports, favorites reports, and scheduled jobs.
- **Distributor AW Hostname**: Enter the machine name of the computer where the HDS is enabled.

**Step 6**
Select the **Outbound Option Support** checkbox only if you want to install the Outbound Option reporting templates. Leave it blank if you do not use Outbound Option. This is blank by default.

**Step 7**
Configure SSL 3.0 Encryption for WebView.

**Note**
These settings are enabled only if you are installing on a Windows 2003 server. When these settings are not enabled, SSL will be turned off.

Leave **Enable Encryption (128-bit) for Authentication** checked (the default) to accept Secure Socket Layer encryption. Clear it if you do not want to enable SSL.

Check **Enable Encryption of the Entire Session** only if you want all pages to be encrypted. By default, this is not checked.

For more on SSL Encryption, see About SSL, page 10-4.

**Step 8**
Click Next to see a read-only screen showing the parameters you set in Steps 5 through 8.
You can click Back from this screen to return to the WebView Node Properties dialog box to edit your selections.

**Step 9**
Click Next to proceed with the installation.
You see a progress bar and messages as WebView files, WebView templates, and Jaguar Watchdog files are installed.

Step 10  At the Restart dialog box, click **Restart**.

See [Users Unable to Log in to WebView, page 11-12](#) for the list of logs that record WebView installation.
About WebView Users

To access WebView, you must:

- Be added as an Active Directory user.
- Have network access to the WebView server.
- Install a supported Web browser and enable the browsers settings appropriately. See The Web Browser, page 1-7.
- Enter the correct WebView URL: http://<webviewserver>/<instance>.

Note: If SSL is enabled for the full session, enter https://<webviewserver>/<instance>.

Creating WebView Users

WebView reporting users are administrators who connect to the WebView server to run WebView reports.

In Release 7.0(0), the preferred method to create WebView reporting users is by using Active Directory authentication and adding users to the WebView domain group.

There are three levels in the ICM/IPCC Active Directory hierarchy: Instance, Facility, and ICM Root. At each level, there is a WebView group.

In order to login to WebView with full access, a user must be a member of at least one of the following:

- the WebView group of the Instance
- the WebView group of the facility that contains the Instance
- the WebView group of the ICM Root

For more on how to use the Domain Manager Tool to add users to the WebView Domain Security Group, refer to the Domain Manager online help. Also see WebView User Authentication Model, page 10-2.

In a System IPCC Enterprise deployment, users are added using the web-based administration tool. Refer to the System IPCC Web Administration tool online help for more information.

ICM Configuration Manager User List

Prior to Release 7.0(0), users were added with the ICM Configuration Manager User List tool.

You can still use this tool to add users with restricted access, for example, to add ‘read-only’ access or to enforce feature control.

Also use the Configuration Manager to create WebView supervisors. (WebView supervisors are agents who are configured to run WebView reports for their agents, teams, and skill groups and to change configuration for their teams.)

Refer to the ICM Configuration Manager tool online help for further explanation.
WebView Supervisors

An individual who is created as a WebView user through Active Directory and who is also configured as a Supervisor through Configuration Manager will be treated as a Supervisor in WebView and will see restricted information in WebView reports.

Specifically, on Agent reports, a Supervisor can select as report items only those agents and agent teams that he or she has been configured to supervise:

- In the Agent-by-Agent subcategory, Supervisors can select as report items only those agents who are assigned to teams supervised by the logged-in user.
- In the Agent-by-Team subcategory, Supervisors can select as report items only those teams for which the logged-in user is configured as a Supervisor.
- In the Agent-by-Skill Group subcategory, Supervisors can select as report items only those skill groups that include agents who are on teams that they supervise. However, the report will show all agents in the Skill Group, even agents who are not on the Supervisor's team.
- In the Agent-by-Peripheral subcategory, Supervisors can select as report items only those peripherals with which agents they supervise are associated. However, the report will show all agents under that peripheral, even agents who are not on the Supervisor's team.

WebView User Password Expiration and Domain Security Settings

WebView (ICM) users get their security setting from the domain on which they are created. The user’s password expiration date is enforced by the user’s domain, not by WebView. Therefore, the WebView administrator must be aware of the domain security policy setting on password expiration so that WebView users are not accidentally locked out of their accounts.

WebView users cannot change their password from within WebView. However, the WebView administrator can create and change WebView users passwords with the User List tool.

For additional information on the WebView password, see WebView User Unable to Change Password, page 11-14.
Logging into WebView

**Step 1** Open the browser window.

**Step 2** Enter the WebView URL: https://<webviewserver>/<instance>.

This login procedure assumes SSL is enabled. If you are not using SSL, you can enter http as the protocol identifier.

**Step 3** Press Enter.

**Step 4** At the prompt, enter your WebView user name and password.

**Note** Usernames are not case-sensitive. Passwords are.

If you have installed WebView correctly, the browser displays the opening WebView page.

### Supported Username Formats

You can login to WebView by entering the username in the following ways:

- `<domain><user>`
- `<domain>/<user>`
- User Principal Name (e.g. user@domain.com)
- \user (will default to the domain that the WebView server is associated with)
- /user (will default to the domain that the WebView server is associated with)
- user (will default to the domain that the WebView server is associated with)
Troubleshooting Your WebView Installation

The browser does open the WebView page, or you see the opening WebView page, but you cannot log in.

- Are you using a supported browser, per the Hardware and System Software Specification for Cisco ICM/IPCC Enterprise & Hosted Editions, Releases 7.0(0) and 7.1(x)?
- Did you use the correct the URL? If SSL is enabled, did you use the https protocol: https://<webviewserver>/<instance>.
- Did you enter the correct domain name, username, and password?
- Does the machine on which you have installed WebView conform to the requirements listed in the Hardware and System Software Specification for Cisco ICM/IPCC Enterprise & Hosted Editions, Releases 7.0(0) and 7.1(x)?
- Is the World Wide Web Publishing Service running?
- Is the Jaguar server running?
- Does the ServletExec log indicate errors? That log file is ServletExec.log.

You can log in to WebView, but you cannot see any agents/skills/etc when you create a report.

- Is the SQL Server database that hosts the awdb running?
- If you are running in a partitioned environment, does the logged-in user have permission to see the items they are requesting?
- Is there a temporary network error? One way to check this is to click the new Refresh Item List link.
- Does the Jaguar log indicate database permission errors. That log file is called Jaguar.log.

For more troubleshooting tips, see Chapter 11, “Troubleshooting Tips.”

Uninstalling WebView

Follow these steps to uninstall WebView if you do not administer a System IPCC deployment:

**Step 1** Select Start > Programs > ICM Admin Workstation > Setup.

**Step 2** At the Cisco ICM Setup screen:
- Select the Instance
- Select WebView
- Click Delete.

This removes WebView and the registry key for WebView.

**Step 3** Uninstall the WebView Third Party software as described in Uninstalling and Reinstalling the Third-Party Software, page 2-9.

To uninstall WebView in a System IPCC deployment:
Step 1  Uninstall IPCC software from your Administration & WebView Reporting machine as described in the *System IPCC Installation and Configuration Guide for Cisco IPCC Enterprise Edition*.

Step 2  Uninstall the WebView Third Party software as described in Uninstalling and Reinstalling the Third-Party Software, page 2-9.
P A R T  2

Administration
About WebView Users

WebView reporting users are:

- **Contact Center Administrators**, who are able to run any of the WebView reports to monitor contact center statistics at the enterprise level. Administrator accounts are created either by using the User List tool or by using Active Directory.

- **Contact Center Team Supervisors**, who are able to run Agent Team reports to review activity for their teams and only their teams.

Reporting users log in by entering the WebView URL from the browser on their client PCs or workstations (http://<webviewserver>/<instance>).

If SSL is enabled for the full session, reporting users must log in with a URL that begins with https and not with http. See About SSL, page 10-4.

Creating WebView Users

The preferred method to create WebView reporting users is by using Active Directory authentication and adding users to the WebView domain group.

There are three levels in the ICM/IPCC Active Directory hierarchy: Instance, Facility, and ICM Root. At each level, there is a WebView group.

In order to login to WebView with full access, a user must be a member of at least one of the following:

- the WebView group of the Instance
• the WebView group of the facility that contains the Instance
• the WebView group of the ICM Root

For more on how to use the Domain Manager Tool to add users to the WebView Domain Security Group, refer to the Domain Manager online help. Also see WebView User Authentication Model, page 10-2.

In a System IPCC Enterprise deployment, users are added using the web-based administration tool. Refer to the System IPCC Web Administration tool online help for more information.

ICM Configuration Manager User List

Prior to Release 7.0(0), users were added with the ICM Configuration Manager User List tool.

You can still use this tool to add users with restricted access, for example, to add ‘read-only’ access or to enforce feature control.

Also use the Configuration Manager to create WebView supervisors. (WebView supervisors are agents who are configured to run WebView reports for their agents, teams, and skill groups and to change configuration for their teams.)

Refer to the ICM Configuration Manager tool online help for further explanation.

WebView Supervisors

An individual who is created as a WebView user through Active Directory and who is also configured as a Supervisor though Configuration Manager will be treated as a Supervisor in WebView and will see restricted information in WebView reports.

Specifically, on Agent reports, a Supervisor can select as report items only those agents and agent teams that he or she has been configured to supervise:

• In the Agent-by-Agent subcategory, Supervisors can select as report items only those agents who are assigned to teams supervised by the logged-in user.
• In the Agent-by-Team subcategory, Supervisors can select as report items only those teams for which the logged-in user is configured as a Supervisor.
• In the Agent-by-Skill Group subcategory, Supervisors can select as report items only those skill groups that include agents who are on teams that they supervise. However, the report will show all agents in the Skill Group, even agents who are not on the Supervisor’s team.
• In the Agent-by-Peripheral subcategory, Supervisors can select as report items only those peripherals with which agents they supervise are associated. However, the report will show all agents under that peripheral, even agents who are not on the Supervisor’s team.

Supervisors can see, but cannot execute, other WebView reports. Supervisors who attempt to generate a report other than one listed above see an error message stating that they are not authorized to view the data.

Password Expiration and Domain Security Settings

WebView (ICM) users get their security setting from the domain on which they are created. The user’s password expiration date is enforced by the user’s domain, not by WebView. Therefore, the WebView administrator must be aware of the domain security policy setting on password expiration so that WebView users are not accidentally locked out of their accounts.
WebView users cannot change their password from within WebView. However, the WebView administrator can create and change WebView users passwords with the User List tool. For additional information on the WebView password, see **WebView User Unable to Change Password, page 11-14**.
Logging in to WebView

**Step 1**  Open the browser window.

**Step 2**  Enter the WebView URL: https://<webviewserver>/<instance>.

This login procedure assumes SSL is enabled. If you are not using SSL, you can enter http as the protocol identifier.

**Step 3**  Press Enter.

**Step 4**  At the prompt, enter your WebView user name and password.

---

**Note**  Usernames are not case-sensitive. Passwords are.

If you have installed WebView correctly, the browser displays the opening WebView page.

---

Supported Username Formats

You can login to WebView by entering the username in the following ways:

- `<domain><user>`
- `<domain>/<user>`
- User Principal Name (e.g. user@domain.com)
- `/user` (will default to the domain that the WebView server is associated with)
- `/user` (will default to the domain that the WebView server is associated with)
- `user` (will default to the domain that the WebView server is associated with)
After Logging In

Once logged in, reporting users can generate reports that display integrated information about various aspects of contact center operations.

**Real-time reports** offer up-to-the-minute data collected now and in the last five- and thirty-minute intervals.

**Historical reports** present contact center activity in selected half-hour or daily intervals.

The data sources for WebView reports are the real-time database (AWDB) and the Historical Database Server (HDS), which are created on the primary distributor Admin Workstation.

Favorite reports, saved report definitions, as well as scheduled report jobs, are stored in the WebView database (WVDB). This database is also located on the distributor Admin Workstation.

Report data is determined by the category and scope of the template the user selects and also by the items (for real time and historical templates) and the date range (for historical templates) that the user chooses when generating a report from the template.

WebView is installed with more than 200 Cisco-provided report templates, which are organized in categories. Users who require additional templates to meet specific analysis needs have the option to purchase, install, and integrate InfoMaker 10.x software from Sybase to create custom templates. Custom templates are typically modified versions of out-of-the-box WebView templates, with columns added or deleted and SQL queries added or revised. Refer to the *Template Design Guide Using InfoMaker for Cisco ICM/IPCC Enterprise & Hosted Editions* for the procedure to install and use InfoMaker to create custom templates.
The WebView Database

This chapter includes the following topics:

- About the WebView Database, page 5-2
- Location of the WebView Database, page 5-3
- WebView Database Deployment Models, page 5-4
- Working with a Second (Failover) WebView Database, page 5-6
- Redirecting the WebView Server to Another WebView Database, page 5-7
- About WebView Database Tables, page 4-12

For detailed information on database administration, see the *ICM Administration Guide for Cisco ICM Enterprise Edition*. 

The WebView database is used to store, update, maintain, and track saved report definitions, favorites, and scheduled report jobs:

- When you save a report definition, the template name, report items, scaling factor, and date/time range used to generate the report are stored in the WebView database.
  
  You can access and use saved reports in WebView only if they are stored in the WebView database.

- When you mark a report as a favorite, that user preference is stored with the report in the WebView database.

- When you update or delete a saved report definition or a scheduled report, that change is saved to the WebView database.

- When you schedule a report job, that report schedule with its parameters are stored in the WebView database.
  
  If you schedule a job to run once, the job is removed from the database after it has executed.
  
  If you schedule a recurring job, the job remains in the database, executing each day and time that you specified, until you delete the job in WebView.

The WebView database stores this data in four Microsoft SQL tables. These tables are described in About WebView Database Tables, page 4-12.

The WebView database is located on the distributor Admin Workstation and can be shared by a group of WebView servers, as configured during setup. See the next page for more on the location.
Location of the WebView Database

The WebView database must be located on a primary distributor Admin Workstation.

The option to create a WebView Database is a checkbox on the Real-time distributor Properties dialog box when you run ICM Setup to install a real-time distributor Admin Workstation.

With Release 7.0(0), you can now install one or more ‘standalone’ WebView server(s) on machine(s) separate from the Admin Workstation.

Regardless of how many WebView servers you set up, you typically configure them all to point to the same WebView database. You do this by entering the machine name for that AW as the location of the WebView database for each WebView Server installation. See Step 5 in the Installing Cisco ICM/IPCC Enterprise WebView Software, in Chapter 3.

In this way, all reporting users can access the same information about saved reports, favorites, and scheduled print jobs.

If you set up more than one distributor Admin Workstation, you have the option to create a second (failover) WebView database. If the primary WebView database is out of service, you can configure the WebView server(s) to point to the failover WebView database. See How to Redirect to a Failover WebView Database, page 4-11.
WebKit Database Deployment Models

Depending on the size and needs of the call center, you can deploy the WebKit server according to one of these deployment models:

- WebKit Database in a Standard Deployment, page 5-4
- WebKit Database in a Large-Customer Deployment, page 5-5

WebKit Database in a Standard Deployment

In the standard “all-in-one” deployment, the WebKit server, the WebKit database, and the real-time and historical databases co-reside on the distributor Admin Workstation.

During the distributor AW setup, when you are prompted for the location of the WebKit database, you indicate that the WebKit database is on that local machine.

Figure 5-1  WebKit Server and WebKit Database on Same Machine
WebView Database in a Large-Customer Deployment

The large-customer deployment, new with Release 7.0(0), supports installing WebView separately from the distributor Admin Workstation.

You can require multiple WebView servers initially, or you might start out with one and set up additional WebView servers as your enterprise grows.

If you have multiple WebView servers, during each WebView installation, when the Node Properties dialog box prompts for the WebView database host name, you enter the machine name of the distributor AW where the WebView database resides.

In this way, all reporting users can access the same favorites, shared reports, and scheduled report definitions from any of the servers.

**Note**
The WebView servers and the WebView database must be on the same release of WebView. If they are not, you see a WebView database error message. See WebView Database Messages, page 11-21.

---

**Figure 5-2**  Multiple WebView Servers Pointing to One WebView Database
Working with a Second (Failover) WebView Database

To allow users continued access to favorites and saved report definitions, you must install and maintain a copy of the WebView database. If the primary WebView database fails, you can redirect to the failover database without re-running ICM Setup.

Redirecting to the failover database is achieved by changing the ODBC DSN and can take about an hour. Reporting users can continue to work with WebView during that time but will not have access to favorites, shared reports, and scheduled report definitions until the switchover is complete.

If you choose to maintain a WebView database for use in a failover scenario, implement a regular backup schedule to ensure that it is current and contains the same favorites and shared reports as the primary WebView database.

*Figure 5-3  Redirecting to a Failover WebView Database*
Creating a Second (or Failover) WebView Database

Step 1  Install a second ICM AW. If you have already installed a second AW, run ICM Setup, select that AW and click **Edit**.

Step 2  In the Real-time Distributor Properties dialog box, select **WebView Database**.

Step 3  Click **Next** and proceed with the setup. When the installation is complete, and you are prompted to do so, exit from Setup.

**Note** You need to implement the backup/restore procedure to make sure that the backup database is kept up with current data.

Redirecting the WebView Server to Another WebView Database

This section explains how to redirect the WebView server(s) when the location of the WebView database changes; for example, if the WebView database is moved to a different server or if you need to point to a backed-up, failover WebView database.

Redirecting the WebView server to a second WebView database can take up to an hour. During this time, reporting users can use WebView but are unable to access favorites, shared reports, or scheduled report definitions.

Reports that were scheduled to run while the WebView server is being redirected will fail.

After the WebView server has been redirected, favorites, shared reports, and scheduled reports are available, provided that they are part of the backup database.

**Note** Use Active Directory tools to verify that the Jaguar server account has rights to the new WebView database.
Redirect to a Failover WebView Database

Log in as administrator on the WebView server, and follow the steps below:

Step 1  Click Start > Programs > Administrative Tools > Data Sources (ODBC).
Step 2  Click the System DSN tab.
Step 3  Select wvdb ODBC DSN (<instancename>WVDB_wv) and click Configure.
Step 4  Change the server name and click Apply.
Step 5  Test WebView to verify the access to the new WebView database.

WebView Database Tables

The WebView database consists of four database tables. The sections that follow describe the structure of these database tables:

- The WebViewVersion Table, page 4-12
- The Print Jobs Table, page 4-13
- The Report Table, page 4-15
- The User Preferences Table, page 4-17

The WebViewVersion Table

This table is used by WebView software for version checking of the WebView database. It describes the current schema of the database and shows the schema history.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Type</th>
<th>Allow Nulls</th>
<th>Constraint/Index Database Table Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebViewVersion</td>
<td>Real</td>
<td>No</td>
<td>Primary Key</td>
<td>The version of WebView database</td>
</tr>
<tr>
<td>LastUpdateDate</td>
<td>DateTime</td>
<td>No</td>
<td>Primary Key</td>
<td>The date and time that the database was last created or upgraded</td>
</tr>
</tbody>
</table>
The Print Jobs Table

This table contains one record for each scheduled print job (print and save to file). The table refers to the Report table for report parameters.

**Table 5-2 Print Jobs Table**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Constraint/Index Database Table Header</th>
<th>Data Types in ICM/IPCC databases</th>
<th>Allow Nulls</th>
</tr>
</thead>
<tbody>
<tr>
<td>JobTrackID</td>
<td>A unique ID to track the print job</td>
<td>Primary Key</td>
<td>char(50)</td>
<td>No</td>
</tr>
<tr>
<td>Frequency</td>
<td>The number of times the print job is to be run</td>
<td></td>
<td>char(1)</td>
<td>No</td>
</tr>
<tr>
<td>TokenValue</td>
<td>A random number generated from the value of the job ID</td>
<td></td>
<td>char(260)</td>
<td>No</td>
</tr>
<tr>
<td>JobTime</td>
<td>The time the print job is to be run</td>
<td></td>
<td>char(260)</td>
<td>No</td>
</tr>
<tr>
<td>Command</td>
<td>The command-line string that schedules the print job</td>
<td></td>
<td>char(1000)</td>
<td>No</td>
</tr>
<tr>
<td>ReportID</td>
<td>The unique ID identifying the report to be printed</td>
<td>int</td>
<td>int</td>
<td>No</td>
</tr>
<tr>
<td>DayDates</td>
<td>The day(s) and date(s) on which the report is to be printed</td>
<td></td>
<td>char(1000)</td>
<td>Yes</td>
</tr>
<tr>
<td>ClientJobID</td>
<td>The ID number of the job on the WebView client computer where the print job is created</td>
<td>int</td>
<td>int</td>
<td>Yes</td>
</tr>
<tr>
<td>ClientHost</td>
<td>The name of the WebView host computer from which the print job is printed</td>
<td>char(260)</td>
<td>char(260)</td>
<td>Yes</td>
</tr>
<tr>
<td>PrintCount</td>
<td>The number of print jobs</td>
<td>int</td>
<td>int</td>
<td>No</td>
</tr>
<tr>
<td>ServerPrint</td>
<td>The server from which the job is printed</td>
<td>int</td>
<td>int</td>
<td>No</td>
</tr>
<tr>
<td>Printer</td>
<td>The name of the printer selected to do the print job</td>
<td>char(260)</td>
<td>char(260)</td>
<td>Yes</td>
</tr>
<tr>
<td>FileLocation</td>
<td>The location of the file to be printed</td>
<td>char(260)</td>
<td>char(260)</td>
<td>Yes</td>
</tr>
<tr>
<td>SaveFileName</td>
<td>The file name of the print job</td>
<td>char(260)</td>
<td>char(260)</td>
<td>Yes</td>
</tr>
<tr>
<td>OwnerID</td>
<td>The person who created the print job</td>
<td>int</td>
<td>int</td>
<td>Yes</td>
</tr>
<tr>
<td>Instance</td>
<td>The ICM instance where the print job is created</td>
<td>char(260)</td>
<td>char(260)</td>
<td>No</td>
</tr>
<tr>
<td>ClientIP</td>
<td>The IP address of the computer on which the print job is created.</td>
<td>char(16)</td>
<td>char(16)</td>
<td>Yes</td>
</tr>
<tr>
<td>FileFormat</td>
<td>The format of the report to be printed. For example: HTML, PDF, or XLS</td>
<td>char(10)</td>
<td>char(10)</td>
<td>Yes</td>
</tr>
<tr>
<td>PrinterPort</td>
<td>The port number to which the printer, selected for the print job, is connected</td>
<td>char(10)</td>
<td>char(10)</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table 5-2  Print Jobs Table (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Constraint/Index Database Table Header</th>
<th>Data Types in ICM/IPCC databases</th>
<th>Allow Nulls</th>
</tr>
</thead>
<tbody>
<tr>
<td>PrinterDriver</td>
<td>The print driver on the printer selected to do the print job</td>
<td>char(260)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>PrinterName</td>
<td>The name of the printer doing the print job</td>
<td>char(260)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>PrintLocation</td>
<td>The location of the printer selected for the print job</td>
<td>char(260)</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>PDF_Is_Portrait</td>
<td>Attribute that specifies the orientation used when printing a report in PDF format</td>
<td>bit</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>PDF_PaperSize</td>
<td>Attribute that specifies the paper size used when printing a report in PDF format</td>
<td>smallInt</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>FileNameAppend Date</td>
<td>Attribute, necessary when saving a report, that specifies whether a new file name is generated with the filename plus report creation date or a default name is used</td>
<td>Default 0</td>
<td>bit</td>
<td>Yes</td>
</tr>
<tr>
<td>UserGuid</td>
<td>Unique identifier of the user who scheduled the print job</td>
<td>varchar(64)</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
### The Report Table

This table contains one record for each saved report. It holds report parameters such as items selected and thresholds. The User Preferences and Print Jobs tables refer to reports stored in this table.

**Table 5-3 Report Table**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Constraint/Index Database Table Header</th>
<th>Data Types in ICM/IPCC databases</th>
<th>Allow Nulls</th>
</tr>
</thead>
<tbody>
<tr>
<td>ReportID</td>
<td>The unique ID of the saved report</td>
<td>Primary Key</td>
<td>int</td>
<td>No</td>
</tr>
<tr>
<td>Instance</td>
<td>The ICM instance on which the report data is created</td>
<td>char(10)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>OwnerID</td>
<td>This is a pre-7.0 field that is retained for upgrade from 5.0/6.0 to 7.0. For 7.x software, and after an upgrade to 7.x, this field in no longer used.</td>
<td>int</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>CustomerID</td>
<td>The unique ID of the company to which the report creator belongs</td>
<td>int</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>The name of the saved report</td>
<td>char(260)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>An optional user-entered description of the report</td>
<td>text</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>IsPublic</td>
<td>Whether or not the report is shared or private</td>
<td>bit</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>IsRealTime</td>
<td>Whether or not the report is real-time or historical</td>
<td>bit</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>The report category</td>
<td>char(260)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>Table or graph</td>
<td>char(1)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Template</td>
<td>The name of the template from which the report was created</td>
<td>char(260)</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>ItemsSelected</td>
<td>The items selected in the report to be reported on</td>
<td>text</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>StartDateTime</td>
<td>If selected in the report, the beginning date and time for the report data</td>
<td>datetime</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>EndDateTime</td>
<td>If selected in the report, the end date and time for the report data</td>
<td>datetime</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>RelativeDataType</td>
<td>If selected in the report, the relative date and time range for the report data, relative to the day the report is run; for example: Today or Next Week</td>
<td>SmallInt</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Table 5-3  Report Table (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Constraint/Index Database Table Header</th>
<th>Data Types in ICM/IPCC databases</th>
<th>Allow Nulls</th>
</tr>
</thead>
<tbody>
<tr>
<td>DrillDownTemplate</td>
<td>The name of the report template assigned to a parent report component. Drill-down reports display filtered versions of the parent report data</td>
<td></td>
<td>char(260)</td>
<td>Yes</td>
</tr>
<tr>
<td>DrillDownCategory</td>
<td>The category of drill-down template</td>
<td></td>
<td>char(260)</td>
<td>Yes</td>
</tr>
<tr>
<td>Thresholds</td>
<td>The threshold or list of thresholds set in the report</td>
<td></td>
<td>text</td>
<td>Yes</td>
</tr>
<tr>
<td>RefreshRate</td>
<td>The rate in seconds at which to refresh a real-time report</td>
<td></td>
<td>int</td>
<td>Yes</td>
</tr>
<tr>
<td>Scale</td>
<td>Attribute that specifies the scale to show a report, in %</td>
<td>Default 100</td>
<td>smallInt</td>
<td>Yes</td>
</tr>
<tr>
<td>UserGuid</td>
<td>The unique ID of the user who saved the report</td>
<td></td>
<td>varchar(64)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The User Preferences Table

This table contains one record for each favorite saved by each user.

Table 5-4  User Preferences Table

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Constraint/Index Database Table Header</th>
<th>Data Types in ICM/IPCC databases</th>
<th>Allow Nulls</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserGuid</td>
<td>The unique ID of the person who designated the report as a favorite</td>
<td>Primary Key</td>
<td>varchar(64)</td>
<td>Yes</td>
</tr>
<tr>
<td>ReportID</td>
<td>The unique ID of the saved report</td>
<td>Primary Key</td>
<td>int</td>
<td>No</td>
</tr>
</tbody>
</table>
Jaguar Administration and the Jaguar Watchdog

This chapter includes the following topics that pertain to Jaguar Administration and to the Jaguar Watchdog:

- Jaguar Administration, page 6-1
  - Changing the Jaguar Admin Password, page 6-1
  - Setting the Size of the Jaguar Log File, page 6-3
  - Deleting Jaguar Log Files, page 6-3
- The Jaguar Watchdog, page 6-5
  - Jaguar Watchdog Properties, page 6-5
  - Executing a Batch File after Jaguar Restarts, page 6-6
  - About Jaguar Watchdog Logging, page 6-7

Jaguar Administration

Jaguar—also known as EAServer and Enterprise Application Server—is one of the applications installed from the ICM Third-Party Tools CD. Among the functions of the Jaguar Server are to generate reports and to query the database.

Changing the Jaguar Admin Password

After installing Jaguar, the administrator might want to change the default Jaguar Admin password. Although it is not a requirement to do so, changing the Jaguar Admin password is a precaution to prevent unauthorized persons from connecting to the Jaguar service and passing commands that might potentially compromise the server.

How to change the Jaguar Admin password

1. In the Start menu, select Programs > Sybase > EAServer 5.1.0 > EAServer Manager. This opens the Sybase Central dialog box.
2. In the Tools menu of the Sybase Central dialog box, select Connect > EAServer Manager. This opens the Login dialog box.
3. In the Login dialog box, click Connect. If you do not see a message, continue to Step 4.
If you see a message saying the User Name field is empty:

a. Enter jagadmin in the User Name text box.

b. Enter <your machine name> in the Host Name text box.

Note A previous version of Jaguar required you to enter localhost. This version requires you to enter your machine name. To find your machine name, right-click My Computer on your desktop and select Properties from the pop-up menu. Select the Network Identification tab to see your machine name.

c. Retain the default (9000) in the Port Number text box.

d. Click Connect.

Step 4 From the directory tree in the Sybase Central dialog box, select EAServer Manager > Servers > Jaguar.

Step 5 In the menu bar, select File > Properties.

Step 6 In the Server Properties:Jaguar dialog box, select the Security tab.

Step 7 In the Administration box, click Set jagadmin Password.

Step 8 In the Administrator Password dialog box, enter the password in the New jagadmin Password text box. Then re-enter it in the Verify text box.

Step 9 Click OK repeatedly to close the dialog boxes. Select File > Exit from the menu bar to close the Sybase Central dialog box.

Note This procedure changes the password. The procedure below is also necessary so that WebView recognizes the new password.

How to configure the WebView jagconnections.properties file with the new Jaguar Admin password

Step 1 In a text editor, open the file %Jaguar%/html/classes/com/cisco/atg/jagconnection.properties where %Jaguar% is the system variable pointing to the directory location of the Jaguar (EAServer) files.

Step 2 After JAGCONNECT_JAGUAR_ADMIN_PWD=, enter your new password as shown in this example jagconnection.properties File:

```
JAGCONNECT_CORBA_ORB_CLASS=com.sybase.CORBA.ORB
JAGCONNECT_JAGUAR_SERVER=
JAGCONNECT_IIOP_PORT=9000
JAGCONNECT_JAGUAR_ADMIN=jagadmin
JAGCONNECT_JAGUAR_ADMIN_PWD=newpassword
JAGCONNECT_JAGUAR_SYS_BEAN=webview/n_lcmsysinfo
JAGCONNECT_JAGUAR_DW_BEAN=webview/n_lcmdw
```

Step 3 Save the jagconnection.properties file.

The password will be encrypted by WebView the first time it is used.
### Setting the Size of the Jaguar Log File

Jaguar software writes to a log file as it processes information. The default maximum size for the log file is 10 Megabytes. When the log reaches that size, it is zipped and moved to a `logarchives` subfolder and a date/timestamp is appended to the filename.

To change the default maximum log size, use the following procedure.

**How to set the size of the Jaguar log file**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Start menu, select Programs &gt; Sybase &gt; EAServer 5.1.0 &gt; EAServer Manager. This opens the Sybase Central dialog box.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Tools menu of the Sybase Central dialog box, select Connect &gt; EAServer Manager. This opens the Login dialog box.</td>
</tr>
</tbody>
</table>
| Step 3 | In the Login dialog box:  
  a. Enter `jagadmin` in the User Name text box.  
  b. Enter `<your_machine_name>` in the Host Name text box.  
  c. You can leave the default (9000) in the Port Number text box.  
  d. Click Connect.  |
| Step 4 | In the directory tree box of the Sybase Central dialog box, expand EAServer Manager and then Log Profiles > prod > Handlers. |
| Step 5 | In the right pane, right-click the eas handler and choose Properties. |
| Step 6 | On the Type tab, change the Max size value from the default (10m) to the size you want (for example, 50m). |
| Step 7 | Click OK to exit out of the EAServer Manager. |

### Deleting Jaguar Log Files

Once you set the log file size, Jaguar creates a new log file each time the data grows beyond that size. Consequently, you can have many log files in the Jaguar directory. Delete old log files occasionally to keep them from consuming too much space on your system.

**How to delete Jaguar Log files**

| Step 1 | Go to the Jaguar root directory where they are stored. The default location for this directory is `%JAGUAR%\bin\logarchives` where `%JAGUAR%` is an environment variable defined in windows. |
| Step 2 | Select the outdated log files and delete them. |

### Troubleshooting Jaguar

See these sections in Chapter 11, “Troubleshooting Tips”: 

---

*WebView Installation and Administration Guide for Cisco Enterprise & Hosted Editions, Release 7.0(0)*

![Page number: 6-3]
- EAServer/Jaguar Installation Fails, page 11-7
- Jaguar Server Connection Fails After Restart, page 11-9
- Jaguar Service Verification, page 11-9
The Jaguar Watchdog

The Jaguar Watchdog is a new utility introduced in WebView Release 7.0(0).
It is installed to the `<ICMRoot>\web\webview\watchdog` directory and is enabled automatically when you install WebView Reporting from ICM Setup.
The Jaguar Watchdog runs as a service of the operating system and monitors the Jaguar service whether or not reporting users are logged in to WebView.
Its function is to continuously test the operation of the Jaguar service and to restart the service if it fails to respond.
The WatchDog can be configured to run a batch file to perform custom actions (such as memory dump and log gathering) before restarting.
No action is required on the part of the reporting user.

Jaguar Watchdog Properties

Editable properties have been added to the adminui.properties file for the Jaguar Watchdog configuration.
The location of the adminui.properties file is:
`<ICMRoot>\web\webview\reporting\servlet\properties\adminui.properties`
For more on these properties, see Jaguar WatchDog, page 9-5.
Executing a Batch File after Jaguar Restarts

Jaguar Watchdog is configured to execute a batch file after Jaguar restarts.

Calling a batch file enables you to code the execution of any tasks you might want to run, such as emailing an administrator about the restart, and to manage the way EAServer is restarted.

If you choose to execute some tasks before EAServer is restarted (such as a Windows userdump), you can disable the EAServer auto-restart and restart Jaguar from the batch file itself.

The batch file that is installed and configured by default (C:\icm\web\webview\watchdog\jaghook.bat) is shown below. This file serves as an example and has the Jaguar restart code commented out.

```bash
REM echo Time: > restart.log
REM time /t >> restart.log
REM echo Date: >> restart.log
REM date /t >> restart.log
REM echo -------- > restart.log
REM echo Calling Shutdown >> restart.log
REM call jagtool shutdown >> restart.log
REM echo Sleeping .... >> restart.log
REM sleep 10 > nul
REM echo Waking up .... >> restart.log
REM net start Jaguar >> restart.log
```
About Jaguar Watchdog Logging

Be default, there are five Watchdog log files, each with a maximum size of 5 megabytes. These files are located in the same directory as the Jaguar Watchdog application (<ICMRoot>\web\webview\watchdog).

The files are named WatchDog.0.log, WatchDog.1.log ... WatchDog.4.log. WatchDog0.log is the most current, and WatchDog4.log is the oldest.

Both the number of log files and the maximum size are configurable.

When WatchDog.0.log grows to 5 megabytes, it is renamed WatchDog.1.log, and a new WatchDog.0.log is created. The numbers for all the other logs increase by one, and the oldest log (WatchDog.4.log) is deleted. With this mechanism, there will never be more than five logs, and WatchDog.0.log is always the most recent.
CHAPTER 7

Time and Date in Reports

To correctly interpret the data in WebView reports, reporting users must be aware of the date formats and of the time values and the time zones on which those values are based.

This chapter includes the following information:
- Date and Time Formats in WebView Reports, page 7-1
- Time Zone Values for Report Viewing, page 7-1
- Central Controller Time Zone and Reporting Data, page 7-2
- Checking WebView AW Time Synchronization, page 7-2
- Time and Time Zones Dependencies, page 7-3
- How Date Formats are Set, page 7-3
- Dates and Date Ranges in Mixed-Language Installations, page 7-5
- List of International Date Formats, page 7-6

Date and Time Formats in WebView Reports

When a report is generated in WebView, DateTime values appear in three places:
- In the report header stating the datetime range that an historical report covers.
- In the report data.
- In the report footer specifying when the report was run.

Time Zone Values for Report Viewing

To correctly view and understand a report, reporting users must be aware of the three possible time zones, which are:
- Their own time zone
- The time zone of the AW from which the WebView server receives data
- The time zone of the Central Controller
Central Controller Time Zone and Reporting Data

In ICM/IPCC Enterprise, data is produced by the PGs and NICs, which communicate with the Central Controller.

When the data is written to the Central Controller database by the Logger or to the real-time or the historical database by the distributor AW, all date and time values are converted to the Central Controller time zone.

Thus, all data in the database is in terms of the Central Controller time zone.

Note: Since all of the data in the database is written in Central Controller local time, all reporting done in WebView must be with respect to Central Controller time. For example, when a user selects a date and time range for an historical report, the user must enter the data with respect to the Central Controller’s time zone.

Checking WebView AW Time Synchronization

Make sure that the time on the distributor AW server is synchronized with the time on the ICM Central Controller:

- If the AW is in the same domain as the Central Controller, then the time will automatically be synchronized. However, make sure that the Windows Time Service is enabled on the AW.
- If the AW is in a different domain from that of the ICM Central Controller, then you can also use the NET TIME command to synchronize the time.

For example: net time /domain:boston

If the time on the AW is not synchronized with the time on the Central Controller, then report execution time will not be synchronized with the data in the report.

For example, if the AW time lags behind the Central Controller time by 2 minutes and a report is executed at 10:00 AM on the WebView server, then the report execution time on the WebView report would be 10:00 AM, but the report data could have a time of 10:02 AM.

Note: Do not use ICM synchronization (not available on the AW but available on the CallRouter and the PG).

By default, the Disable ICM Time Synchronization box is selected in ICM Setup (in the MDS & DMP Properties dialog box, which appears when you select the advanced settings for the peripheral gateway component). Refer to the ICM Installation Guide for Cisco ICM Enterprise Edition for more information.

Time Zone Field

In many database tables that have a DateTime field, there is also a TimeZone field.

The TimeZone field is the time zone of the Central Controller when the record was written. It tells the offset of Central Controller time from GMT.
This field is used for the daylight savings time adjustment so that the Logger does not write duplicate keys in the database when the time “falls back” (that is, when time rolls back an hour for US daylight saving time in the fall). The time zone of the PG or NIC that generated the data is not recorded in the database.

**Time and Time Zones Dependencies**

The table below shows the time synchronization and time zone dependencies among the various components in the reporting system relative to the Router, which the ICM/IPCC system assumes to have the correct time.

<table>
<thead>
<tr>
<th>Component</th>
<th>Time Synchronized with Router</th>
<th>Time Zone Synchronized with Router</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Logger</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PG/NIC</td>
<td>Yes</td>
<td>Not necessarily</td>
</tr>
<tr>
<td>AW</td>
<td>Not necessarily</td>
<td>Not necessarily</td>
</tr>
<tr>
<td>WebView Client</td>
<td>Not necessarily</td>
<td>Not necessarily</td>
</tr>
</tbody>
</table>

In Table 7-1, *Not Necessarily* means although the ICM/IPCC components might be time synchronized or time zone synchronized with the Router, there is no enforcement of this policy, nor is it reasonable to assume that your system is automatically set up this way.

For a detailed explanation of how ICM software handles time synchronization, see the *ICM Administration Guide for Cisco ICM Enterprise Edition* available on the Cisco web site in the Documentation section of the Cisco Customer Contact software web page.

The PG or NIC is not required to be in the same time zone as the Central Controller. However all time that flows between the PG or NIC and the Router is in GMT (Greenwich Mean Time) and thus time zones do not matter.

The Router, Logger, PG, and NIC need to be time synchronized in order for routing to happen correctly. However, the WebView server and the WebView client can be off by several minutes, and the reports will still make intuitive sense to the reporting user.

**How Date Formats are Set**

WebView sets date format in reports according to the language setting in the Internet Explorer browser. WebView supports nine languages on the server and can support the date formats of the locales listed in Table 7-2.

If WebView does not detect any of these languages, it defaults to US-English (mm/dd/yyyy) format.

The languages appearing in the Internet Explorer language list are actually locales; that is, a combination of ISO-639 language code and ISO-3166 country code.

The mappings between locales and date formats are defined in the file, wvLocale.properties, in the form of: `<locale>==<date format>`

For example: De=DD/MM/YYYY
WebView supports multiple locales. The mapping between the locales and the associated date formats is shown in Table 7-2 on page 7-6.

To set the language/locale in Internet Explorer, follow these steps:

---

**Step 1**  Select **Tools > Internet Options** from the browser menu.

**Step 2**  Click the Languages button on the General tab.

**Step 3**  Click **Add** and select a language.

**Step 4**  Click the **Move Up** button to order the priority of the languages.

**Note**  WebView uses the highest priority language for the date format.

**Step 5**  Click **OK** twice to exit.

---
Dates and Date Ranges in Mixed-Language Installations

Although WebView maps the language settings from the client web browser to an appropriate date format, the Date Time range under the report title always displays in the format used by the WebView server.

**Important:** In all cases, the Internet Explorer locale at the WebView Client must use the same date format as the locale at the WebView Server. For example, if the WebView Server has the US English locale (with the format MM/DD/YYYY), then the WebView Client must also use a browser locale with the MM/DD/YYYY format.

In addition, a WebView Client can employ Microsoft Windows and Internet Explorer localized in a language that meets one of these two criteria:

1. The WebView Server that it connects to uses English Microsoft Windows. For example, a Russian WebView Client may connect to an English Windows Webview Server.
2. The WebView Server that it connects to uses a language for Microsoft Windows that is included in the same native character set as the WebView Client’s Microsoft Windows language. (Character set corresponds to SQL Server Collation indicator above.) For example, an Italian WebView Client may connect to a German Windows WebView Server because both Italian and German are included in the Latin1 character set.

Refer to Table 7-2 for a list of all locales and date formats.
List of International Date Formats

The languages appearing in the IE language list are actually locales, a combination of ISO-639 language code and ISO-3166 country code.

The mapping between locales and date formats is defined in \
\icm\web\webview\reporting\servlet\wvLocale.properties, in the form of: <locale =<date format>

For example, de=DD/MM/YY

Table 7-2 list the locales that WebView supports and shows the mapping between the locales and the date formats.

<table>
<thead>
<tr>
<th>Locales</th>
<th>Date Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Be</td>
<td>DD/MM/YY</td>
<td>Byelorussian</td>
</tr>
<tr>
<td>Ca</td>
<td>DD/MM/YY</td>
<td>Catalan</td>
</tr>
<tr>
<td>Cs</td>
<td>DD/MM/YY</td>
<td>Czech</td>
</tr>
<tr>
<td>Da</td>
<td>DD/MM/YY</td>
<td>Danish</td>
</tr>
<tr>
<td>De</td>
<td>DD/MM/YY</td>
<td>German</td>
</tr>
<tr>
<td>de_AT</td>
<td>DD/MM/YY</td>
<td>German (Austria)</td>
</tr>
<tr>
<td>de_CH</td>
<td>DD/MM/YY</td>
<td>German (Switzerland)</td>
</tr>
<tr>
<td>de_LU</td>
<td>DD/MM/YY</td>
<td>German (Luxembourg)</td>
</tr>
<tr>
<td>El</td>
<td>DD/MM/YY</td>
<td>Greek</td>
</tr>
<tr>
<td>en</td>
<td>MM/DD/YY</td>
<td>English</td>
</tr>
<tr>
<td>en_AU</td>
<td>DD/MM/YY</td>
<td>English (Australia)</td>
</tr>
<tr>
<td>en_CA</td>
<td>DD/MM/YY</td>
<td>English (Canada)</td>
</tr>
<tr>
<td>en_GB</td>
<td>DD/MM/YY</td>
<td>English (United Kingdom)</td>
</tr>
<tr>
<td>en_IE</td>
<td>DD/MM/YY</td>
<td>English (Ireland)</td>
</tr>
<tr>
<td>en_NZ</td>
<td>DD/MM/YY</td>
<td>English (New Zealand)</td>
</tr>
<tr>
<td>en_US</td>
<td>MM/DD/YY</td>
<td>English (United States)</td>
</tr>
<tr>
<td>en_ZA</td>
<td>YY/MM/DD</td>
<td>English (South Africa)</td>
</tr>
<tr>
<td>es</td>
<td>DD/MM/YY</td>
<td>Spanish</td>
</tr>
<tr>
<td>es_AR</td>
<td>DD/MM/YY</td>
<td>Spanish (Argentina)</td>
</tr>
<tr>
<td>es_BO</td>
<td>DD/MM/YY</td>
<td>Spanish (Bolivia)</td>
</tr>
<tr>
<td>es_CL</td>
<td>DD/MM/YY</td>
<td>Spanish (Chile)</td>
</tr>
<tr>
<td>es_CO</td>
<td>DD/MM/YY</td>
<td>Spanish (Colombia)</td>
</tr>
<tr>
<td>es_CR</td>
<td>DD/MM/YY</td>
<td>Spanish (Costa Rica)</td>
</tr>
<tr>
<td>es_DO</td>
<td>MM/DD/YY</td>
<td>Spanish (Dominican Republic)</td>
</tr>
<tr>
<td>es_EC</td>
<td>DD/MM/YY</td>
<td>Spanish (Ecuador)</td>
</tr>
<tr>
<td>es_ES</td>
<td>DD/MM/YY</td>
<td>Spanish (Spain)</td>
</tr>
<tr>
<td>es_GT</td>
<td>DD/MM/YY</td>
<td>Spanish (Guatemala)</td>
</tr>
<tr>
<td>Locales</td>
<td>Date Format</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>es_HN</td>
<td>MM/DD/YY</td>
<td>Spanish (Honduras)</td>
</tr>
<tr>
<td>es_MX</td>
<td>DD/MM/YY</td>
<td>Spanish (Mexico)</td>
</tr>
<tr>
<td>es_NI</td>
<td>MM/DD/YY</td>
<td>Spanish (Nicaragua)</td>
</tr>
<tr>
<td>es_PA</td>
<td>MM/DD/YY</td>
<td>Spanish (Panama)</td>
</tr>
<tr>
<td>es_PE</td>
<td>DD/MM/YY</td>
<td>Spanish (Peru)</td>
</tr>
<tr>
<td>es_PR</td>
<td>MM/DD/YY</td>
<td>Spanish (Puerto Rico)</td>
</tr>
<tr>
<td>es_PY</td>
<td>DD/MM/YY</td>
<td>Spanish (Paraguay)</td>
</tr>
<tr>
<td>es_SV</td>
<td>MM/DD/YY</td>
<td>Spanish (El Salvador)</td>
</tr>
<tr>
<td>es_UY</td>
<td>DD/MM/YY</td>
<td>Spanish (Uruguay)</td>
</tr>
<tr>
<td>es_VE</td>
<td>DD/MM/YY</td>
<td>Spanish (Venezuela)</td>
</tr>
<tr>
<td>fi</td>
<td>DD/MM/YY</td>
<td>Finnish</td>
</tr>
<tr>
<td>fr</td>
<td>DD/MM/YY</td>
<td>French</td>
</tr>
<tr>
<td>fr_BE</td>
<td>DD/MM/YY</td>
<td>French (Belgium)</td>
</tr>
<tr>
<td>fr_CA</td>
<td>YY/MM/DD</td>
<td>French (Canada)</td>
</tr>
<tr>
<td>fr_CH</td>
<td>DD/MM/YY</td>
<td>French (Switzerland)</td>
</tr>
<tr>
<td>fr_LU</td>
<td>DD/MM/YY</td>
<td>French (Luxembourg)</td>
</tr>
<tr>
<td>hr</td>
<td>YY/MM/DD</td>
<td>Croatian</td>
</tr>
<tr>
<td>hu</td>
<td>YY/MM/DD</td>
<td>Hungarian</td>
</tr>
<tr>
<td>is</td>
<td>DD/MM/YY</td>
<td>Icelandic</td>
</tr>
<tr>
<td>it</td>
<td>DD/MM/YY</td>
<td>Italian</td>
</tr>
<tr>
<td>it_CH</td>
<td>DD/MM/YY</td>
<td>Italian (Switzerland)</td>
</tr>
<tr>
<td>ja</td>
<td>YY/MM/DD</td>
<td>Japanese</td>
</tr>
<tr>
<td>ko</td>
<td>YY/MM/DD</td>
<td>Korean</td>
</tr>
<tr>
<td>nl</td>
<td>DD/MM/YY</td>
<td>Dutch</td>
</tr>
<tr>
<td>nl_BE</td>
<td>DD/MM/YY</td>
<td>Dutch (Belgium)</td>
</tr>
<tr>
<td>no</td>
<td>DD/MM/YY</td>
<td>Norwegian</td>
</tr>
<tr>
<td>pl</td>
<td>YY/MM/DD</td>
<td>Polish</td>
</tr>
<tr>
<td>pt</td>
<td>DD/MM/YY</td>
<td>Portuguese</td>
</tr>
<tr>
<td>pt_BR</td>
<td>DD/MM/YY</td>
<td>Portuguese (Brazil)</td>
</tr>
<tr>
<td>ro</td>
<td>DD/MM/YY</td>
<td>Romanian</td>
</tr>
<tr>
<td>ru</td>
<td>DD/MM/YY</td>
<td>Russian</td>
</tr>
<tr>
<td>sk</td>
<td>DD/MM/YY</td>
<td>Slovak</td>
</tr>
<tr>
<td>sl</td>
<td>YY/MM/DD</td>
<td>Slovenian</td>
</tr>
<tr>
<td>sq</td>
<td>YY/MM/DD</td>
<td>Albanian</td>
</tr>
<tr>
<td>sr</td>
<td>YY/MM/DD</td>
<td>Serbian</td>
</tr>
<tr>
<td>sv</td>
<td>MM/DD/YY</td>
<td>Swedish</td>
</tr>
<tr>
<td>tr</td>
<td>DD/MM/YY</td>
<td>Turkish</td>
</tr>
</tbody>
</table>
### List of International Date Formats

<table>
<thead>
<tr>
<th>Locales</th>
<th>Date Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>uk</td>
<td>DD/MM/YY</td>
<td>Ukrainian</td>
</tr>
<tr>
<td>zh</td>
<td>YY/MM/DD</td>
<td>Chinese</td>
</tr>
<tr>
<td>zh_CN</td>
<td>YY/MM/DD</td>
<td>Chinese (China)</td>
</tr>
<tr>
<td>zh_HK</td>
<td>YY/MM/DD</td>
<td>Chinese (Hong Kong)</td>
</tr>
<tr>
<td>zh_TW</td>
<td>YY/MM/DD</td>
<td>Chinese (Taiwan)</td>
</tr>
</tbody>
</table>
Template Maintenance

This chapter contains the following topics:

- About Templates, page 8-1
- Caching Templates and Items, page 8-3
  - Refreshing the Cache, page 8-3
  - Configuring Caching, page 8-3
- How to Run PATCHPBL to Update or Fix Templates, page 8-6

About Templates

Templates provide the SQL queries, the format, the columns, the headers, the default and dynamic sorting, and the groupings of data that can appear in the report.

The reporting user selects a template and specifies the items and (for historical reports) the date range to qualify the content that appears when a report is generated from the template.
How Templates are Organized

More than 200 Cisco-provided templates are available with WebView. Templates are stored in `icm\<icm_instance_name>\aw\custom`.

They are organized in subdirectories within custom—one subdirectory for each report category. Each report-category directory contains:

- A file named `PPB050.PBL`
  
  This is the PowerBuilder Library file that contains all templates, Cisco-provided and custom, within that report category. Each report-category folder has its own `PPB050.PBL` file.

- One or more files with the extension of `.SRD`
  
  These are the individual template files and are for Cisco templates only (and not for custom templates).

- A file named `srodelist.txt`
  
  This is the list of all template files in the report-category library (in the `PPB050.PBL`).

Cisco Templates and Custom Templates

Cisco templates are installed when you run WebView Reporting from ICM Setup.

Custom templates are templates created using Sybase InfoMaker.

Refer to Template Design Guide Using InfoMaker for Cisco ICM/IPCC Enterprise & Hosted Editions for more on custom templates.
Caching Templates and Items

Refreshing the Cache

The WebView interface now provides a way for reporting users to apply an immediate refresh for the list of templates and for the list of items.

The templates page and the items page both have a link to Refresh List, allowing reporting users to see updated values immediately. This refresh-on-demand does not require you to restart IIS Admin Services or to log out users. When the cache is refreshed, all users who are logged in can see the new templates and items.

See the WebView online help for more information.

Configuring Caching

By default, caching is enabled for report templates and report items. The time interval after which the cache refreshes is also set by default, as is the interval after which the cache is purged.

Caching improves system performance by reducing the number of times that WebView queries the database.

Lists of cached items and templates are stored in the memory space of New Atlanta ServletExec.

- Report items are cached only if the ICM database is not partitioned.
- Report templates are cached regardless of database partitioning.

You can specify many cache settings using the adminui.properties file, located in the \<ICM ROOT>\web\webview\reporting\servlet\properties\ directory.

Basic cache configurations you can modify include enabling and disabling caching and setting the cache refresh and purge times. You can also enable and disable separate caching for supervisors.

For NAM environments, you can enable customer call type filtering so that each customer has a separate cache for call type report items and templates for that customer’s call types.

If you modify the adminui.properties file, you must restart the IIS Admin services on the WebView server machine for the changes to take effect.

By default, caching is enabled for report templates and report items. The time interval after which the cache refreshes is also set by default, as is the interval after which the cache is purged.

Enabling and Disabling Caching

To enable or disable caching, complete the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Set the value of the DISABLE_ITEM_LIST_CACHING property to true or false.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Restart the IIS Admin services for the change to take effect.</td>
</tr>
</tbody>
</table>

Setting the Cache Refresh Time

To set the cache refresh time, complete the following steps:
**Caching Templates and Items**

**Step 1**  
Set the value of the `WEBVIEW_LISTCACHE_LIVETIME` property to the number of minutes after which you want the cache to refresh.  
For example: `WEBVIEW_LISTCACHE_LIVETIME = 240`

**Step 2**  
Restart the IIS Admin services for the change to take effect.

**Setting the Cache Purge Time Factor**

The cache purge time factor controls the interval after which the cache is purged.

By default, the cache purge time factor is 4 and the cache live time is 120 minutes. By these default settings, the cache is purged after 8 hours.

Templates and items that have been in the cache for less than the value set for the `WEBVIEW_LISTCACHE_LIVETIME` property are not purged. For example, if the `WEBVIEW_LISTCACHE_LIVETIME` property is set to 120, items that have been in the cache for fewer than 120 minutes are not purged.

If you notice that the size of the cache is consuming too much memory, set the value of this property to a small number so that the cache purges more often.

**To set the cache purge time factor, complete the following steps:**

**Step 1**  
Set the value of the `PURGE_TIME_MULTIPLIER` property to the factor by which you want to multiply the value of the `WEBVIEW_LISTCACHE_LIVETIME` property.  
For example: `PURGE_TIME_MULTIPLIER = 2.`

**Step 2**  
Restart the IIS Admin services for the change to take effect.

**Enabling and Disabling Supervisor Caching**

Supervisors who log in to WebView and run reports from the Agent report categories view data for only those agents, teams, and skill groups that they supervise.

Each supervisor can have his/her own cache for the agent report categories: Agent By Agent, Agent By Team, Agent By Skill Group, and Agent By Peripheral. These are the only categories for which supervisors are allowed to run reports.

By default, report template and item supervisor caching is enabled for the Agent report categories.

If the supervisor caches consume too much memory, you can either reset the `PURGE_TIME_MULTIPLIER` property or disable supervisor caching.

**To disable supervisor caching, complete the following steps:**

**Step 1**  
Set the value of the `ENABLE_SUPERVISOR_CACHING` property to `false`.

**Step 2**  
Restart the IIS Admin services for the change to take effect.

**To enable supervisor caching, complete the following steps:**
**Step 1**  Set the value of the `ENABLE_SUPERVISOR_CACHING` property to `true`.

**Step 2**  Restart the IIS Admin services for the change to take effect.
How to Run PATCHPBL to Update or Fix Templates

If Cisco templates need to be updated after a WebView upgrade, or if a Cisco template needs to be replaced (for example, if it was deleted or changed by mistake), you can use the PATCHPBL utility to regenerate the report library files.

The PATCHPBL utility does not update or overwrite custom templates. See the Template Design Guide Using InfoMaker for Cisco ICM/IPCC Enterprise & Hosted Editions for information on how to use Sybase InfoMaker to create and edit custom templates.

What the PATCHPBL Utility Does

The PATCHPBL utility regenerates the PPB050.PBL files. If a PPB050.PBL file does not exist, the utility creates that file.

The PATCHPBL utility goes through each report-category directory, reads each category’s srlist.txt file, and copies all the listed SRD files into the PPB050.PBL file.

How to Run the PATCHPBL Utility

The PATCHPBL utility is located in the ICM\bin directory and is put there when WebView is installed.

To run the PATCHPBL utility, from the command-prompt window, use the following command format:

PATCHPBL -root <drive>:\ICM\<instance_name>\aw

For example: PATCHPBL -root C:\ICM\Cisco\aw
WebView Registry Settings and Property Files

This chapter covers the following registry and property file settings on the WebView server:

It includes the following sections:

- Registry Settings, page 9-1
  - AllowAdminLogin, page 9-1
  - Event, page 9-2
- Property Files, page 9-3
  - adminui.properties, page 9-3
    Administration and User Interface, page 9-3
    Caching, page 9-4
    Graph Sizing, page 9-4
    PowerBuilder ActiveX Control, page 9-5
    Jaguar WatchDog, page 9-5
    SSL Encryption, page 9-6
    Footer, page 9-6
  - jagconnection.properties, page 9-8
  - WebView.properties, page 9-9
  - wvLocale.properties, page 9-9

Registry Settings

**Note**

Registry entries that are set as a result of entries in ICM setup are not recorded here.

**AllowAdminLogin**

Prior to Release 7.0(0), the registry settings included a TRUE|FALSE value to allow or disallow the administrator account to log in to WebView.

By default, the administrator account could not log in to WebView.
In Release 7.0, ‘AllowAdminLogin’ is ignored. To log in to WebView, an administrator account needs to be granted access to WebView as any other user. That is, the administrator must be in an appropriate WebView group in Active Directory.

**Event**

**Key:** HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc\ICM\<instance>\Distributor\RealTimeDistributor\CurrentVersion\Logger\CurrentVersion\HistoricalData\Event  
**Name:** Event  
**Data Type:** DWORD  
**Acceptable Values:** [0 | 1]  
**Purpose:** Enables/Disables event replication from the logger to the HDS. 0 is disable, 1 is enable. If Event replication is disabled, then no events will appear in Event Viewer. 0 is the default.

---

**Note**  
The registry key is only valid on the Admin Workstation, regardless of whether WebView is installed on the Admin Workstation. The key indicated to the AW whether it should pull event data from the logger database into the historical database, which is what WebView eventually reports on.
Property Files

This section explains the four files that hold WebView properties.
For normal use, it is not be necessary to change values in the properties files.

adminui.properties

Location: <ICMRoot>\web\webview\reporting\servlet\properties\adminui.properties

Purpose: The main properties file for WebView. Allows you to define various settings. Sections in this properties file are listed below.

Administration and User Interface

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>adminui.ADMIN_TIMEOUT=</td>
<td>The length of time a WebView session can be idle before the user is asked to log in again,</td>
<td>120</td>
</tr>
</tbody>
</table>
**Property Files**

### Caching

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEBVIEW_LISTCACHE_LIVETIME=</td>
<td>Cache time to live</td>
<td>120</td>
</tr>
<tr>
<td>DISABLE_ITEM_LIST_CACHING=</td>
<td>Enable/Disable caching of items list for all categories</td>
<td>false</td>
</tr>
<tr>
<td>ENABLE_SUPERVISOR_CACHING=</td>
<td>Enable/Disable caching of items list for supervisors</td>
<td>true</td>
</tr>
<tr>
<td>SUPERVISOR_CATEGORIES=</td>
<td>Categories where special treatment for supervisor is applicable. Categories are separated by semicolon.</td>
<td>agteam;agtper;agtskg;peragt</td>
</tr>
<tr>
<td>PURGE_TIME_MULTIPLIER=</td>
<td>Multiplier factor for purge thread to clean up cached items. Multiplier factor is multiplied to 'livetime' for purge thread intervals. Example: If live time is 2 hours and multiplier is 4, then purge thread would be kicked off every 8 hours.</td>
<td>4</td>
</tr>
<tr>
<td>ENABLE_CALTYP_CUSTOMER_FILTER=</td>
<td>Enables/disables filtering based on customer id for call type category. This key must be set to 'true' for service provider installations</td>
<td>false</td>
</tr>
</tbody>
</table>

### Graph Sizing

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRAPH_WIDTH=</td>
<td>Graph width in PowerBuilder units</td>
<td>3500</td>
</tr>
<tr>
<td>GRAPH_HEIGHT=</td>
<td>Graph height in PowerBuilder units</td>
<td>1750</td>
</tr>
<tr>
<td>GRAPH_SIZETODISPLAY=</td>
<td>Graph sizetodisplay - boolean</td>
<td>false</td>
</tr>
<tr>
<td>GRAPH_BORDER=</td>
<td>Graph border - boolean</td>
<td>false</td>
</tr>
<tr>
<td>GRAPH_VALUELABELFONHEIGHT=</td>
<td>Graph font size for label string on value axis</td>
<td>12</td>
</tr>
<tr>
<td>GRAPH_SERIELABELFONHEIGHT=</td>
<td>Graph font size for label string on series axis</td>
<td>12</td>
</tr>
<tr>
<td>GRAPH_CATEGORYLABELFONHEIGHT=</td>
<td>Graph font size for category label</td>
<td>12</td>
</tr>
<tr>
<td>GRAPH_VALUEDISPLAYFONHEIGHT=</td>
<td>Graph font size for data strings on value axis</td>
<td>10</td>
</tr>
<tr>
<td>GRAPH_SERIESDISPLAYFONHEIGHT=</td>
<td>Graph font size for data strings on series axis</td>
<td>10</td>
</tr>
<tr>
<td>GRAPH_CATEGORYDISPLAYFONHEIGHT=</td>
<td>Graph font size for category data display strings</td>
<td>10</td>
</tr>
<tr>
<td>GRAPH_LEGENDDISPLAYFONHEIGHT=</td>
<td>Graph font size for legend strings</td>
<td>10</td>
</tr>
</tbody>
</table>
### PowerBuilder ActiveX Control

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>PBACTIVEX_WIDTH=</td>
<td>PowerBuilder ActiveX control width in browser - in pixels</td>
<td>120</td>
</tr>
<tr>
<td>PBACTIVEX_HEIGHT=</td>
<td>PowerBuilder ActiveX control height in browser - in pixels</td>
<td>550</td>
</tr>
<tr>
<td>PBACTIVEX_VSBAR=</td>
<td>PowerBuilder ActiveX control vertical scroll bar - boolean</td>
<td>true</td>
</tr>
<tr>
<td>PBACTIVEX_HSBAR=</td>
<td>PowerBuilder ActiveX control horizontal scroll bar - boolean</td>
<td>true</td>
</tr>
</tbody>
</table>

### Jaguar WatchDog

For a detailed description of the Jaguar Watchdog settings, see Chapter 6, “Jaguar Administration and the Jaguar Watchdog.”

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>WATCHDOG_COMPONENTS</td>
<td>Do not change this property.</td>
<td>n_icmsysinfo; n_icmdw; n_icmauth; n_wvreportfns</td>
</tr>
<tr>
<td>WATCHDOG_CONNECTION_ATTEMPTS_INTERVAL</td>
<td>Amount of time in seconds between connection attempts to EAServer.</td>
<td>15</td>
</tr>
<tr>
<td>WATCHDOG_CONNECTION_ATTEMPTS</td>
<td>Number of times the Watchdog attempts to connect to EAServer before sending a request to the OS to restart EAServer.</td>
<td>10</td>
</tr>
<tr>
<td>WATCHDOG_EASERVER_RESTART_TIME</td>
<td>Amount of time in seconds to wait for EAServer to restart before reattempting to connect.</td>
<td>120</td>
</tr>
<tr>
<td>WATCHDOG_EXCEPTIONS_TO_IGNORE</td>
<td>A semicolon-separated list of exceptions the WatchDog ignores when running a method. An entry of &quot;*&quot; causes it to ignore all exceptions. In the case of a CORBA exception (such as org.omg.CORBA.COMM_FAILURE), list the last part only; for example, &quot;COMM_FAILURE.&quot; Other exceptions must be fully qualified.</td>
<td></td>
</tr>
<tr>
<td>WATCHDOG_MEGABYTES_PER_LOG</td>
<td>Maximum size a log file can grow before the next file is created.</td>
<td>5 meg.</td>
</tr>
<tr>
<td>WATCHDOG_NUMBER_LOG_FILES</td>
<td>Number of log files to rotate through. When one log file reaches the size threshold, Watchdog creates and starts filling the next. See About Jaguar Watchdog Logging, page 6-7.</td>
<td>5</td>
</tr>
<tr>
<td>WATCHDOG_PACKAGE</td>
<td>Do not change this property.</td>
<td>webview</td>
</tr>
</tbody>
</table>
### Property Files

#### SSL Encryption

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL_ENCRYPTION_LEVEL=</td>
<td>The encryption level for WebView. This is modified by the SSL Encryption Utility only. Do not modify this value in the adminui.properties file. See The SSL Encryption Utility, page 10-6. Values are: none – All information is sent in clear text between the browser and the server, including usernames and passwords when logging into WebView authentication – The login information (username and password) will be encrypted, but the rest of the session will be in clear text session - The entire WebView session, including login, viewing reports, etc. will be encrypted.</td>
<td>Authentication</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
<td>Value</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>FOOTER_FR_LEFT=</td>
<td>Values in the footer of reports.</td>
<td>user</td>
</tr>
<tr>
<td>FOOTER_FR_RIGHT=</td>
<td>Values in the footer of reports.</td>
<td>report</td>
</tr>
<tr>
<td>FOOTER_SR_LEFT=</td>
<td>Values in the footer of reports.</td>
<td>date</td>
</tr>
<tr>
<td>FOOTER_SR_RIGHT=</td>
<td>Values in the footer of reports.</td>
<td>template</td>
</tr>
</tbody>
</table>
jagconnection.properties

**Location:** <EAServerRoot>/html/classes/com/cisco/atg/jagconnection.properties

**Purpose:** Specifies connection parameters for WebView to connect to the Jaguar Server. Modify the values in this file if you change connection parameters for Jaguar such as Username, Port, Password, and so on.

**Sample jagconnection.properties file:**

```properties
JAGCONNECT_CORBA_ORB_CLASS=com.sybase.CORBA.ORB
JAGCONNECT_JAGUAR_SERVER=
JAGCONNECT_IIOP_PORT=9000
JAGCONNECT_JAGUAR_ADMIN=jagadmin
JAGCONNECT_JAGUAR_ADMIN_PWD=
JAGCONNECT_JAGUAR_SYS_BEAN=webview/n_icmsysinfo
JAGCONNECT_JAGUAR_DW_BEAN=webview/n_icmdw
JAGCONNECT_JAGUAR_AUTH_BEAN=webview/n_icinauth
JAGCONNECT_JAGUAR_WVREPFNS_BEAN=webview/n_wvreportfns
```


**WebView.properties**

*Location:* `<ICMRoot>\web\webview\reporting\servlet\WebView.properties`

*Purpose:* Contains all WebView-specific localized information in English. This is the default that will be used if there is no localized file for the default locale of the WebView server machine.

**wvLocale.properties**

*Location:* `<ICMRoot>\web\webview\reporting\servlet\wvLocale.properties`

*Purpose:* Contains the mapping between locales and date format.
WebView Security: Active Directory and Secure Socket Layer

This chapter covers two security features in WebView Reporting. It includes the following topics:

- **About Active Directory, page 10-2**
  - Domain Rights for the WebView Administrator, page 10-2
  - User Membership in the WebView Domain Local Security Group, page 10-2
  - WebView User Authentication Model, page 10-2
- **About SSL, page 10-4**
  - SSL Configuration at ICM Setup, page 10-4
  - Changes at User Log In, page 10-4
  - The SSL Encryption Utility, page 10-6
About Active Directory

The Microsoft Active Directory® (AD) service ensures integrity and security in network environments by managing information about access rights to applications, files, databases, and other resources.

The authentication model in Release 7.0(0) is aligned with Active Directory in compliance with accepted Microsoft blueprints. Required privileges for ICM WebView are limited in accordance with AD standards.

For details on Active Directory, refer to the Staging and Active Directory Guide for Cisco ICM/IPCC Enterprise & Hosted Editions.

Domain Rights for the WebView Administrator

To install the WebView Reporting component of ICM Setup, the WebView administrator must have local admin and setup rights to the ICM domain.

No other configuration and reporting functions require overall domain administrative capability.

User Membership in the WebView Domain Local Security Group

In the previous release, each user account was created individually. The individual who created user accounts did so by using the User List tool in the ICM Configuration Manager utility.

This remains a valid method of adding user accounts.

Customers now have the option to assign WebView privileges to any AD users by making them members of the WebView Domain Local Security Group (DLG).

This is now the way to add users in Release 7.0(0).

WebView User Authentication Model

This section explains how WebView user authentication aligns with the ICM Active Directory model. The hierarchy of AD Organizational Unit's (OU's) and the Domain Local Security Group's (DLG's) in an ICM deployment is as follows:

```
<Root>
  CiscoICM_<function>

<Facility>
  <facility_name>_<function>

<Instance>
  <facility_name>_<instance_name>_WebView
```

A WebView user account would be an account in the AD with membership of "<facility_name>_<instance_name>_WebView" DLG within the respective "<Instance>" OU.
Consequently, in Release 7.0(0), the qualification requirements for a WebView user account change from Windows NT domain account with an entry in the USER_GROUP table to Active Directory account with membership in WebView Domain Local Security Group (DLG) within respective Organizational Unit (OU) for that instance.

**Figure 10-1  Active Directory**

Using standard Active Directory tools, the User List Tool, or the ICM Domain Manager tool, the AD administrator can assign WebView privileges to any AD users by making them members of the WebView Domain Local Security Group (DLG).

No special privileges are assigned to members of WebView DLG at the facility and ICM root OU's

**UserNames**

You can login to WebView by entering the username in the following ways:

- `<domain><user>`
- `<domain>/<user>`
- User Principal Name (user@domain.com)
- `\user` (defaults to domain associated with the WebView server machine)
- `/user` (defaults to domain associated with the WebView server machine)
- `user` (defaults to domain associated with the WebView server machine)
About SSL

Secure Socket Layer (SSL) is a protocol that allows secure communication between a web browser and the web server.

The 7.0(0) release of WebView supports 128-bit encryption for SSL 3.0 when the WebView server is installed in a Windows 2003 Server environment with Microsoft Internet Information Services (IIS) version 6.0.

For upgrade customers who have Windows 2000 Server and IIS 5.0, the SSL option is greyed out in ICM Setup, and when it is installed, it will be disabled.

SSL Configuration at ICM Setup

The WebView Node Properties screen in ICM Setup includes a group box to configure SSL 3.0 Encryption for WebView.

This group box has the following controls:
- a checkbox for Enable Encryption (128-bit), which is selected by default.
- a checkbox to encrypt the Session

The administrator can change the default configuration from ICM Setup and also has the option to change the configuration at any time by invoking the SSL Encryption Utility. See The SSL Encryption Utility, page 10-6 for information on how to use the utility.

Accepting the defaults:
- generates a self-signed certificate (using OpenSLL), imports that certificate to the local Machine Store, and installs it on the IIS Web Server.
  A self-signed certificate is a certificate that has not been signed by an external authority. It ensures that an encrypted Web connection is in place.
- ensures that the Authentication information entered for WebView log in (user name and password) is encrypted

If the administrator installs multiple WebView servers, each is set up with its own certificate, and SSL can be configured independently for each.

If another certificate is already installed, ICM Setup does not replace it or overwrite the existing certificate.

The administrator can subsequently obtain and install a certificate that is signed by a corporate Certificate Authority or by a trusted third-party CA such as Verisign. Administrators who choose to do this can simply follow the procedure presented by that CA or refer to the instructions in the Microsoft Knowledge Base to configure IIS directly.

Changes at User Log In

This section explains two minor changes that reporting users experience when SSL is enabled.

URL

If SSL is enabled for Authentication, the reporting user enters a WebView URL that begins with http.
If SSL is enabled for the full Session, the URL for each page begins with https.
Security Alert

The first time reporting users open an SSL-enabled page, they see a Security Alert prompting them to accept the server certificate.

Options on this message are Yes, No, or View Certificate.

- Selecting Yes accepts (trusts) the certificate for this browser session only. The Security Alert will display the next time the user accesses WebView.
- Selecting No prevents the WebView access. The browser displays a blank page.
- Selecting View Certificate opens a screen that presents the option to install the certificate. Clicking Install saves the certificate locally, and the Security Alert does not display again.
The SSL Encryption Utility

The SSL Encryption Utility is a standalone application that any local administrators on the WebView server can use to change the SSL settings without launching ICM Setup.

Launching the Utility

If the WebView server is located on the distributor Admin Workstation, administrators can run this utility from the AW Program Group.

If the WebView server is located on a separate machine, administrators can run this utility from the WebView server (/icm/bin/sslutil.exe).

User Interface

The SSL Encryption Utility has two tabs.

- The Configuration tab shows whether SSL is currently enabled for the ICM web-based application detected in your environment. These are WebView, Dynamic Reskilling/WebConfig, and Internet Script Editor.
  
  To make changes on this tab, select the ICM instance. Then, for that instance, select or deselect SSL 3.0 Encryption.

  For WebView, selecting Enable Encryption enables two radio buttons: Authentication and Session.
  
  - Authentication encrypts the login page with user name and password but does not encrypt the session.
  
  - Session assumes Authentication and encrypts all pages sent between the user and the WebView server (such as queries, reports, and help).

- The Certificate Authentication tab has one button: Execute.

  Click it to verify if a certificate was previously created. If a certificate exists, the administrator sees a prompt to overwrite or cancel.

  If no certificate exists, the utility creates a self-signed certificate in <installDrive>\icm\ssl\host.crt.

Applying changes updates the encryption values in the adminui.properties (to none, auth, or session). The administrator does not need to restart IIS for the changes to take effect.
Troubleshooting Tips

This chapter contains troubleshooting information on these topics:

Logs, page 11-4

Third-Party Software, page 11-5
  - Browser Setting for Trusted Sites, page 11-5
  - Checking New Atlanta ServletExec, page 11-5
  - Debugging: Turning it On and Off for Third-Party Tools, page 11-6
  - EAServer/Jaguar Installation Fails, page 11-7
  - Error 2221: Determine Current User Security Type, page 11-7
  - Error After Changing the Jaguar Admin Password, page 11-7
  - Error: IIS Admin Service Configuration, page 11-7
  - Error: The Windows Scripting Host Must be Installed, page 11-9
  - Jaguar Server Connection Fails After Restart, page 11-9
  - Jaguar Service Verification, page 11-9
  - Removing Old Versions of EAServer/Jaguar, page 11-10
  - Third-Party Software Licenses, page 11-10
  - World Wide Publishing Service: Stopping it and Restarting WebView, page 11-11

Installation and Login, page 11-12
  - Java Code Displays After Login, page 11-12
  - Users Unable to Log in to WebView, page 11-12
    - Are They Entering the Correct UserName?, page 11-12
    - Are They a Member of the WebView Group?, page 11-12
    - Are They Seeing HTTP Error 403.4?, page 11-12
    - Are They Using a Blank Password?, page 11-13
    - Has the IP Address Changed?, page 11-13
    - Has the Password Expired or the User Account Been Disabled?, page 11-13
    - Is Jaguar Working Correctly?, page 11-13
  - WebView Database Messages at Login, page 11-13
  - WebView Supervisors Rights and Active Directory Account, page 11-14
• WebView User Unable to Change Password, page 11-14

Job Scheduler, page 11-15

• Job Scheduler Does Not Work
  – Are Terminal Services Running on the Client?, page 11-15
  – Does the User Have Access to a Printer?, page 11-15
  – Does the User have Minimum Rights?, page 11-15
  – Is ActiveX Enabled?, page 11-15
  – Is Fast User Switching Disabled on the Client?, page 11-15
  – Is the User Logged in When the Job is Triggered?, page 11-16
  – Is the WebView Server added to the Trusted Sites List?, page 11-16

• Job Scheduler File Not Found Message, page 11-16
• Job Scheduler Upgrade Does Not Migrate Jobs to New Server, page 11-16

Reports and Templates, page 11-17

• 3000 Row Limit, page 11-17
• Agent Data Does Not Appear in Reports, page 11-17
• Blank Dialer Port Status Real-Time Report, page 11-18
• Blank Pages When Report is Rendered, page 11-19
• Caltype Items in Reports, page 11-19
• Date Formats are Incorrect or Historical Reports do not show for a Specified Time Period, page 11-19
• Error Retrieving Information from the Web Server, page 11-20
• Errors Running Reports, page 11-20
• Graphical Reports Do Not Print, page 11-20
• Graphical Reports Do Not Work Correctly, page 11-21
• Header truncated in French Reports, page 11-21
• Historical Reports Do Not Work Correctly, page 11-21
  – Historical Reports Fail, page 11-21
  – Historical Reports Saved with Fixed Date Do Not Work Correctly, page 11-22
  – Historical Reports Slow the System, page 11-22
• Pages do not Display Correctly, page 11-22
• Private and Favorite Reports Not Displayed After Upgrading, page 11-24
• Saved Reports Do Not Work, page 11-25
• Time difference between ICM Record and WebView Report, page 11-25

You can also find installation and maintenance troubleshooting information in other sections of this guide:

• If you are having problems with your WebView installation, check Troubleshooting Your WebView Installation in Chapter 3.
• For information on browser settings, see The Web Browser, page 1-7.
• If you have questions about templates, see Chapter 8, “Template Maintenance.”

For troubleshooting tips on the WebView application, refer to the WebView online help.

For troubleshooting tips on custom templates, refer to Template Design Guide Using InfoMaker for Cisco ICM/IPCC Enterprise & Hosted Editions.

If you still have problems, obtain technical assistance, as described in the Preface of this guide.
Logs

Refer to these logs for errors and information recorded during the installation of the third-party tools:

**WebView Third-Party Installer:** C:\Temp\WVThirdPartyInstaller.log

**JDK Installer:** C:\Temp\jdk142Setup.log

**New Atlanta ServletExec Installer:** C:\Temp\NASEI.log

**Sybase EAServer 5.0 Installer:** C:\Temp\EAServer50.log

**Sybase EAServer 5.1 Installer:** C:\Temp\EAServer51.log

**Sybase PowerBuilder VM 10 Installer:** C:\Temp\pbvm10install.log

Refer to these logs for errors, warnings, and Java exceptions recorded while using the WebView application:

**New Atlanta ServletExec:** C:\Program Files\New Atlanta\ServletExec ISAPI\ServletExec.log

**Sybase EAServer:** C:\Program Files\Sybase\EAServer\bin\jaguar.log

Refer to this log for errors and information recorded while using Job Scheduler:

**Job Scheduler:** <SYSTEM32DIR>\JobScheduler.log

The JobScheduler.log is located on the system where the job was scheduled to execute. That is, it is located on the client system, if the job was scheduled to print or save to the client. It is located on the WebView server, if the job was scheduled to print or save there.
Third-Party Software

Browser Setting for Trusted Sites

Enhanced security settings in newer versions of Internet Explorer prevent some WebView features from working correctly. For example, you might experience blank pages and issues with the Job Scheduler and with graphical reports.

To resolve this, add the WebView Server to the Trusted Sites list on the browser as follows:

**Step 1** Select **Tools > Internet Options > Security** from the browser menu.

**Step 2** Click **Trusted Sites**. Then click **Sites...**

**Step 3** In the Trusted Sites dialog box, enter these URLs for WebView:

http://<webview_server>
https://<webview_server>

**Step 4** Click **Add**.

**Step 5** Click **OK** to apply the setting and close the Trusted Sites dialog box.

**Step 6** Click **Custom Level** on the Security tab and verify that the following are enabled:

- Download signed ActiveX controls
- Run ActiveX controls and plug-ins
- Script ActiveX controls marked safe for scripting

**Step 7** If these settings are enabled, click **Cancel**.

If they are not enabled, enable them, click **OK**, and confirm your change.

**Step 8** Click **OK** to exit the tool.

Checking New Atlanta ServletExec

Follow this procedure to test whether New Atlanta ServletExec is running:

**Step 1** Navigate to http://localhost/servletexec/admin from a browser on the WebView server.

**Step 2** At the ServletExec Administration login page, enter the username of **admin** and no password.

If you can log in, ServletExec is running.

If ServletExec is not running, you will not see a login page:

- If no page is served up, make sure that IIS Admin is running, and the World Wide Web Publishing service is started.
- Check that the default website is running in the Internet Information Services Console.
- Verify that ServletExec is installed. Use **Control Panel > Add/Remove Programs** to do this.
If you see a blank screen or an error, check the `ServletExec.log` and `ServletExecNative.log` files for further error messages.

Consider uninstalling and re-installing the third-party tools. See Uninstalling and Reinstalling the Third-Party Software, page 2-9.

Refer to the New Atlanta documentation, which is installed on your server, for information on a utility named `DBMon` that can be used to troubleshoot of ServletExec.

### Debugging: Turning it On and Off for Third-Party Tools

**To turn ServletExec Debug On/Off:**

1. Navigate to, and open, this file: `c:\<icmroot>\web\webview\reporting\servlet\properties\adminui.properties`
2. Edit the key `WEBVIEW_DEBUG` as follows:
   - Set to `true` for Debug On.
   - Set to `false` for Debug Off.
3. Restart the IISAdmin and W3SVC services for the changes to take effect.

**To turn EAServer/Jaguar Debug On/Up**

1. Navigate to this file `c:\<icmroot>\web\webview\utils\DebugOn.reg`.
2. Right-click on the file and choose `Edit`.
3. Modify "Debug"=dword:0000000x. Settings are as follows:
   - x=1 is basic debugging.
   - x=2 is more detailed debugging. This is typically the highest level you will need.
   - x=3 is the most detailed debugging. This setting makes logs grow very quickly. Use it only when troubleshooting header locking in reports.
4. Save `DebugOn.reg` and close the file.
5. Double-click `DebugOn.reg` and click `Yes` when asked to add the information to the registry.
6. Restart the Jaguar service for changes to take effect.

**To turn EAServer/Jaguar Debug Off.**

1. Double-click `DebugOff.reg` and click `Yes` when asked to add the information to the registry.
2. Restart the Jaguar service for changes to take effect.
EAServer/Jaguar Installation Fails

If the Jaguar server fails to start, you might have performed a custom EAServer/Jaguar installation that was not tested by Cisco Systems. WebView supports the EAServer only as configured by the Cisco Third-Party installer and by the ICM installer. Do not deviate from the typical configuration without contacting Cisco.

To restore to a supported configuration, follow these procedures:

1. Follow the instructions in Chapter 2 to uninstall EAServer/Jaguar. See page 2-9.
2. Follow the instructions in Chapter 3 to uninstall WebView. See page 3-8.
3. Restart the computer.
4. Rerun the Third-Party software installation and select the typical installation option. See page 2-6.
5. Reinstall the ICM WebView software.

Note: This tip does not apply to System IPCC Enterprise deployments.

Error 2221: Determine Current User Security Type

This message might appear when you are installing the distributor Admin Workstation:

SEVERE: Error 2221 occurred while trying to determine the current user security type.

It indicates that the Admin Workstation cannot contact the Domain Controller. Make sure the Admin Workstation is part of a domain, that a domain administrator is logged in, and that the domain can be reached and is started.

Note: This tip does not apply to System IPCC Enterprise deployments.

Error After Changing the Jaguar Admin Password

If you change your Jaguar admin password, WebView requires that you change it two places—in both the EAServer Manager Login dialog box and in the jagconnection.properties file.

If you change the password in EAServer Manager without also changing it in the jagconnection.properties file, you will see an error message similar to this when you attempt to open WebView: Error - LogonUser returned an error code = 1326.

See Changing the Jaguar Admin Password, page 6-1.

Error: IIS Admin Service Configuration

During the installation of the third-party software for WebView, you might see an error message that the IIS Admin Service was configured incorrectly.
When IIS Admin Service starts up, the account information stored in IIS is synchronized with the local SAM, but the COM+ applications are not automatically updated. The result is that requests to out-of-process applications fail.

To resolve this problem, run the `synciwam.vbs` admin script to update the IIS COM+ applications with the correct identity.

**Follow this procedure to perform the synchronization:**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Navigate to <code>&lt;IIS Install Drive&gt;/Inetpub/AdminScripts/synciwam.vbs.</code></td>
</tr>
<tr>
<td>Step 2</td>
<td>Right click <code>synciwam.vbs</code>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>Open with Command Prompt.</strong></td>
</tr>
<tr>
<td>Step 4</td>
<td>A command window opens and runs the <code>synciwam.vbs</code> script. Wait until the script completes and closes.</td>
</tr>
</tbody>
</table>
Error: The Windows Scripting Host Must be Installed

When installing the third-party software, you might see this error message:

The Windows Scripting Host must be installed. Download and run the installer from Microsoft: <<url>>. Setup will now abort.

The windows scripting host is the engine that runs Visual Basic scripts (VBScripts) on a Windows computer. It is necessary for the execution of the WebView Third-Party software installer, which uses VBScripts for certain critical tasks.

Follow this procedure to install the Scripting Host:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Navigate to the URL defined in the error message and download the installer appropriate for your operating system.</td>
</tr>
<tr>
<td>2</td>
<td>Navigate to the folder where you downloaded the file, open the file to initiate the installation, and accept all defaults.</td>
</tr>
<tr>
<td>3</td>
<td>When the installation completes, restart your computer and run the WebView Third-Party Installer.</td>
</tr>
</tbody>
</table>

Jaguar Server Connection Fails After Restart

After Jaguar is restarted by the Windows Services Control Panel, it might intermittently fail to release the port.

If Jaguar appears to be running after a restart, but WebView users cannot log in or run reports, follow this procedure to shut down and Jaguar:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open a command prompt.</td>
</tr>
<tr>
<td>2</td>
<td>Browse to the Program Files/Sybase/EAServer/bin folder.</td>
</tr>
<tr>
<td>3</td>
<td>Enter this command: jagtool shutdown.</td>
</tr>
<tr>
<td>4</td>
<td>Use the Windows Services Control Panel to start the service back up.</td>
</tr>
</tbody>
</table>

Jaguar Service Verification

Follow this procedure to verify that Jaguar service is installed and started:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>From the Start menu, select Programs &gt; Administrative Tools &gt; Services.</td>
</tr>
<tr>
<td>2</td>
<td>In the Services dialog box, make sure that Jaguar is listed (installed) and started:</td>
</tr>
<tr>
<td></td>
<td>• If it is not started, right click on Jaguar and select the Start option from the pop-up selection box.</td>
</tr>
<tr>
<td></td>
<td>• If it is not installed, run the following from the command line window: %JAGUAR%\bin\serverstart.bat -install. Then, start the service as indicated in the first bullet.</td>
</tr>
</tbody>
</table>
Removing Old Versions of EAServer/Jaguar

Before you install EAServer, it is best to make sure that you are starting with a clean slate. Do not install EAServer (Jaguar) ‘over itself’. To remove any remnants of EAServer (Jaguar), perform the following steps. Then re-run setup.

Step 1  Stop the following NT services: IISAdmin, Jaguar, Sybase EP Management Agent, sysam.
Step 2  Close any open Services control panel windows.
Step 3  Close any windows with the title “Jaguar CTS Jaguar”.
Step 4  Run the file: `c:\program files\sybase\CIMRepository-3_0_0\bin\stoprepository.bat`.
Step 5  Run the file: `c:\Program Files\Sybase\AgentManager-3_0_0\bin\am_stop.bat`.
Step 6  From a command prompt, execute the following command: `%JAGUAR%\bin\serverstart.bat -remove`
Step 7  From a command prompt, execute the following command: `c:\Program Files\Sybase\SYSAM-1_0\bin\installs.exe -n sysam -r`
Step 8  From a command prompt, execute the following command: `c:\Program Files\Sybase\shared-1_0\bin\sybjsvc.exe -d -sn"Sybase EP Management Agent."
Step 9  Delete the entire `c:\program files\sybase` folder.
Step 10 Delete the folder `c:\flexlm`.
Step 11 Delete the registry key: HKEY_LOCAL_MACHINE\Software\Sybase.
Step 12 Delete the registry key: HKEY_LOCAL_MACHINE\Software\Sybase, Inc.
Step 13 Remove the following Environment Variables: Jaguar, LM_LICENSE_FILE, SYBASE_SYSAM.
Step 14 Remove any references to the sybase folders from the PATH and CLASSPATH environment variables.
Step 15 Restart the computer.

Third-Party Software Licenses

Cisco Systems distributes and automatically installs the four-CPU license for New Atlanta ServletExec ISAPI 4.1. If the server on which you are installing WebView has more than four processors, you must obtain a greater-than-four CPU license from New Atlanta.

Follow this procedure to install a four-CPU or more license for New Atlanta:

Step 1  Install the WebView third-party software. See Chapter 2, “Installing the Third-Party Software.”.
Step 2  Install the WebView Reporting software. See Chapter 3, “Installing WebView.”
Step 3  Obtain the license from New Atlanta if you have not already done so.
Step 4  Open the file `<NewAtlantaRoot>\ServletExec ISAPI\ServletExec Data\servers.properties`, where `<NewAtlantaRoot>` is the New Atlanta directory; for example: `C:\Program Files\New Atlanta`.
Step 5  Change the line `servletexec.serial=<license_#>` such that `<license_#>` is your new license number.
Step 6  Save the file and restart the IIS Admin NT service for the change to take effect.

**World Wide Publishing Service: Stopping it and Restarting WebView**

You might encounter this error: Stopping the World Wide Web publishing service stops WebView. Restarting the web publishing does not bring WebView back up.

This error is due to a limitation in IIS whereby stopping the World Wide Web Publishing service, but not the IIS Admin service, crashes New Atlanta with errors. When you restart the Web Publishing service, New Atlanta does not start.

To resolve this, restart the IIS Admin Service as follows:

- **Step 1**  From the Start button, select **Settings > Control Panel > Administrative Tools > Services.**
- **Step 2**  In the Services dialog box list of services, double click **IIS Admin Service.**
- **Step 3**  In the IIS Admin Service Properties dialog box, click **Start.**
  Click **OK** and then exit the Services dialog box.
Installation and Login

See Troubleshooting Your WebView Installation, page 3-8 for a checklist of solutions to typical installation issues. This section explains less common issues.

Java Code Displays After Login

Seeing Java code rather than the WebView window when you log in to WebView can indicate that some WebView files are missing from the New Atlanta directory.

This occurs if you uninstalled and then reinstalled the New Atlanta ServletExec. Your uninstallation of Servlet Exec might have removed WebView files that were in the New Atlanta Servlet directory.

To resolve this, in addition to reinstalling the New Atlanta Servlet, rerun ICM Setup in Upgrade All mode to reinstall the missing WebView files.

Then run WebView to verify that it displays properly.

If you still see Java code when you open WebView, call the Cisco TAC.

Users Unable to Log in to WebView

Are They Entering the Correct UserName?

Make sure that the username has one of the recognized formats described in UserNames, page 10-3.

Try the form <domain>\username to ensure that WebView is not assuming the wrong domain.

Are They a Member of the WebView Group?

Use the standard Active Directory tools or the ICM Domain Manager utility to make sure the user is a member of the WebView group at the Instance, Facility, or Root level for the desired instance.

Are They Seeing HTTP Error 403.4?

If SSL is enabled for the Full Session and a user is unable to log in or sees an 403.4 HTTP error, make sure to use the https protocol in the URL.

If Full Session SSL Encryption is enabled at ICM Setup, then the URL to log in to WebView must include the https protocol; for example: https://<server>/<instance>.

Similarly, when you add the WebView server to the Trusted Sites, you must use the https protocol.

If SSL is enabled, and you enter http://<server>/<instance>, you see an error message similar to this:

HTTP Error 403.4
Forbidden: SSL required. This error indicates that the page you are trying to access is secured with Secure Sockets Layer (SSL). In order to view it, you need to enable SSL by typing "HTTPs://" at the beginning of the address you are attempting to reach. Please contact the Web server's administrator if the problem persists.
If SSL is not enabled, and you enter `https://<server>/<instance>`, WebView automatically redirects you to `http://<server>/<instance>`. You will not see an error.

**Are They Using a Blank Password?**

Although it is possible to create an Active Directory user with a blank password, the WebView login requires a password. Users with blank passwords will be unable to access WebView.

**Has the IP Address Changed?**

If the IP Address for the WebView server has changed, WebView might be unable to contact Jaguar by the machine name, causing the login connection to fail and the Jaguar WatchDog to reboot Jaguar repeatedly.

To resolve this, set WebView to connect to Jaguar by the server’s external IP Address, as follows:

**Step 1** Navigate to the `jagconnection.properties` file.
This file is located at: `%JAGUAR%\html\classes\com\cisco\atg\jagconnection.properties`.

**Step 2** Open the file and look for the key `JAGCONNECT_JAGUAR_SERVER`. By default, it is set to blank.

**Step 3** Set that key to the machine’s external IP Address (not `127.0.0.1`).

**Has the Password Expired or the User Account Been Disabled?**

Try logging into a Windows machine to verify that the password and the account status of the user are still valid.

**Is Jaguar Working Correctly?**

See Jaguar Server Connection Fails After Restart, page 11-9.
Also see Jaguar Service Verification, page 11-9.

**WebView Database Messages at Login**

When you log in to WebView, you might see one of these messages:

- The WebView database is not up to date.
- The WebView database has been updated but the WebView application has not.

These messages occur when there is a mismatch between the version of the WebView application and the version of the WebView database schema.

This happens when the Admin Workstation hosting the WebView database has been upgraded, but the WebView component has not, or vice versa.
If you see either of these messages, verify that the distributor Admin Workstation hosting the WebView database and the WebView component have both been upgraded to the same version. See The WebViewVersion Table, page 5-8.

- The WebView database cannot be contacted. Saved Reports, Favorites, and Job Scheduler will not be available. Please contact your administrator.

This message occurs when the WebView database cannot be contacted (for example, the database server is down or SQLServer is not started). If you see this message, check the following:

- Is the Admin Workstation that hosts the WebView database running and is SQL Server running on that Admin Workstation?
- Does the WebView database (wvdb) exist on the Admin Workstation?
- Was the correct machine entered for the WebView Database Hostname during WebView installation?
- Does the Jaguar log show details about errors that WebView is receiving from SQL Server?

**WebView Supervisors Rights and Active Directory Account**

Supervisors have limited WebView rights that allow them to run Agent and Skill Group reports that are associated with the Agent Teams they supervise. In addition, Supervisors can run Call Type reports as long as they are not associated with a "Customer".

The facility for Supervisors to see how many calls are truly in queue (for Call Types), as well as to see and manage Service Levels, has been removed.

The workaround is to create a second Active Directory account for Supervisors who wish to be WebView users.

**WebView User Unable to Change Password**

A WebView password cannot be changed or updated from within WebView. It can only be changed or reset on an ICM workstation.

ICM users must be aware of the domain-security policy setting on password expiration. If it is anything other than never, a WebView user who does not log into an ICM workstation could have their password expire without being able to change it.

If a WebView user’s password expires, the user must either login into an ICM workstation or see the domain administrator to reset the password. If you do not know the domain-security policy setting, see your domain administrator.
Job Scheduler

Job Scheduler Does Not Work

Are Terminal Services Running on the Client?

Make sure there are no terminal services running on the machine where the scheduled job is going to be run.

Does the User Have Access to a Printer?

Make sure the user has access to a printer.

Does the User have Minimum Rights?

Verify that the local system account has minimum local security policy privileges.

To do this, follow this procedure:

Step 1
Click Settings > Control Panel > Administrative Tools > Local Security Policy.

Step 2
In the left tree, navigate to Local Policies > User Rights Assignment.

Step 3
In the right pane, locate each of these privileges:
- Act as part of the operating system
- Adjust memory quotas for a process
- Bypass traverse checking
- Create a token object
- Replace a process-level token

Step 4
For each privilege listed in Step 3, perform the following actions:
- Right-click the privilege and select Security...
- Click Add.
- If the local machine is not listed as being assigned the privilege, add the local machine account to the privilege and click OK.

Is ActiveX Enabled?

To view graphical reports and to use the WebView Job Scheduler, you must enable all ActiveX Controls and plug-ins in the browser’s Security Settings.

See Browser Setting for Trusted Sites, page 11-5 for the procedure to ensure that these settings are correct.

Is Fast User Switching Disabled on the Client?

Make sure that Fast User Switching (FUS) is disabled on the machine where the scheduled job is going to be run on.
Is the User Logged in When the Job is Triggered?

Make sure that the user is logged in at the time the job is scheduled to run and that only one user is logged in.

To check that only one user is logged in, open Task Manager and click Show processes from all users to verify that only one explorer.exe is running.

Is the WebView Server added to the Trusted Sites List?

Job Scheduler can also work incorrectly if the WebView server is not added to the Trusted Sites list on the browser. See Browser Setting for Trusted Sites, page 11-5.

Job Scheduler File Not Found Message

When you are using the Job Scheduler to run a report that is saved to a file, you might see a File Not Found message similar to this:

File Not found: c:\icm\e2\aw\sched\SchedRep-665630630.csv (The system cannot find the path specified.)

(The actual message is specific to the system you are running.)

This occurs if the IUSR_<machine_name> user does not have permission to create the temp directory in which scheduled reports are queued on the server.

The Microsoft operating system account, IUSR_<machine_name>, is a member of the Guests group and is used by the IIS Admin Service for anonymous requests and process accounts. IUSR is sometimes spelled IUSER and means Internet User. The WebView JobScheduler uses this account for processing its jobs.

If the IUSR_<machine_name> user is not explicitly given different permissions, then it will operate with the permissions of the Everyone group. The Everyone user might not have access to create the C:\icm\<instance_name>\aw\sched (Job Scheduler folder), where the scheduled jobs are stored.

Even though giving the IUSR_<machine_name> user permission to create the Job Scheduler folder will resolve this issue, incorrect permissions inside the C:\icm directory are indicative of more serious problems.


Job Scheduler Upgrade Does Not Migrate Jobs to New Server

Customers who upgrade to Release 7.0(0) using the technology refresh model might see scheduled reports on the WebView screen but find that the report is not actually scheduled to run on the server.

Refer to the ICM Upgrade Guide for Cisco ICM/IPCC Enterprise & Hosted Editions for the procedure to move scheduled report jobs to the new WebView server.
Reports and Templates

3000 Row Limit

WebView reports display a maximum of 3000 rows.

When you create a WebView report, if your selections of items and date range return more than 3000 rows of data, you will see a warning message. WebView generates the report, but the data is truncated at the 3000th row.

The summary columns will correctly add the data that appears in the report; however, the data in a particular grouping that appears on the report may not be all of the data in the database for that grouping.

To avoid this restriction, limit the items or shorten the date range for the report. You can also create a custom report that aggregates at a higher level.

1000 Item Selection Limit

When you create a WebView report, if your selection of items exceeds 1000, you will see the following warning message:

“You can select a maximum of 1000 items.”

To avoid this restriction, limit the selection of items to 1000. If you are generating an agent report, you can select from a list of agents; if you are running a skill group report, you can select from a list of skill groups, and so forth.

Agent Data Does Not Appear in Reports

You do not see agent data in a report until you enable the flow of agent data from a specific peripheral to a specific real-time distributor.

Use the following procedure to enable agent data.

Step 1  In the ICM Configuration Manager, open Start > Programs > ICM Admin Workstation > Configuration Manager > Peripherals > PG Explorer.

Step 2  In the PG Explorer, select the peripheral to which an agent(s) is assigned.

Step 3  Select the Peripheral tab.

  • Review the Client Type.

    If the peripheral’s client type is CallManager/Soft ACD, you must select Default desk settings in the Peripheral tabs. Otherwise, skip this step.

  • Review the Agent Desk Settings

    Agent desk settings are settings for an IPCC agent’s phone or PC screen that are defined in the ICM database. Other types of agents have these settings defined in the ACD.

    If NONE is the only option in the selection list, you need to create desk settings. To create desk settings, use the ICM Configuration Manager’s Agent Desk Settings List tool.

Step 4  Select the Agent Distribution tab.

Agent distribution is the flow of agent data from a specific peripheral to a specific real-time distributor.
• Check **Enable agent reporting**.
• Enter any needed agent distribution entries.

You can stop the flow of all agent real-time data to a distributor when you are not viewing agent real-time reports.

---

**Blank Dailer Port Status Real-Time Report**

If the Dailer Port Real-Time report for Cisco Outbound Option (dialpr01) is always blank in WebView, check the following:

* Does the `Dialer_Port_Real_Time` table in the database on the distributor Admin Workstation exist and contain data?
* What is the setting of this registry key in Cisco ICM Blended Agent:
  
  HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\<cust_inst>\Dialer\RTPortFeedDisable

  The `Dialer` registry entry for `RTPortFeedDisable` controls whether the status messages go to the Campaign Manager. By default, this option is set to `true`, which means that status messages are not sent. The purpose this default is to minimize bandwidth between the Dialer and Central Controller.

  This key setting is dynamic. After the `RTPortFeedDisable` value is set to 0, the Dailer Port Real Time report in WebView shows the current status of every telephone line for every dialer in Outbound Option.
Blank Pages When Report is Rendered

If WebView returns a blank page when you run a report, you might need to change one or more browser settings.

- **Trusted Sites**
  If WebView Reporting is installed on a Windows 2003 Server, follow the procedure to make sure that the WebView server is added as a Trusted Site. See Browser Setting for Trusted Sites, page 11-5.

- **Friendly HTTP error messages**
  You might also see a blank page if your browser is configured to mask the text of error messages. Follow the procedure documented in Ensure display of WebView server error messages, page 1-8 to ensure that you see an error message, and not a blank page.

Caltype Items in Reports

To ensure that users see only the appropriate call types:

- In Configuration Manager, associate the user with a Customer so that the user sees only the call types for that Customer.
  In Release 7.0, with Active Directory, WebView users do not have to be added in the User List tool. However, to restrict a user to see only those call types associated with a certain customer, you must add the user in the User List tool and associate the user with the appropriate customer.

- For Service Providers with multiple customers, change the adminui.properties for ENABLE_CALTYP_CUSTOMER_FILTER from the default (which is FALSE) to TRUE. This prevents each customer from seeing all call types.

Date Formats are Incorrect or Historical Reports do not show for a Specified Time Period

If WebView is initially installed with a language selection that uses one date format (for example, installed for French DD/MM/YY) and is subsequently reinstalled with a language selection that uses another date format (for example, reinstalled for English, MM/DD/YY), then the date format used by WebView may be wrong. You might also find that WebView historical reports do not show for a specified time period, even though calls occurred during that time period.

In this case, the date format for the changed language might no longer match the date format in the EAServer.ini file. Follow this procedure to change the date format field:

| Step 1 | Navigate to <drive>:\Program Files\Sybase\EAServer\PowerBuilder. |
| Step 2 | Open the pdodb.ini file. |
| Step 3 | In the [MSSQLSERVER_DATETIME] section, replace instances where the date format is incorrect for your locale. (This is, replace yyyy-dd-mm with yyyy-mm-dd, or vice versa.) |
| Step 4 | Save the change. |
| Step 5 | Restart Jaguar. |
Error on Attempting to Select a WebView Template

If you uninstall Jaguar, in addition to removing the Jaguar files, you remove any WebView files that are installed in the Jaguar directory. If you then reinstall Jaguar and try to run WebView and select a template, you might see an error message similar to this:

```
org.omg.CORBA.OBJECT_NOT_EXIST: minor code: 0 completed: No
```
Rerun ICM Setup in Upgrade All mode to reinstall the missing WebView files.

Error Retrieving Information from the Web Server

This error appears if there is a timeout when Jaguar attempts to create the cache file on the item page.

There was an error while retrieving information from the Web Server. Please try again and contact your WebView administrator for further details.

Possible solutions are to:

- Run the report again.
- Reduce the number of Items you select for the report.
- Try again when there is less load on WebView servers (Jaguar) and/or on the ICM Admin Workstation database.

Errors Running Reports

There was an error running your report. Please try again and contact your WebView administrator for further information.

A message similar to this indicates a SQL error — either because of the query or other unknown factors. The report appears with no data, and this error is displayed. Refer to the Jaguar.log and to the NewAtlanta.log for more detailed information.

To resolve this error, run the report again.

Graphical Reports Do Not Print

With the operating systems Windows XP SP2 and Windows 2003 SP1, you might see an error when you schedule a graphical report to print.

To resolve this, change the browser Internet options to allow active content.

Step 1 From the browser menu, select Tools > Internet Options.
Step 2 Click the Advanced tab.
Step 3 Scroll to the Security options.
Step 4 Check Allow active content to run in files.
Graphical Reports Do Not Work Correctly

There are two possible reasons for this. The reasons and the solutions are applicable to Job Scheduler as well as graphical reports.

Is ActiveX Enabled?

To view graphical reports and to use the WebView Job Scheduler, you must enable all ActiveX Controls and plug-ins in the browser’s Security Settings.

See page 11-15 for the procedure to enable ActiveX Controls.

Is the User Logged in When the Job is Triggered?

Header Truncated in French Reports

If your WebView is localized for the French language, and if the header of reports is truncated or cut off, select a smaller text size in the browser (View > Text Size).

Historical Reports Do Not Work Correctly

This section presents several issues you might encounter with historical reports.

Historical Reports Fail

The following are reasons this can occur.

Is RAM too low?

Large reports might fail if the memory (RAM) allocated to the Java Virtual Machine is set too low in the New Atlanta ServletExec. The default setting is sufficient for normal reporting usage. If the setting is too low, there can be an out-of-memory error in the browser and errors in the ServletExec logs.

By default, the minimum setting allocated is 32MB (32768 KB). The maximum is 256MB.

You can verify and change the settings by opening the ServletExec Administration page from the server. This is located at http://localhost/servlet/admin.

Is TEMPDB large enough?

If large historical reports do not return data, the tempdb database might not be sufficiently large to handle the demand imposed by the queries.

Tempdb is a system database that SQL Server uses to store temporary tables and temporary stored procedures. It is created when SQL Server is installed. By default, it is set to an initial size of 50 MB with a maximum of 2 GB, and Autogrow is turned on.

If your contact center operations require that you run monthly and yearly historical reports for many items, you might consider increasing the initial size of tempdb.

Refer to the ICM Administration Guide for Cisco ICM Enterprise Edition for information on using the ICMDBA tool to change the size of the tempdb.
Historical Reports Saved with Fixed Date Do Not Work Correctly

There exists a condition where you successfully generate an historical report with a fixed date range, then save the report and rerun it again to find that:

- No data is returned, and
- The date range at the top of the report has the year 1900 or has the month and day reversed.

This occurs when the logon user account for the Jaguar service has an incorrect short date format. Jaguar expects the format m/d/yyyy, regardless of regional settings. If this format has been changed, then Jaguar does not interpret the WebView database correctly.

To check for and set this value correctly:

---

**Step 1** On the WebView server, open the service control panel and record the logon account for the Jaguar service. It must be of the form %DOMAIN%\jag%HOSTNAME%.

**Step 2** Using a domain utility, set the password of the jaguar user to a known value.

**Step 3** On the WebView server, log off the current user and log in with the jaguar user account.

**Step 4** Click Start > Control Panel > Regional and Language Options.

**Step 5** In the regional options, set the short date format to m/d/yyyy. Click OK and log off.

**Step 6** Log back into the WebView server with a regular user account and verify that you can now successfully run your saved historical reports with fixed dates.

---

Historical Reports Slow the System

Large historical reports can take extra time to create depending on the amount of data. Large numbers of historical reports can also slow down the simultaneous creation of real-time reports.

Use the Job Scheduler to create large historical reports during the evening hours or when the system is not in heavy use.

Pages do not Display Correctly

You might see errors on the pages that WebView generates such as Java errors and errors that ServletExec cannot write to the page. You might also see text strings that appear to be incorrect or missing and malformed pages (for example, graphics are missing or colors are wrong.)

There are several possible resolutions to these page display errors.

- Check that the World Wide Publishing service is running.
- Rerun ICM Setup in Upgrade All mode to reinstall missing WebView files.
- **Delete compiled pages**
  
  Because ServletExec compiles pages before displaying them, if some files have changed since they were last compiled, the display can be a mixture of new and old pages.

  Resolve this issue by deleting the compiled pages, which forces ServletExec to recompile all of the pages.

  To delete the compiled pages:
– Delete this entire folder: C:\Program Files\New Atlanta\ServletExec ISAPI\ServletExec Data\default \default-app\pagecompile.

– Close the browser and run the reports again.

• Add the WebView server to Trusted Sites

Pages can also display incorrectly if the WebView server is not added to the Trusted Sites list on the browser. See Browser Setting for Trusted Sites, page 11-5.
Private and Favorite Reports Not Displayed After Upgrading

Users who are not migrated correctly to Active Directory during an upgrade might not see their Favorites or their private reports in WebView.

Each object created in the Active Directory is assigned a globally unique identifier (GUID). Users created in AD have a UserGuid record in the USER_GROUP table in the Admin Workstation database. This UserGuid in the Admin Workstation database populates tables in the WebView database; for example, the t_Report, t_UserPreferences and t_PrintJobs tables.

Therefore, to resolve this issue:

- Add the users to Active Directory.
- Use the Domain Conversion Utility to import the users into the Admin Workstation database.
- Run the wvusersync utility to synchronize the Admin Workstation database and the WebView database.

Note  The utility uses integrated authentication to connect to the database, and the user who invokes the utility must have access to both databases.

Follow this procedure to run wvsync:

**Step 1**  Navigate to the `<icm>\web\webview\wvdb` directory on the distributor Admin Workstation where the WebView database is located.

**Step 2**  Locate and run `wvusersync.bat`. The output is appended to `c:\temp\wvusersync.log` with a datetime stamp.
Saved Reports Do Not Work

If a reporting user cannot access a saved report, and if the saved report was based on a custom template, the name of the custom template may have changed.

If the saved report was based on a Cisco template, and you upgraded WebView, then the template may have been deleted or moved to a different reporting category.

In these situations, the reporting user must create a new saved report based on the renamed or relocated template.

Note

This issue is specific to upgrades from Release 4.6.2. No templates were deleted in Releases 5.0, 6.0, or 7.0.

Time difference between ICM Record and WebView Report

There is a potential for WebView report times to differ from the ICM records.

This can occur for these reasons:

• The system time on the distributor AW and on the ICM Central Controller are not synchronized.
• The Windows Time Service is not enabled.

See Checking WebView AW Time Synchronization, page 7-2 for details.
Symbols

- .PBL files 8-2, 8-6
- .SRD files 8-2, 8-6

Numerics

- 3000 row limit 11-17

A

Active Directory 10-2
- and WebView users 3-5, 11-12
- issues after upgrade 11-24
- Jaguar Server account rights 5-7
- user authentication 10-2
- USERGUID 11-24
- user name formats 3-7, 4-4, 10-3, 11-12
- WebView DLG 10-2

ActiveX Controls 9-5, 11-15, 11-21

administrator
- and AD domain rights 10-2
- creating 3-5
- defined iii-ix
- domain security 3-6, 4-2
- log in 9-1
- rights for third-party tool installation 2-2
- rights for WebView installation 3-2

adminui.properties 6-5, 8-3, 9-3

Admin Workstation
- co-resident with WebView server 1-4, 1-12
- database 1-2, 1-4, 3-3
- installation errors 11-7

language selection 1-18
primary and secondary 1-9, 1-15, 5-3
requirements 1-4
separate from WebView server 1-12
time synchronization 7-2
agent data 11-17
Agent Names field 1-17
AllowAdminLogin 9-1
ASCII character support 1-17
authentication 10-4
AW see Admin Workstation

B

BOM see ICM Bill of Materials

browser
- cache settings 1-8
- language setting 1-19
- locales for date format 7-3
- security settings 11-15, 11-21
- troubleshooting 11-19
- Trusted Sites 1-7, 1-15

caching
- browser settings 1-8
- customer call type filtering 8-3
- enabling and disabling 8-3, 8-4
- properties 9-4
- purge time 8-4
- refresh 8-3
- call types 8-3, 11-19
Central Controller time zone 7-2
certificate
  from CA 10-4
  saving locally 10-5
  self-signed 10-4
  verifying 10-6
  see also SSL
Cisco CEM and CCS components 2-4
Cisco Security Agent 2-4, 2-6, 3-2
Cisco templates 1-2, 8-2
  regenerating with PATCHPBL 8-6
client workstation requirements 1-7
collation designators 1-17
creating
  failover WebView database 5-6
  users 10-2
custom templates 1-2, 8-6
  changing names 11-25
  refreshing cache 8-3

D

databases 1-2, 1-4
  see also WebView database, ICM real time database, HDS
date formats 1-18, 7-3, 11-19, 11-22
deleting page compiles 11-22
deployment model
  hosted 1-16
  large-customer 1-12
  standard 1-2
Description field 1-17
document conventions iii-xi
Domain Manager 3-5, 4-2, 11-12
domain name 3-7, 4-4

E

EAServer 1-10, 2-6, 6-1

logs 11-4
  monitoring 6-5
  restarting 6-5
  troubleshooting 11-7
  uninstalling 2-10, 11-10
  see also Jaguar Server
enabling and disabling
  agent data 11-17
  basic caching 8-3
  encryption 10-6
  Event Viewer 9-2
  Jaguar Watchdog 6-5
  SSL encryption 10-6
  supervisor caching 8-4
event
  changing configuration 10-6
  defaults 10-4
Error 2221 11-7
error messages
  changing Jaguar password 11-7
  running reports 11-20
  selecting WebView template 11-20
  third-party software installation 2-7
  WebView database 11-13
  Windows Scripting Host 11-9
Event Viewer
  enabling and disabling 9-2

F

Fast User Switching 11-15

G

Global Table 5-8
  graphical reports
    property settings 9-4
    troubleshooting 11-21
H

HDS 1-2, 1-5, 1-9, 3-1
historical reports 1-2
troubleshooting 11-21
hosted deployments 1-16
http 10-4
HTTP 403.4 error 11-12
https 1-2, 3-7, 3-8, 4-4, 10-4, 11-12

I

ICM
Active Directory model 10-2
Configuration Manager User List 3-5, 4-2, 10-2
domain 10-2
Time Synchronization 7-2
ICM Bill of Materials iii-x, 1-4
ICM Setup
administrator rights 10-2
language selection 1-17
SSL configuration 10-4
Upgrade All mode 2-10, 11-12, 11-22
IIS 1-6, 1-9, 1-10
troubleshooting 11-7
InfoMaker 1-2, 2-3
installation
WebView from ICM Setup 3-3
WebView third-party software 2-6
IP Address for WebView server 11-13

J

ejagconnection.properties 9-8, 11-7, 11-13
Jaguar 1-10, 6-1
and WebView IP address 11-13
changing Admin Password 6-1
error when changing password 11-7
Server connections 6-2, 9-8
Jaguar log file 3-8, 6-3
deleting 6-3
setting size 6-3
Jaguar Server 2-6, 6-1
AD rights to WebView database 5-7
connection properties 9-8
restarting 11-9
troubleshooting 11-9
verifying 11-9
see also EAServer
Jaguar Watchdog 1-7, 6-5
collection 6-5
disabling 6-5
executing batch file 6-6
logs 6-7
properties 9-5
JDK log 11-4
Job Scheduler
and Trusted Sites 11-16
and user login 11-16
for large reports 11-22
logs 11-4
troubleshooting 11-15

L

language selection 1-17, 1-18, 1-19
large-customer deployment 1-12, 5-5
Licenses 11-10
locales 7-3, 9-9
localization 1-17, 9-9
logger time zone 7-2
log in 3-7, 4-4
https protocol 10-4
troubleshooting 11-12
logs 11-4
Jaguar 6-3, 11-4
Jaguar Watchdog 6-7
New Atlanta ServletExec 11-4
Index

third-party installation 2-7, 11-4

N
New Atlanta ServletExec 1-11, 2-4, 2-6, 8-3, 11-5
  additional licenses 11-10
  logs 11-4
  troubleshooting 11-5

O
Outbound Option Support 3-3

P
page compiles 11-22
password 3-6, 3-7, 4-2, 4-4, 11-13, 11-14
  blank 11-13
  Jaguar 6-1, 11-7
PATCHPBL 8-6
PowerBuilder Virtual Machine 2-3
PPB050.PBL 8-6
Print Jobs Table 5-9
Property Files
  adminui.properties 8-3, 9-3
  jagconnection.properties 6-2, 9-8
  WebView.properties 9-9
  wvLocale.properties 9-9

R
real-time reports 1-2
Reason Code field 1-17
registry settings
  AllowAdminLogin 9-1
  Event 9-2
reports
  blank pages 11-19
  date values in 7-3
errors when running 11-20
footer properties 9-7
graph properties 9-4
Job Scheduler 11-22
missing agent data 11-17
saved 5-11, 11-25
time zones 7-1
troubleshooting 11-22
ReportTable 5-11
requirements
  Admin Workstation 1-4
  ICM Bill of Materials iii-x
  third-party licenses 11-10
  WebView client 1-7
  WebView server 1-6

S
saved reports 5-11, 11-25
security
  Active Directory 10-2
  browser 11-5
  Cisco Security Agent 2-4, 2-6
  domain security setting 3-6, 4-2
  SSL 10-6
  user passwords 3-6, 4-2
SQL collation designators 1-17
SQL Server database 1-12, 3-8
SSL 10-4
  installation options 3-3
  properties 9-6
  Security Alert message 10-5
  self-signed certificate 10-4
  see also certificate
SSL Encryption Utility 10-6
standard deployment 1-2, 1-12, 5-4
Sun JDK 2-6
supervisor caching 8-4
supervisors 3-5, 3-6
Index

System IPCC  iii-x, 2-9, 3-5, 3-8, 4-2

T

templates  1-2, 8-6
  and upgrades  11-25
  changing custom template names  11-25
  custom and Cisco  1-2
  deleted or replaced  11-25
  error when selecting  11-20
  location  11-25
  troubleshooting  11-25
third-party software  1-6, 2-6
  administrator rights  2-2
  applications on CD  2-3
  debugging  11-6
  disk space requirements  2-4
  installation errors  11-7, 11-9
  installing  2-6
  location and sequence of installation  2-1
  log  2-7, 11-4
  troubleshooting  11-7
  uninstalling  11-7, 2-9
time and time zone
  dependencies  7-3
  Time Zone Date field  7-2
  troubleshooting  11-25
  WebView server synchronization  7-2
timeout  9-3
troubleshooting
  additional tips  11-1
  browser  11-19
  changing Jaguar Admin password  11-7
  EAServer installation  11-7
  enabling agent data  11-17
  graphical reports  11-21
  IIS  11-7
  initial steps  3-8
  Job Scheduler  11-15
  report performance  11-22
  running reports  11-20
  selecting WebView templates  11-20
  templates  11-25
  verifying Jaguar Server  11-9
  WebView logon  11-13
  WebView password  11-14
  Windows Scripting Host error  11-9
Trusted Sites  1-7, 11-5, 11-16

U

uninstalling
  EAServer  2-10
  old versions of Jaguar  11-10
  third-party software  1-13, 2-9
  WebView  3-8
USERGUID  11-24
User Preferences Table  5-12
users
  Active Directory accounts  10-2
  Active Directory name format  10-3
  authentication  10-4
  passwords  3-6, 4-2
  reporting users  1-2
  setting up  3-5, 10-2
  user name format  3-7, 4-4

W

WebView
  Active Directory authentication  10-2
  adminui.properties file  9-3
  client  1-7
  co-locating with CEM or CCS  2-4
  deployment models  1-12
  language selection  1-18
  large-customer deployment  1-12
  mixed-language deployment  1-16
overview 1-2
password 11-14
setting properties 9-3
SSL defaults 10-4
standard deployment 1-2
timeout 9-3
troubleshooting 11-13
uninstalling 3-8
WebView.properties 9-9
WebView database 1-2, 1-5, 3-3, 5-2
Active Directory rights 5-7
backup 5-6
error messages 5-5, 11-13
failover 5-3, 5-6
in large-customer deployment 5-5
in standard deployment 5-4
multiple 5-6
redirecting 5-7
shared by multiple servers 5-3, 5-5
tables 5-8
version 5-8
WebView installation iii-ix, 1-7, 3-3
upgrading iii-ix
WebView login
and Job Scheduler 11-16
errors 11-13
https protocol 3-7, 4-4, 10-4
troubleshooting 3-8
WebView reports 1-2
date format 7-3
enabling agent data 11-17
error when selecting template 11-20
supported locales 7-3
upgrade issues 11-24
WebView server 1-5
and third-party software 2-1
capacity guidelines 1-6
co-resident with Admin Workstation 1-4, 1-12
deployment models 5-5, 5-6
installing multiple 1-12
IP address 11-13
localization 9-9
property file settings 9-1
registry settings 9-1
requirements 1-6
time synchronization 7-2
WebView troubleshooting 3-8
WebView URL 3-5, 3-7, 4-4, 10-4
WebView users
creating an administrator 3-5
creating a user 3-5, 10-2
password expires 11-14
reporting users 1-2
troubleshooting log in 11-12
username and password 3-7, 4-4
WebViewVersion Table 5-8
Windows Scripting Host error 11-9
Windows Time Service 7-2, 11-25
World Wide Web publishing service 3-8, 11-11
wvLocale.properties 7-3, 9-9
wvsync utility 11-24