

# Symphony Marimba Client Automation CMS and Tuner User Guide



Supporting

Symphony Marimba Client Automation CMS version 9.0.00

November 2015

## Contacting Symphony Teleca Customer Support

You can obtain technical support by contacting Customer Support by telephone or e-mail. We are available 24/7/365:

Please send an e-mail to: [CustomerSupport@Symphonyteleca.com](mailto:CustomerSupport@Symphonyteleca.com) OR

Call us at +1 214 396 0493 or US Toll Free Number +1 855 394 1543

Before contacting Symphony Teleca support

Please gather the following information and have it ready before contacting Symphony Teleca.

This will help us service your request immediately:

Marimba channel version for each module being used

Sequence of events leading to the issue

Error messages received along with the time and date that you received them

Environment details (number of transmitters, type of transmitters, number of endpoints, Operating System from servers and endpoints, Database version)

Details about the problem

Screenshots of errors

Attachments of relevant logs and configuration files

0

© Copyright 2015 Symphony Teleca, Corporation or its subsidiaries. All rights reserved. All information contained in this document is confidential and proprietary to Symphony Teleca, Corporation and may not be disclosed, reproduced, used, modified, made available, used to create derivative works, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, by or to any person or entity without the express written authorization of Symphony Teleca, Corporation. In consideration for receipt of this document, the recipient agrees to treat this document and its contents as confidential and agrees to fully comply with this notice. This document refers to numerous products by their trade names. In most, if not all, cases their respective companies claim these designations as Trademarks or Registered Trademarks. This document and the related software described herein are supplied under license agreement or nondisclosure agreement and may be used or copied only in accordance with the terms of such agreement. The information in this document is subject to change without notice and does not represent a commitment on the part of Symphony Teleca, Corporation. Contact Symphony Teleca, Corporation Customer Support to verify the date of the latest version of this document. The names of companies and individuals used in the sample database and in examples in the manuals are fictitious and are intended to illustrate the use of the software. Any resemblance to actual companies or individuals, whether past or present, is purely coincidental. Symphony Teleca, Corporation reserves all copyrights, trademarks, patent rights, trade secrets and all other intellectual property rights in this document, its contents and the software described herein.

### **Restricted rights legend**

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Section 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time.

## **Customer support**



# Contents

Preface . . . . .	19
Audience and document scope . . . . .	19
Accessing product documentation. . . . .	19
Using the documentation channel. . . . .	20
Searching across the entire Symphony Marimba Client Automation documentation set . . . . .	20
Related documentation . . . . .	22
What is new in this guide for Marimba 9.0.00? . . . . .	24
Contact information. . . . .	25
Section I    Introduction and Overview . . . . .	27
Chapter 1    Introduction . . . . .	29
How to read this document. . . . .	30
Using help . . . . .	31
Chapter 2    Profiles and administration tools . . . . .	33
What are profiles? . . . . .	34
What are administration tools? . . . . .	34
When to use profiles versus administration tools . . . . .	34
Administration tool settings override profile settings . . . . .	35
Examples of when to use administration tools . . . . .	35
Updating profiles . . . . .	35
Updating an existing profile . . . . .	36

Replacing a profile . . . . .	37
<b>Chapter 3 Infrastructure security overview . . . . .</b>	<b>39</b>
<b>Passwords . . . . .</b>	<b>40</b>
<b>Using SSL . . . . .</b>	<b>40</b>
Using server-side certificates . . . . .	41
Using client-side certificates . . . . .	41
Using SSL-enabled LDAP servers . . . . .	42
Using SSL-enabled CMS . . . . .	43
Distributing root certificates securely . . . . .	44
Using mixed-mode SSL . . . . .	44
Using wildcard certificates . . . . .	45
<b>Trusting channel content . . . . .</b>	<b>45</b>
Using trusted transmitters . . . . .	46
Using channel signing . . . . .	46
Using security tuner properties . . . . .	47
Signing installers . . . . .	48
<b>Setting up tuners to use SSL . . . . .</b>	<b>49</b>
<b>Enabling SSL across multiple tuners in the infrastructure. . . . .</b>	<b>52</b>
To deploy a certificate using a profile . . . . .	52
To package and deploy certdb . . . . .	53
<b>Section II System Settings . . . . .</b>	<b>57</b>
<b>Chapter 4 Common Management Services basics . . . . .</b>	<b>59</b>
<b>CMS overview. . . . .</b>	<b>60</b>
<b>Console and command-line interfaces . . . . .</b>	<b>60</b>
<b>System settings overview . . . . .</b>	<b>61</b>
Configuring System Settings before using applications . . . . .	62
<b>Chapter 5 Getting started with CMS and the console . . . . .</b>	<b>65</b>
<b>Logging in to the console for the first time . . . . .</b>	<b>66</b>
<b>Logging out of the console . . . . .</b>	<b>66</b>
<b>Console navigation . . . . .</b>	<b>67</b>
Switching between applications . . . . .	67

Viewing status information . . . . .	68
<b>The Getting Started page . . . . .</b>	<b>68</b>
Setting console preferences . . . . .	68
Roles and system settings information . . . . .	69
Customer support and documentation links . . . . .	69
<b>CMS and cookies . . . . .</b>	<b>69</b>
<b>Chapter 6 General settings . . . . .</b>	<b>71</b>
<b>Managing applications . . . . .</b>	<b>72</b>
Viewing information about applications . . . . .	72
Starting and stopping applications . . . . .	72
Updating applications . . . . .	73
Subscribing to new applications . . . . .	75
Removing applications . . . . .	76
Setting the user timeout . . . . .	77
Setting the browser access port and bind address . . . . .	78
What is the browser access port? . . . . .	78
What is the bind address? . . . . .	78
Changing the browser access port and bind address . . . . .	78
Configuring the console to use SSL . . . . .	79
Properties for supplying SSL client-certificate information . . . . .	81
Working with performance settings . . . . .	81
Managing log files . . . . .	83
Log files for the applications . . . . .	83
Setting where log files are stored . . . . .	84
Setting the log file rolling policies . . . . .	85
Configuring email notifications . . . . .	85
Configuring FTP upload settings . . . . .	86
Restarting CMS and the console . . . . .	87
Updating CMS and the console . . . . .	88
Configuring Deployment Manager Integration settings . . . . .	88
<b>Chapter 7 Multi-Tenancy . . . . .</b>	<b>91</b>
<b>Introduction . . . . .</b>	<b>93</b>
What is a tenant? . . . . .	93
Who is a Super Administrator? . . . . .	94

Key features . . . . .	94
Support for Multi-Forest. . . . .	95
Advantages of Multi-Tenancy. . . . .	95
Default environment in 9.0.00 . . . . .	96
What happens when you upgrade to 8.5.00?. . . . .	96
Architecture of Multi-Tenancy . . . . .	97
How tenants are managed? . . . . .	97
How to use the Application Permissions tab to specify access permissions for tenant administrators to web application channels . . . . .	97
Different types of deploying Marimba infrastructure . . . . .	98
Tenant specific properties . . . . .	99
Using command-line to perform operations in a Multi-Tenant environment	100
Using the database in a Multi-Tenant environment . . . . .	100
Schema Manager Channel changes to support Multi-Tenancy . . . . .	102
Multi-Tenancy changes in Infrastructure Administration . . . . .	105
Different scenarios while deploying Marimba 9.0.00 . . . . .	106
Upgrading to 9.0.00 . . . . .	107
Using 9.0.00 for the first time - a fresh installation . . . . .	108
Deploying Marimba 9.0.00 on cloud . . . . .	109
Logging on to CMS Console in Marimba 9.0.00 . . . . .	112
User Roles . . . . .	113
Role of Emergency Administrator or Super Administrator . . . . .	113
The role of Primary Administrator . . . . .	114
User roles in a Multi-Tenancy . . . . .	115
Configuring a tenant. . . . .	118
Workflow of configuring a tenant . . . . .	118
Chapter 8	
User authentication and roles . . . . .	126
User authentication overview . . . . .	127
What are user roles? . . . . .	127
Selecting the user authentication type . . . . .	128
Managing the local user database . . . . .	130
Using a local user database or a directory service. . . . .	130
Adding users to the local user database . . . . .	131
Searching for users in the local user database . . . . .	131
Changing passwords for users in the local user database. . . . .	132

	Changing roles for users in the local user database . . . . .	133
	Removing users from the local user database . . . . .	133
	Finding logged in users in the local user database . . . . .	134
	<b>Using smartcard authentication for CMS.</b> . . . . .	134
	Requirements . . . . .	135
	To enable smartcard authentication . . . . .	135
	To use smartcard authentication . . . . .	135
	<b>Mapping roles to groups in a directory service</b> . . . . .	137
	<b>Setting an emergency administrator password</b> . . . . .	139
<b>Chapter 9</b>	<b>Configuring data sources</b> . . . . .	140
	<b>About the Java Kerberos system</b> . . . . .	141
	Prerequisite . . . . .	142
	<b>Managing directory services</b> . . . . .	145
	Adding or editing a directory service . . . . .	145
	Removing a directory service . . . . .	151
	Using automatic discovery for Active Directory . . . . .	152
	Advanced settings for the directory service . . . . .	153
	Using the base DN and bind DN . . . . .	154
	Permissions required for the bind DN . . . . .	156
	Changing the bind DN password . . . . .	156
	Setting up multiple directory services for failover . . . . .	157
	<b>Managing databases</b> . . . . .	157
	Adding or editing a database . . . . .	158
	Removing a database . . . . .	159
	<b>Synchronizing data from the directory service with the database</b> . . . . .	160
	<b>Configuring the CMS for integration with a NAP database</b> . . . . .	162
<b>Chapter 10</b>	<b>Setting up access control lists</b> . . . . .	163
	<b>What are access control lists?</b> . . . . .	164
	<b>Target view and user/group view</b> . . . . .	165
	<b>Overview of targets</b> . . . . .	166
	Browsing targets . . . . .	167
	Searching for targets. . . . .	167
	<b>Assigning permissions for ACLs</b> . . . . .	170
	Setting target permissions for ACLs . . . . .	171

Setting user and group permissions for ACLs . . . . .	172
<b>Assigning permissions for applications</b> . . . . .	174
Working with Policy Manager permissions . . . . .	174
Working with Report Center permissions. . . . .	175
Setting target permissions for applications . . . . .	176
Setting user and group permissions for applications . . . . .	178
<b>Deleting permissions for ACLs and applications</b> . . . . .	180
Deleting target permissions. . . . .	180
Deleting user and group permissions. . . . .	181
<b>Deleting ACL users</b> . . . . .	182
<b>Inheritance of permissions</b> . . . . .	183
 Chapter 11 Action Request System settings . . . . .	187
<b>Configuring the AR settings</b> . . . . .	188
<b>Configuring for the AR database</b> . . . . .	189
 Chapter 12 Working with web services . . . . .	191
<b>Viewing the web services</b> . . . . .	192
<b>Changing the service status</b> . . . . .	192
<b>Publishing web services to the Atrium Web Service Registry</b> . . . . .	193
 Chapter 13 Troubleshooting system settings . . . . .	195
 Chapter 14 Infrastructure Status Monitor . . . . .	201
<b>Configuring the Infrastructure Status Monitor</b> . . . . .	203
<b>Viewing the Infrastructure Status Monitor</b> . . . . .	207
Dashboard tab . . . . .	207
Server Component Status and Client Component Status . . . . .	210
Replication Status (Not In Sync) . . . . .	210
SNMP Alerts . . . . .	210
Critical Server Component Status . . . . .	211
<b>Viewing component tabs</b> . . . . .	211
Master tab . . . . .	211
Mirror tab . . . . .	212
Repeater tab . . . . .	213
Proxy tab . . . . .	214

Client tab . . . . .	215
CMS tab. . . . .	217
Health Status page . . . . .	218
Creating repeater groups and viewing group statistics. . . . .	219
Viewing audit log entries . . . . .	220
Filtering log entries . . . . .	220
Using the audit log table controls . . . . .	221
Configuring settings (Setting tab) . . . . .	221
Configuring the logging plug-in. . . . .	221
Defining component health . . . . .	220
Configuring email notifications . . . . .	223
Configuring vPro settings . . . . .	225
Configuring vPro agent watchdog settings for Infrastructure Status Monitor	225
Configuring the maximum number of concurrent threads to handle vPro agent watchdog settings in ISM. . . . .	225
Setting display preferences . . . . .	225
Using a custom channel to collect and display customized stats attributes in ISM . . . . .	227
Overview of implementing the custom channel . . . . .	227
Prerequisites . . . . .	227
Creating the custom channel . . . . .	228
Publishing the custom channel . . . . .	232
Configuring the database. . . . .	233
Configuring the tuner to send custom stats data . . . . .	238
SNMP alerts . . . . .	242
Viewing the status of deployed jobs in ISM dashboard and using Report Center query . . . . .	245
<b>Section III Tuner Administration . . . . .</b>	<b>247</b>
<b>Chapter 15 Tuner basics . . . . .</b>	<b>249</b>
<b>What is a tuner? . . . . .</b>	<b>250</b>
Tuner icon behavior. . . . .	250
<b>What are channels and packages? . . . . .</b>	<b>250</b>
<b>Tuner installation directory. . . . .</b>	<b>251</b>
<b>Tuner workspace directory . . . . .</b>	<b>252</b>

Checking for tuner workspace corruption . . . . .	254
<b>What is Tuner Administrator? . . . . .</b>	<b>255</b>
<b>Administering a tuner . . . . .</b>	<b>256</b>
Browser-based interface (console) . . . . .	256
Profiles . . . . .	256
Command-line interfaces . . . . .	257
<b>64-bit Tuner . . . . .</b>	<b>257</b>
Introduction . . . . .	257
Upgrade path . . . . .	258
Fallback Mechanism. . . . .	259
Java Heap and PermGen settings for 64-bit Tuners. . . . .	260
<b>Marimba over Internet. . . . .</b>	<b>261</b>
 Chapter 16	
Getting started with Tuner Administration . . . . .	263
Prerequisites before using Tuner Administration . . . . .	264
General process for administering a tuner . . . . .	265
Previewing and applying configuration settings . . . . .	265
Starting and stopping tuners . . . . .	268
Logging in to and out of Tuner Administrator . . . . .	269
Using roles to limit access to Tuner Administrator features . . . . .	269
Logging in to Tuner Administrator . . . . .	270
Logging out of Tuner Administrator . . . . .	271
Operations for one tuner versus multiple tuners. . . . .	270
Connecting to one or more tuners . . . . .	271
Manually entering a list of tuners . . . . .	273
Selecting from a list of recently used tuners . . . . .	274
Querying for a list of tuners . . . . .	278
Triggering a deployment job from Tuner Administration . . . . .	282
Monitoring a job (multiple tuners only) . . . . .	282
What is a job? . . . . .	283
Viewing job status details . . . . .	283
Stopping, resuming, and retrying a job . . . . .	285
Viewing information about a tuner . . . . .	288
Restarting a tuner . . . . .	288
Updating a tuner . . . . .	289
Updates to profiles and tuner binaries . . . . .	290

Scanning the machine on which the tuner is running . . . . .	291
What is Scanner Service? . . . . .	291
Scanning the machine . . . . .	292
Updating the policy on the endpoint where the tuner is running . . . . .	293
What is Policy Service? . . . . .	293
Updating the policy . . . . .	293
Updating transmitters and proxies. . . . .	294
Updating Patch Service on the endpoint where the tuner is running . . . . .	295
What is Patch Service? . . . . .	295
Updating Patch Service . . . . .	296
Starting the console window . . . . .	296
Waking up an endpoint using the WoW feature . . . . .	298
 Chapter 17 Package and channel management for a tuner . . . . .	302
Viewing channels on the tuner . . . . .	303
Filtering the list of channels using groups. . . . .	303
Sorting the list of channels . . . . .	304
Performing actions on channels . . . . .	307
Subscribing to channels . . . . .	307
Starting and stopping channels . . . . .	309
Updating channels . . . . .	309
Changing a channel URL. . . . .	310
Unsubscribing channels . . . . .	311
Deleting channels. . . . .	312
Verifying and repairing packages . . . . .	312
Viewing and changing channel-specific information . . . . .	313
Viewing general channel information . . . . .	314
Setting the update schedule for a channel. . . . .	315
Viewing and setting the capabilities for a channel . . . . .	318
 Chapter 18 General tuner settings . . . . .	320
Choosing a user interaction mode . . . . .	321
What is the user interaction mode? . . . . .	321
Specifying a user interaction mode for a tuner. . . . .	322
Advanced: tuner properties for each user interaction mode . . . . .	322
Setting update restrictions for channels . . . . .	324

Specifying tuner reboot options (Windows only) . . . . .	326
Common Reboot Service properties . . . . .	328
Common reboot service – Track History of Actions . . . . .	329
 Chapter 19 Tuner properties . . . . .	332
What are tuner properties? . . . . .	333
Adding tuner properties . . . . .	333
Editing tuner properties . . . . .	334
Deleting tuner properties. . . . .	335
 Chapter 20 Tuner security . . . . .	338
Specifying the trusted transmitters for the tuner. . . . .	339
What are trusted transmitters? . . . . .	339
Adding transmitters to the trusted transmitters table . . . . .	339
Editing transmitters in the trusted transmitters table . . . . .	340
Removing transmitters from the trusted transmitters table . . . . .	341
Specifying remote administration access to the tuner . . . . .	341
Using a directory service for remote administration access . . . . .	343
Working with SSL settings . . . . .	345
Enabling secure tuner administration . . . . .	346
Client-side certificates . . . . .	347
Tuner robustness service protection . . . . .	348
Limitations . . . . .	349
Tuner self-integrity check . . . . .	350
 Chapter 21 Advanced tuner settings . . . . .	352
CMS UI Infrastructure Properties. . . . .	353
Using a proxy with the tuner . . . . .	357
Proxy settings for the tuner. . . . .	358
Proxy exceptions for the tuner . . . . .	358
Specifying multiple proxies for failover. . . . .	359
Managing the bandwidth usage of the tuner . . . . .	361
Specifying JVM arguments for the tuner . . . . .	362
Viewing JVM properties . . . . .	362
Specifying SNMP settings . . . . .	363
Using a 3rd party SNMP manager . . . . .	363
Specifying ISM (Infrastructure Status Monitor) settings . . . . .	364

Specifying vPro settings . . . . .	365
Using the MESH feature to allow tuners to get content from peer tuners . . . . .	366
Enable the MESH feature in tuners . . . . .	367
Enabling the MESH feature in tuners . . . . .	370
Getting MESH status . . . . .	371
Handling tuner corruptions . . . . .	373
Types of tuner corruptions . . . . .	373
Repairing various types of corruptions . . . . .	374
Repairing a corrupted tuner . . . . .	377
SMCA support for multihomed computer . . . . .	379
Multihomed computer . . . . .	379
Support for multihomed computers . . . . .	379
Limitations of using multihomed computers . . . . .	379
Session isolation. . . . .	380
Workflow of Session Isolation . . . . .	383
Session Isolation for minimal mode tuner . . . . .	383
Platform support . . . . .	383
Limitations . . . . .	384
Prerequisites . . . . .	384
Enabling Session Isolation . . . . .	385
Disabling Session Isolation . . . . .	385
Log messages and debug information . . . . .	385
Tuner behavior with session migration. . . . .	386
Session affinity property . . . . .	386
Interactive Detection Service for Windows Server 2012 and Windows 8 . . . . .	388
Chapter 22 Tuner background information . . . . .	390
Tuner diagnostics . . . . .	391
Using advanceddiagnose.bat . . . . .	392
Status reports . . . . .	392
Debug reports . . . . .	394
Log reports . . . . .	395
Tuner logging. . . . .	396
Platform-specific log files . . . . .	396
Tuner history logs. . . . .	398

Tuner audit logs . . . . .	399
Controlling how tuner logs roll . . . . .	400
The individual channel history logs . . . . .	401
<b>Tuner background. . . . .</b>	<b>403</b>
Tuners and Intel AMT . . . . .	403
Tuner IDs . . . . .	405
Network detection in the tuner . . . . .	406
Minimal mode . . . . .	409
Garbage collection . . . . .	410
Application distribution protocol . . . . .	410
Behavior of autostart channels with the tuner minimal mode . . . . .	411
<b>Chapter 23 Lite Weight Administrator Console . . . . .</b>	<b>412</b>
<b>    Introduction to Lite Weight Administrator Console . . . . .</b>	<b>413</b>
Advantages of LWAC . . . . .	413
Browser support . . . . .	414
Logging into the LWAC to perform operations on the transmitter . . . . .	414
Navigating in the Lite Weight Administrator Console . . . . .	415
Editing Transmitter settings . . . . .	416
Editing transmitter properties. . . . .	417
Managing channels in the transmitter . . . . .	419
Transmitter diagnostic options . . . . .	423
Logging on to Lite Weight Tuner Administrator . . . . .	425
Prerequisites . . . . .	425
Using the Lite Weight Tuner Administrator . . . . .	425
Known issues . . . . .	428
<b>Chapter 24 Handling JRE . . . . .</b>	<b>430</b>
<b>    Introduction . . . . .</b>	<b>431</b>
Upgrade scenario . . . . .	432
Detection of JRE . . . . .	432
Prerequisites . . . . .	432
Property to specify use of the installed JRE on an endpoint . . . . .	432
Workflow of JRE detection and starting the tuner . . . . .	433
How to find the JRE version which the Tuner is currently using on an endpoint? .	433

Can I uninstall JRE on an endpoint? . . . . .	434
JRE handling while creating a profile for an endpoint tuner. . . . .	434
Log messages . . . . .	434
Chapter 25 Marimba Monitoring Service . . . . .	436
Introduction to Marimba Monitoring Service (MaMoS) . . . . .	437
The MaMoS Service . . . . .	439
External Watchdog using OS specific scheduler . . . . .	440
Key features of MaMoS . . . . .	440
Advantages of MaMoS. . . . .	441
Limitations . . . . .	441
Problem - Action matrix for critical Infrastructure Components in MaMoS	442
Modules registered with MaMoS . . . . .	443
MaMoS components . . . . .	443
Prerequisites . . . . .	443
Configuring components for MaMoS . . . . .	444
Configuring MaMoS through properties . . . . .	444
Setting the debug flag . . . . .	447
SNMP alerts for MaMoS in ISM. . . . .	451
Using the ?status command. . . . .	451
MaMoS Logging . . . . .	452
Optional Tuner property to configure MaMoS . . . . .	453
Index . . . . .	454



# Preface

The *Symphony Marimba Client Automation CMS and Tuner User Guide* is part of the Symphony Marimba Client Automation product.

## Audience and document scope

This guide provides information on administering the Common Management Services (CMS) and tuner infrastructure components.

For information on administering the transmitter and proxy components, see the *Symphony Marimba Client Automation Transmitter and Proxy User Guide*. For information on planning the infrastructure and installing the components, see the *Symphony Marimba Client Automation Installation Guide*. All are available on the Channel Store.

This guide assumes that you are already familiar with the basics of Symphony Marimba Client Automation technology, formerly called Configuration Automation, Configuration Management, and Marimba. You should have a general understanding of the Internet, HTTP, and the World Wide Web, and of what is involved in planning and deploying a product suite for your company.

## Accessing product documentation

You can access Symphony Marimba Client Automation documentation in the following ways:

- Using the documentation channel (page 20)

- Searching across the entire Symphony Marimba Client Automation documentation set (page 20)

## Using the documentation channel

If you are using a Windows platform, you can subscribe to the Symphony Marimba Client Automation Product Documentation channel. You can download the contents to a Windows computer from the Channel Store.

You can find the latest documentation channel in Channel Store.

## Searching across the entire Symphony Marimba Client Automation documentation set

Symphony Marimba Client Automation comes with a large documentation set in PDF format, which can make it difficult to quickly find exactly what you need. With Adobe Reader version 7.0 and later, you can perform a full-text search across all of your PDFs that reside in the same directory, including subdirectories.

### ► To search for a word or phrase in the PDFs contained in the Marimba Client Automation Product Documentation channel

- 1 Ensure that you have installed the documentation channel as described in “Using the documentation channel” on page 20.
- 2 If you do not have Adobe Reader version 7.0 or later, you can download the latest Adobe Reader version from [www.adobe.com](http://www.adobe.com) for free.
- 3 Start Adobe Reader.
- 4 Click the search icon (binoculars) in the toolbar.

If the search icon is missing, try right-clicking the toolbar to find more toolbar options. Different versions of Adobe Reader put the option in different places.

- 5 After the Search window is displayed, select All PDF Documents in under **Where would you like to search?**
- 6 Click the folder selection box and choose **Browse for Location**.
- 7 Browse to the top-level folder that contains the PDF documents installed with the Marimba Client Automation Product Documentation channel.

- 8 Type a search term in the **What word or phrase would you like to search for?** box and click **Search**.

The search tool searches for the term you entered in all of the PDFs in the chosen directory and its subdirectories and displays the results.

## Related documentation

Symphony provides Symphony Marimba Client Automation documents in PDF format. These documents are written for system administrators and are listed in the following table.

Guide	Description
<i>Symphony Marimba Client Automation Concepts Guide</i>	Introduces you to Symphony Marimba Client Automation and its components and defines basic concepts about its core technology.
<i>Symphony Marimba Client Automation Installation Guide</i>	Provides: <ul style="list-style-type: none"><li>■ information needed to design an infrastructure for your enterprise, which involves determining the machines you will use for the various components and whether you need to purchase additional hardware and software</li><li>■ instructions for a first-time installation of Symphony Marimba Client Automation and its associated components</li><li>■ instructions about upgrading to the current version</li><li>■ hardware requirements (such as processing speed, disk space, and RAM) and operating system requirements for supported platforms. This guide also lists the supported databases, directory services, and locales</li></ul>
<i>Symphony Marimba Client Automation Application Packager User Guide</i>	Provides information about packaging software for distribution to desktops or servers. This guide also includes information about command-line usage, policies, XML templates, and Windows system macros.
<i>Symphony Marimba Client Automation CMS and Tuner User Guide</i>	Provides information about the Common Management Services (CMS) and tuner infrastructure components. This guide also describes the tools and features you use to configure these components.
<i>Symphony Marimba Client Automation Configuration Discovery Integration for CMDB Getting Started Guide</i>	Provides instructions about planning, installing, and configuring the Configuration Discovery integration. This guide also includes information about relationship classes and mappings, data exchanges, and reconciliation definitions.
<i>Database Schema Guide</i>	Provides reference information about database schema, such as table names, field names, indexes, and primary, foreign, and unique key constraints.
<i>Symphony Marimba Client Automation for Clients Server Management User Guide</i>	Describes how to use Deployment Management and Content Replicator to control and monitor the distribution of content and applications across heterogeneous server platforms and data centers. Deployment Manager extensions to Report Center and Application Packager are also described.

Guide	Description
<i>Symphony Marimba Client Automation Device Management User Guide</i>	Describes how to use Symphony Marimba Client Automation to manage your mobile devices. This includes Scanner Service to perform inventory scans on your mobile device endpoints; Report Center to run queries against your scanned data; Application Packager, using the PDA Packager, to package and publish files and applications to mobile devices; and Policy Service to define subscription policies for your mobile devices.
<i>Symphony Marimba Client Automation Server Management CLI Reference Guide</i>	Provides syntax and usage information about the command-line options used with Content Replicator, Deployment Manager, and Application Packager. Using the SOAP interface feature is also described.
<i>Symphony Marimba Client Automation Patch Management User Guide</i>	Helps you configure and administer Patch Management and the Patch Service plug-in. This guide also includes working with the patch repository, patches, patch groups, and custom patches, and deploying patches.
<i>Symphony Marimba Client Automation Policy Management User Guide</i>	Helps you configure and administer Policy Management and the Policy Service plug-in. This guide also includes integration procedures for directory services, such as Active Directory, ADAM / AD LDS, and Sun ONE Directory.
<i>Symphony Marimba Client Automation Reference Guide</i>	Provides reference information, such as command-line options, tuner properties, proxy properties, transmitter properties, channel properties, channel parameters, channel states, ports, and log IDs with associated log messages.
<i>Symphony Marimba Client Automation Report Center User Guide</i>	Provides instructions about running queries of inventory information, configuring the Inventory and Logging plug-in, configuring endpoints, and integrating Report Center with other Symphony Marimba Client Automation applications.
<i>Symphony Marimba Client Automation Transmitter and Proxy User Guide</i>	Provides information about the transmitters and proxy infrastructure components. This guide also describes the tools and features you use to configure these components.
<i>Definitive Software Library Administrator's Guide</i>	Provides a description of the Definitive Software Library and explains how the DSL is useful to you, how to use the DSL console, and how to access the DSL using Symphony Marimba Client Automation applications, such as Report Center and Application Packager.

## What is new in this guide for Marimba 9.0.00?

- LDAP Properties  
For more information, refer LDAP Properties (page 150).
- WOW Properties  
For more information, refer WOW Properties (page 300).
- Marimba now provides an option to configure server and endpoint properties through UI from CMS and Policy Management.  
For more information, refer Advanced Tuner Settings (page 353).

## Contact information



Section

# I Introduction and Overview

Section 1 discusses the following topics:

- “Introduction” on page 29
- “Profiles and administration tools” on page 33
- “Infrastructure security overview” on page 39



Chapter

# 1 Introduction

This chapter shows you to the content and organization of the *BMC Marimba Client Automation CMS and Tuner User Guide*, and gives you an overview on using the help system.

The following topics are provided:

- How to read this document (page 30)
- Using help (page 31)

# How to read this document

This section describes the content and organization of this guide. This guide contains the following parts and chapters:

Section 1, “Introduction and Overview,” provides an overview of this guide.

- The current chapter.
- “Profiles and administration tools” on page 33, which introduces you to profiles and the administration tools and explains when to use them to configure infrastructure components.
- “Infrastructure security overview” on page 39 explains the security differences when you upgrade to the current version and discusses best practices.

Section 2, “System Settings,” provides information about configuring system settings using Common Management Services (CMS), also called the console. This part includes the following chapters:

- “Common Management Services basics” on page 59
- “Getting started with CMS and the console” on page 65
- “General settings” on page 71
- “User authentication and roles” on page 125
- “Configuring data sources” on page 139
- “Setting up access control lists” on page 161
- “Action Request System settings” on page 185
- “Working with web services” on page 189
- “Troubleshooting system settings” on page 193
- “Infrastructure Status Monitor” on page 199

Section 3, “Tuner Administration,” provides information about configuring tuners in your environment. This part includes the following chapters:

- “Tuner basics” on page 247
- “Getting started with Tuner Administration” on page 261
- “Package and channel management for a tuner” on page 299
- “General tuner settings” on page 317

- “Tuner security” on page 335
- “Tuner properties” on page 329
- “Advanced tuner settings” on page 349
- “Tuner background information” on page 383

## Using help

To access the online help, click the Help button from within the Tuner Administration browser-based application.

The first time you click the Help button, you see a security warning prompting you to install and run an applet that has been code-signed by Quadralay Corporation. This applet provides the online help’s dynamic table of contents, topic search feature , and bookmarking ability. If you do not install the applet, the help system still works, but some functionality is not available.

Help is context-sensitive. When you are on a particular page of the browser-based interface for an application and you click the Help link in the top right corner of the page, the help that appears corresponds to that page of the interface. Some topics contain a hyperlinked list of related topics at the end of the topic (indicated by a “See Also” heading).

To look for help topics, you have the following options in the help window:

- **Contents button.** Lets you see the table of contents for the help topics.
- **Index button.** Lets you scroll through the alphabetical list of entries to find the entry you want. Click the index entry to display the corresponding help topic.
- **Search button.** Lets you search for a word or phrase. Enter one or more words in the field and press Enter or click the Go button. The page displays a list of all the topics in the help system that contain the word or phrase you entered. If you entered more than one word, the search finds help topics that contain all the words you entered. The topics found by searching are ranked in order of relevance.

**Returning to a previous help topic.** If you want to go back to a previous help topic, you can use standard navigation shortcuts. For some browsers, you can press the keyboard Backspace key to go back, or you can right-click and choose Back from the menu that appears. In the help window, there is no Back button.



Chapter

# 2 Profiles and administration tools

This chapter introduces you to the administration tools and profiles and explains when to use each to configure the Symphony Marimba Client Automation infrastructure components.

The following topics are provided:

- What are profiles? (page 34)
- What are administration tools? (page 34)
- When to use profiles versus administration tools (page 34)
- Updating profiles (page 35)

## What are profiles?

*Profiles* provide a central location for defining, storing, and updating the configuration settings that you are applying to a set of machines. You assign profiles to machines in your environment as part of the deployment process, and can regularly edit the profiles. Symphony Marimba Client Automation offers you a predefined set of profiles for the different infrastructure components such as managed nodes (endpoints), master transmitter, mirrors, repeaters, and proxies. You edit the profiles to suit the requirements in your environment.

For more information, choose Applications > Infrastructure > Setup & Deployment, click the Profiles tab, and then click Help.

## What are administration tools?

*Administration tools* refer collectively to the Tuner Administration, Transmitter Administration, and Proxy Administration browser-based applications. The tools let you administer and perform actions on one or more infrastructure components.

## When to use profiles versus administration tools

Both profiles and administration tools let you control multiple components simultaneously, but in the following ways:

- **Edit settings.** Using profiles, you can *modify configuration settings* on multiple components simultaneously. This includes security, performance, log settings, and so on.  
For more information, see “Updating profiles” on page 35.
- **Perform actions.** Using administration tools, you can *perform actions* on multiple components simultaneously, such as starting and stopping tuners, transmitters, or proxies; starting transmitter replication; clearing the cache of proxies; or starting the inventory scan on tuners.  
For more information, see “Operations for one tuner versus multiple tuners” on page 270.

## Administration tool settings override profile settings

Administration tool settings always override profile settings. For example, if you set properties A and B using profiles, and you then change the values for the two properties using the administration tools, the latter values always take effect. If you update the profile or apply a new profile to the machine after you made the changes using administration tools, the values set by the administration tools always take precedence.

For more information, see “Tuner properties” on page 329.

## Examples of when to use administration tools

You should use the administration tools when you are doing the following actions:

- **Making minor changes to a particular machine because of idiosyncrasies of that machine or its environment.** You use profiles to define the base state of machines and then use administration tools to refine further the configuration of a particular machine. For example, if you must modify the performance settings of a machine because of differences in the amount of RAM or available disk space on that machine, you configure the settings using administration tools.
- **Configuring features that you cannot configure using profiles.** Using administration tools, you can configure the following features for and perform the following actions on a tuner that you cannot configure using profiles:

Using Tuner Administration: configuring the administration port to run in SSL mode, displaying the tuner properties currently set for the tuner, displaying how long the tuner has been running, and so on.

Using administration tools, you can perform actions on the tuner such as managing the channels on the tuner, restarting the tuner, scanning the machine, updating the policy, and so on.

## Updating profiles

Using profiles, you can update settings on multiple components in one of the following ways:

- You can edit the profile that is currently assigned to machines. For information, see “Updating an existing profile” on page 36.

- You can assign a different profile to machines. For information, see “Replacing a profile” on page 37.

## Updating an existing profile

You can update the configuration on machines by editing the settings of the profile that is currently assigned to those machines. Each profile is saved as a segment of the Infrastructure Service channel; when Infrastructure Service starts on machines, it downloads and applies any available changes to profile settings and to the tuner binaries.

For information on updating the tuner binaries, see the *Symphony Marimba Client Automation Installation Guide*, available on the Marimba Channel Store.

### ► To edit an existing profile

- 1 After logging in to the Console, choose Applications > Infrastructure > Setup & Deployment.
- 2 Click the Profiles tab.
- 3 Select a profile that is already assigned to a set of machines.
- 4 Click Edit.
- 5 Change configuration settings as necessary.
- 6 If you want, modify the schedule for the Infrastructure Service channel on the Tuner/Profile Updates tab. The default schedule is every day at 4 AM.

The schedule controls how frequently the Infrastructure Service starts on machines, checks for updates, and downloads and applies new profile and binary settings to those machines.

Changes to the schedule take affect after the next time the Infrastructure Service channel runs and after the tuner on those machines restarts.

- 7 On the Tuner/Profile Updates tab, it is recommended that the Automatically restart the tuner after applying updates, if there are any check box is selected.

The check box is selected by default. A tuner restart is required for some profile updates and tuner binary updates to be applied successfully.

- 8 Click Preview and then click Apply.

Edits are published to the Infrastructure Service to which the profile belongs.

## Replacing a profile

You can change the configuration on specific machines by assigning them a new profile. For example, you are moving from a testing to a production environment. You assigned a profile to machines in the testing environment. After you have determined the correct settings for the production environment, you assign a different profile to the machines.

When you replace a profile on machines

- You assign a new profile to machines by using the Profiles tab in Policy Manager or setting the `marimba.tuner.update.profile` tuner property through Tuner Administration. This document discusses using Policy Manager to assign a new profile. When you use Policy Manager to assign a profile, you can leverage collections. A *collection* is a group of machines that match certain criteria that you specify in a Report Center query. After the query runs, you can use Policy Manager to assign a profile to the resulting list of machines (the collection).
- The Infrastructure Service channel runs on a schedule. The next time the Infrastructure Service starts on machines, it downloads and applies any available changes to profile settings and to the tuner binaries. Some changes are applied to machines after the tuner on those machines is restarted.

For information on updating the tuner binaries, see the *Symphony Marimba Client Automation Installation Guide*, available on the Marimba Channel Store.

### ► To replace the profile on a set of machines with a different profile

- 1 Create the new profile.
- 2 Using Report Center, define a collection that includes the set of machines to which you want to assign the new profile.
  - a Create a query and specify the criteria for the set of machines.
  - b Save the query in the Collections folder.
  - c Run the query, either by setting a schedule for it or by running it manually.

The resulting list of machines (the collection) appears as a target in Policy Manager.

- 3 Using Policy Manager, assign the new profile to the collection that you defined.
  - a Locate and select the collection. It should appear in the Collections folder.
  - b Edit the policy for the collection, and go to the Advanced > Profile tab.
  - c On the Profile tab, click Edit.
  - d If you want to see profiles from a different location, enter the transmitter URL (for example, <http://trans.company.com:5282>) and, if access permission is set for the transmitter, enter the user name and password for subscribing to channels. Click Go.

A list of profiles appears on the left side of the page. The profiles are available with the Infrastructure Service on the transmitter you specified. Each profile is saved as a segment of the Infrastructure Service channel.

- e Click a profile so that it appears under Selected Profile on the right side of the page. Click OK.
- f Preview and save the policy.

Performing this procedure sets the following tuner property for the machines:

`marimba.tuner.update.profile`

The value for this property is the name of the new profile segment that you want to assign to the machines. The name of a profile segment has the following format: `.profile_<name>`

Example: `marimba.tuner.update.profile=.profile_ny_mirrors`

The next time Policy Service runs on the machine, the tuner property is set in the `tuner prefs.txt` file. The value in the `tuner prefs.txt` file takes precedence even if the same property is set in the `tuner properties.txt` file (where tuner properties are set using profiles). If you use Tuner Administration to set this property, it is also saved in the `tuner prefs.txt` file.

The next time Infrastructure Service runs on the machine, and after the tuner is restarted, the new profile is applied to that machine.

# 3 Infrastructure security overview

This chapter introduces you to infrastructure security considerations and features. It discusses SSL and using server-side and client-side certificates, SSL-enabled LDAP servers, and SSL-enabled CMS, and lists some best practices for optimum usage. It compares channel content trust levels and recommends when to use each one. A procedure for setting up SSL on tuners is included.

The following topics are provided:

- Passwords (page 40)
- Using SSL (page 40)
- Trusting channel content (page 45)
- Setting up tuners to use SSL (page 49)
- Enabling SSL across multiple tuners in the infrastructure (page 52)

## Passwords

Passwords are encrypted, not encoded. When you upgrade from an older, unsupported version, when the new tuner first starts, it automatically performs a one-time upgrade of unencrypted passwords that are managed by the tuner and passwords managed by individual channels.

Encrypted passwords are stored in the file system (`prefs.txt` files) and are not encrypted in memory. A password is bound to an individual tuner and cannot be used outside that tuner.

Tuners prior to version 7.0 cannot recover encrypted passwords. Passwords must be reconfigured using Channel Manager, Policy Service, and so on.

You can continue to set properties remotely with Tuner Administration. When changes are saved, however, the passwords are encrypted.

## Using SSL

Using SSL makes sure that servers are authenticated and that data maintains its integrity and stays confidential. There are several ways of doing this, and can be used separately or together.

- “Using server-side certificates” on page 41. Servers must authenticate to clients.
- “Using client-side certificates” on page 41. Clients must authenticate to servers.
- “Using SSL-enabled LDAP servers” on page 42. Tuners, transmitters, CMS, and Deployment Manager use an SSL-enabled LDAP server to authenticate clients.
- “Using SSL-enabled CMS” on page 43. CMS must authenticate itself to users.

There are other security considerations when using SSL.

- “Distributing root certificates securely” on page 44
- “Using mixed-mode SSL” on page 44
- “Using wildcard certificates” on page 45

## Using server-side certificates

When you use a server-side certificate, a server must authenticate to a client. For example, before a tuner connects to a transmitter, the transmitter must authenticate itself to the tuner. The tuner then trusts the transmitter with the tuner data. Without server authentication, the client is vulnerable to someone setting up a secure connection from the client to a false server and having the false server then able to access the client data.

With server-side certificates

- Each client must have a local copy of the root certificate before the SSL connection is established.
- The root certificate must be valid and trusted for SSL.
- Strong encryption (128-bit SSL) is enabled by default (version 6.0.3 and later).
- You can use mixed-mode SSL to encrypt transmitter administration, but the tuners subscribe through HTTP.

## Using client-side certificates

Passwords are often the weakest link in password-based authentication schemes. Passwords should be chosen based on security (how unbreakable they are), but are often guessable. Client-side certificates, however, are a stronger form of authentication.

When you use a client-side certificate, a client must authenticate to a server during the SSL handshake. For example, before a tuner connects to a transmitter, the tuner must authenticate itself to the transmitter; before a mirror transmitter replicates to a master, the mirror must authenticate itself to the master; before CMS connects to an LDAP server, CMS must authenticate itself to LDAP.

For example, a bank works with highly confidential data, so you set up the servers to require a client certificate. This can be individual certificates for specific employees or one generic employee certificate that specific employees use. Someone from outside cannot access the network without this additional authentication.

Be aware that client-side certificates have expiration dates and must be kept current.

### With client-side certificates

- Each server must have a local copy of the root certificate before the SSL connection is established.
- The root certificate must be valid and trusted for SSL client certificates.
- SSL servers typically have options to request, not request, or require a certificate from a client.
- You can configure a tuner to always use a specific client certificate. Use the `marimba.security.sslcert=<cert ID>` tuner property.
- A tuner's certificate database contains the encrypted private key corresponding to a client certificate. When a tuner initiates an SSL connection using a client-side certificate, it prompts you to enter the password needed to decrypt the private key.

The password remains in memory for only a set time and then you must re-enter the password. You can configure the time using the `marimba.security.cert.password.timeout=<seconds>` tuner property. The default is 3600 seconds (1 hour).

A tuner does not let you save a private key password. If you have an unattended tuner, you can reset the password to null so you are not prompted to enter one; however, the private key is stored unencrypted in the file system.

## Using SSL-enabled LDAP servers

Tuners, transmitters, CMS, and Deployment Manager can use an LDAP server to authenticate clients. Because confidential data, for example, passwords, are sent to an LDAP server, it is important to make sure an LDAP server is SSL enabled, thus keeping the data confidential.

Without SSL-enabled LDAP server authentication, tuners, transmitters, CMS, and Deployment Manager are vulnerable to someone setting up a secure connection from them to a false LDAP server and having the false server then able to access their data.

Server authentication makes sure that the credentials are invalid reply sent by an LDAP server to tuners, transmitters, CMS, and Deployment Manager cannot be altered to credentials are valid.

### With SSL-enabled LDAP servers

- Enabling SSL for an LDAP server is vendor specific. For example, Microsoft has a process for Active Directory, and Netscape has a process for iPlanet.
- Each client must have a local copy of the root certificate before the SSL connection is established.
- The root certificate must be valid and trusted for SSL.

---

Note: After you enable SSL on an LDAP server, you must restart the tuner on the server and configure the CMS to work with an SSL-enabled LDAP server.

---

## Using SSL-enabled CMS

Users often send sensitive information to CMS. For example, logging in to CMS; configuring plug-in passwords; entering passwords for remote administration and deployment; and configuring authentication services, databases and user roles. It is important that the data remains confidential, and that CMS authenticate itself to the user.

CMS accepts client-side certificates using the smartcard authentication feature. For more information, refer to “Using smartcard authentication for CMS” on page 133.

### With SSL-enabled CMS

- You can configure the SSL settings.
- Each client (browser) must have a local copy of the root certificate before the SSL connection is established.
- The root certificate must be valid and trusted for SSL.

### Internet Explorer settings for an SSL-enabled CMS

In Internet Explorer if you click a link in the CMS console when the CMS is SSL-enabled, a pop-up asks if you want to display unsecure items. To prevent the pop-up from appearing, change your Internet Explorer settings as described in the following procedure.

## ► To configure Internet Explorer for an SSL-enabled CMS

- 1 Choose Tools > Internet Options > and click the Security tab.
- 2 Click Custom Level.
- 3 Under Miscellaneous, set the Display mixed content option to Enable.

## Distributing root certificates securely

Because each server or client must have a local copy of a root certificate before an SSL connection is established or before you work with channel signing or installer signing, you must be able to distribute the root certificates securely before you start.

- If a root certificate is from a well-known certificate authority (for example, VeriSign) then the certificate might already be deployed; for example, in the tuner's certificate database; in a file system for browsers, for example, Internet Explorer and Firefox; and so on.
- If you issue your own root certificate, then the root certificate must be deployed using Profile Manager, either when you are creating a tuner installer or updating already deployed tuners.

**Best practice.** How you distribute root certificates and what kind of certificates you need depend on your environment: few or many machines, clients or servers, new or pre-existing machines. You should take the time to analyze your environment and decide what is most efficient. For a small company or network, you might want to add a root certificate manually for each machine. For a larger company or network, you might want to make the root certificate part of a download, either by creating an installer for new machines or as part of an update for pre-existing machines.

## Using mixed-mode SSL

You can use mixed-mode SSL for transmitters; that is, you can enable SSL for Transmitter Administration while not enabling SSL for the endpoint tuners.

**Best practice.** You should encrypt only those components that need it; for example, Transmitter Administration because it works with administrative information (changing properties, subscribing to channels) and confidential data (publishing requires sending a password), but not an endpoint tuner that is downloading bulk data. This saves time and resources by not requiring the entire system to be encrypted.

SSL criteria can include:

- Must the data always remain confidential?
- Is there any way the data can be altered by someone from the outside?
- Must you authenticate a server to make sure it can be trusted with the data?

## Using wildcard certificates

Wildcard certificates let you use one certificate for multiple servers. Servers are SSL servers and can be tuners, transmitters, CMS, and Deployment Manager. This is useful, for example, when you have a small server farm and want to enable SSL on everything or you do not want a new SSL certificate to set up a new server.

However, because you do not know exactly to which host you are connecting, you lose some degree of authentication. If someone has access to the wildcard certificate, he or she can set up a false transmitter.

**Best practice.** Make sure you have a secure network.

## Trusting channel content

When you download and run channels, or when you package and publish channels for other users to download and run, how can you be sure the channels have not been tampered with? Channel signing is the main way of verifying that a channel has not changed after it was published.

There are several levels of trust.

Trust level	What you use	Example of when to use
Lowest	Trusted transmitters on page 46	Development environment
	Channel signing page 46	QA environment
Highest	Channel signing with security-policy tuner properties page 47	Production environment

There is another signing consideration. See “Signing installers” on page 48.

## Using trusted transmitters

Trusted transmitters can be used when you develop or package channels but do not want to use channel signing or root certificates. For example, a development environment that is totally within a company and its firewalls.

Trusted transmitters let a tuner run channels based on a transmitter IP address or host name. However, this is a weak form of server authentication because IP addresses and DNS names can be spoofed and the tuner can then be redirected without knowing.

**Best practice.** Do not use trusted transmitters in an untrusted network; for example, the Internet.

## Using channel signing

Channel signing makes sure that a channel was not modified after it was published. This prevents, for example, someone altering and re-publishing a channel to contain spyware before the channel gets downloaded to endpoints.

**Best practice.** Anything that can be downloaded from a web server or a file share should be signed. Then you can be sure that what you want users to download is in fact what they download. Users can trust what you post.

**Best practice.** While all BMC Marimba Client Automation channels are signed, channels you package using Application Packager are not signed. Application Packager channels often run executables that can, for example, modify file systems and registries, and install drivers and service packs. The operations are often performed with great privileges, for example, Local System account. If you are dealing with confidential data, you should sign the channels.

### With channel signing

- Each client must have a local copy of the root certificate before the SSL connection is established.
- The root certificate must be valid and trusted to issue channel signing certificates.

When you publish a channel, you use a private key to produce a signature from the original channel. The signature is published with the channel. If the signatures do not match, then the channel was modified after it was published.

If a channel signature is valid, a user must explicitly acknowledge that he or she trusts the certificate before the channel can run. However, you can pre-configure tuners to trust specific certificates so that users are not prompted. By default, tuners trust Marimba and BMC certificates.

## Why verification can fail

Verification can fail at several levels. The examples build on each other.

- Someone tries to modify the channel content without modifying the certificate and signature.

Verification fails because the client cannot recreate the matching signature.

- Someone tries to modify the signature, replacing the true channel signing certificate with a false one so he or she can use a false private key to generate a false signature.

While the tuner does verify the signature, verification fails if the false channel signing certificate was not issued by a valid root certificate. Valid root certificates are contained in the tuner certificate database and can be accessed with Certificate Manager.

- Someone has put a false root certificate in the tuner certificate database.

While verification itself has succeeded, a user must agree to trust the certificate and run the channel.

## Using security tuner properties

There are several tuner properties that can restrict or relax how the tuner enforces its security. Used with channel signing, this is the most trusted level of channel security.

**Best practice.** Use this method when you want more control over what users can and cannot do. For example, you do not want users to make an SSL connection to a server whose certificate was issued by an unknown root, so you set the `marimba.security.noUserOverride=true` property. Users are never asked if they want to make the SSL connection so the connection is always refused.

You can use the following tuner properties to restrict security:

```
marimba.security.channels.onlytrusted=true
```

If true, only signed channels or channels from trusted transmitters can run.

```
marimba.security.noUserOverride=true
```

If true, a user cannot override certificate-related problems such as a channel signed by a root certificate that is not already present locally. A channel cannot run if it is signed by a certificate that is not listed in marimba.security.trusted.certs.

```
marimba.security.trusted.certs=<subject1>|<issuer1>|...|<subjectN>|<issuerN>
```

Specifies certificates that are pre-configured to be trusted. Marimba and BMC certificates are already in the list, so you should only add your own channel signing certificate to this list.

You can use the following tuner properties to relax security:

```
marimba.security.trusted.transmitters
```

Specifies one or more transmitter IP or DNS names to be trusted.

```
marimba.security.ssl.matchdomainonly=true
```

Lets a tuner accept wildcard SSL certificates; for example, \*.acme.com.

```
marimba.security.ignoreExpiration.*
```

Lets a tuner ignore certificate expiration issues.

## Signing installers

Installer signing makes sure that an installer was not modified after it was published. A code-signing certificate is conceptually the same as a channel-signing certificate. Microsoft refers to these as Authenticode certificates.

**Best practice.** If you want users who run the tuner installer to verify that the installer has not been modified after creation, you should sign installers that you create.

When you download and run the BMC Marimba Client Automation installer, Windows prompts you to let the executable run.

When you sign installers

- Each client must have a local copy of the root certificate before the installer is run.

- The root certificate must be locally installed in the Windows certificate store instead of the tuner's certificate database, because the OS, not the tuner, verifies the signature.
- The root certificate must be valid and trusted for signing code.

## Setting up tuners to use SSL

This section explains how to set up tuners to use SSL. Tuner security falls into the following categories:

- **Trusted transmitters.** You can specify which transmitters host channels that tuners should let run or install. See “Tuner security” on page 335.
- **Remote administration.** You can specify which users and groups can use Tuner Administrator to connect to the tuner and administer it. See “Tuner security” on page 335.
- **Secure Sockets Layer (SSL) encrypted communication.** You can ensure that communication between the Tuner Administrator and the tuner is secure and encrypted.

If you want to ensure that communication between the Tuner Administrator and the tuner is secure and encrypted, you must obtain and install a Secure Sockets Layer (SSL) certificate on the machine that hosts the tuner.

---

Note: The administration tools mentioned throughout the rest of this section include Certificate Manager. The availability of Certificate Manager might be limited to a particular group of users in your company, such as system administrators.

---

---

Note: SSL is not supported on MAC computers.

---

To request and install a certificate, use Certificate Manager. Information for requesting, installing, and importing certificates, and for setting the certificate to be trusted for SSL, appear in the Certificate Manager Help (click the Help button from within Certificate Manager).

This section includes the following topics:

- “Enabling secure tuner administration” on page 50
- “Client-side certificates” on page 51

## Enabling secure tuner administration

You can enable secure (encrypted) administration of the tuner. To achieve this, you must import an SSL certificate into the tuner, enable secure administration for the tuner, and then use the secure tuner URL (starting with `https://` instead of `http://`) in Tuner Administrator.

To administer a remote tuner that has SSL enabled, the tuner running the Infrastructure Administration channel (which contains Tuner Administrator) must have the root certificate of the remote tuner in its certificate database.

### ► **To configure a tuner to run in secure mode**

- 1 Run Certificate Manager installed on the tuner, and import the SSL certificate (if you have not already done so). Make sure that the root certificate is trusted for SSL.

For more information, see the Certificate Manager Help, available on the Channel Store.

- 2 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 271.
- 3 After specifying the tuner you want to connect to, click **Edit Settings**.
- 4 Click the **Security > SSL Settings** tab.
- 5 Select the **Use SSL Security** check box.

You cannot select this check box if you do not have certificates installed.

- 6 From the SSL certificate list, select the certificate you want to use.
- 7 If you want, click **View Certificate** to see information about the selected certificate.

A new browser window appears and shows information about the selected certificate, including the serial number, valid dates, owner information, and issuer information.

- 8 In the **Password** field, specify the SSL certificate password and confirm it.
- 9 Select the **Save SSL certificate password on tuner** check box if you want to save and automatically use the password that you provided, so that you do not need to enter the password again when connecting to the tuner. The password is encrypted in the file system.

**Note:** If the password is not saved and if the tuner is restarted, the tuner cannot enable SSL on its RPC port. You must then repeat this step.

- 10 From the Client certificates list, select one of the following options:

- Do not ask for client-side certificates
- Request client-side certificates, but do not require them
- Require client-side certificates

For more information, see “Client-side certificates” on page 51.

- 11 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 264.

**Note:** When you apply changes to the administration port SSL settings, Tuner Administrator warns you and disconnects from the tuner. If you want to continue administering the tuner, you must reconnect. If you have configured the tuner to use a secure port, remember to use `https` instead of `http` in the URL when connecting to the tuner.

## Client-side certificates

You can configure the tuner to require, request, or not ask for client-side certificates. Using Tuner Administrator, you can select one of the following options:

- **Do not ask for client-side certificates.** If you select this option, the tuner does not request certificates from clients (such as Tuner Administrator). However, the client must still provide the correct administration credentials (if required) to administer the tuner.
- **Request client-side certificates, but do not require them.** If you select this option, the tuner requests a client certificate. But if a client does not have one, the client can still access the tuner.
- **Require client-side certificates.** If you select this option, only clients that have a certificate can access the tuner. In this case, Tuner Administrator must have a valid client certificate to connect to the tuner. The Certificate Authority who issued the client certificate must match a root Certificate Authority that the tuner accepts.

# Enabling SSL across multiple tuners in the infrastructure

This section details the steps to enable SSL across multiple tuners in your infrastructure. To do this you must distribute:

- a certdb file that has the installed root and client certificates using either Policy Manager or Deployment Manager
- the tuner properties needed to enable the certificates using an Infrastructure Service profile

## To deploy a certificate using a profile

- 1 Navigate to Applications -> Infrastructure -> Setup and Deployment.
- 2 Click Profiles tab.
- 3 Select the profile from which you want to deploy the certificate.
- 4 Click Edit.
- 5 Click Security tab.
- 6 Click Certificates tab.
- 7 Select the certdb file from the location on your computer where you have stored it.

Note: Select a certdb file which contains a valid certificate.

- 8 Click Custom Properties.
- 9 Include the following 7 properties as part of the endpoint tuner profile:
  - marimba.tuner.rpc.secure=true
  - marimba.tuner.rpc.clientauth=none
  - marimba.security.ssl.matchdomainonly=true
  - marimba.tuner.rpc.certpw=<certificate password in base64 format>
  - marimba.tuner.rpc.cert.id=<certificate token - copy this from the certificate itself>
  - marimba.security.ignoreExpiration.ssl=true
  - marimba.tuner.display.noerrors=true
- 10 Click Preview.

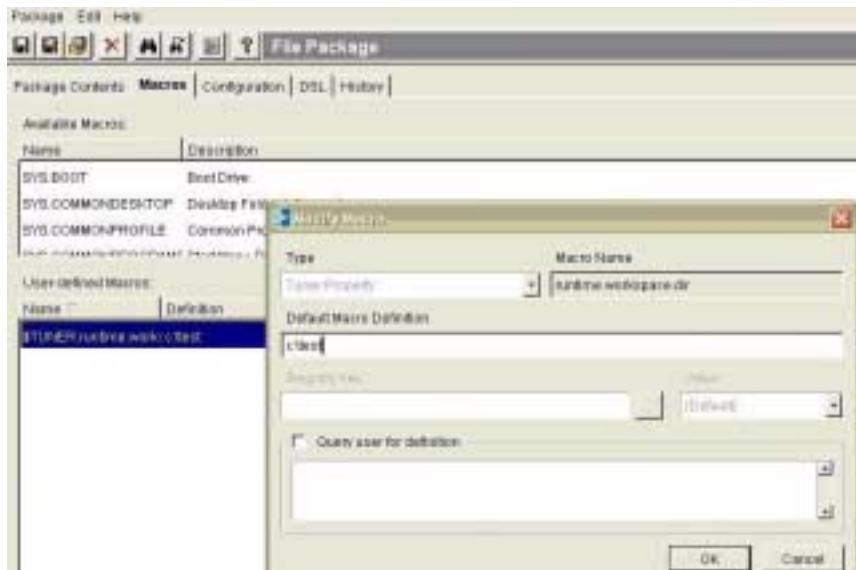
- 11 After you preview the changes, click **Apply**.

Once the tuner is updated, the certdb will be updated with the new certificates.

## To package and deploy certdb

- 1 If you do not have a pre-existing setup, then install the tuner. Otherwise skip this step.
- 2 From a machine that has the root and the client certificates to deploy, use the Package Editor (of Application Packager) to create a simple application package that:
  - contains the certdb file
  - specifies a macro that refers to the `runtime.workspace.dir` tuner variable which contains the destination for the certdb file, as shown in Figure 3-1 on page 53

Figure 3-1: Specifying the macro



You can distribute the package to the endpoints using either Policy Manager or Deployment Manager.

- 3 Start the Infrastructure Service channel so that it restarts the tuner and updates the changes made to the profile.

You can also set an update schedule as described in “Setting the update schedule for the certdb package.”

## Setting the update schedule for the certdb package

Setting an update schedule allows you to update this package at a later time when a new certdb file is published. There are two options for setting an update schedule for the certdb package:

- If you know the expiry of the certificates in advance, you can set the update schedule for the package for that point in time.
- Or you can schedule regular updates during which certdb (at the endpoint) can update itself whenever any change is introduced in the certdb package.

In either case, ensure that the `marimba.tuner.rpc.cert.id` property in the profile is also updated with the value of new certificate and that the profile is updated on the endpoint.

## When Client and root certificates expire on the endpoint

When the client and root certificates expire on the endpoint, update the package you created for the certdb file:

- 1 Import the new SSL certificate to the Master tuner (or test tuner) and enable SSL which will update the certdb file.
- 2 Repackage the new certdb file as described in “To package and deploy certdb” on page 53 and republish the package to the transmitter.
- 3 In the endpoint profile, edit the value of the `marimba.tuner.rpc.cert.id` property with certificate id of the new certificate. Also update the `marimba.tuner.rpc.certpw` property if there is a change in the tuner certificate password to the new password in base64 format.
- 4 Update the pre-installed package on the endpoint or let the endpoints update themselves based on the package update schedule.
- 5 Update the Infrastructure Service channel and start it.

When the endpoints receive the updates to the package, the old certdb file is replaced with the new one.

---

Note: Do not distribute one certificate at a time because `certdb` contains both the certificates (SSL & Client).

---



Section

# III System Settings

Section 2 discusses the following topics:

- “Common Management Services basics” on page 59
- “Getting started with CMS and the console” on page 65
- “General settings” on page 71
- “User authentication and roles” on page 125
- “Configuring data sources” on page 139
- “Setting up access control lists” on page 161
- “Action Request System settings” on page 185
- “Working with web services” on page 189
- “Troubleshooting system settings” on page 193



Chapter

# 4 Common Management Services basics

This chapter introduces you to the Common Management Services (CMS) application and explains the role it plays in a BMC Marimba Client Automation system. It describes the different ways you can configure and administer CMS in your enterprise.

The following topics are provided:

- CMS overview (page 60)
- Console and command-line interfaces (page 60)
- System settings overview (page 61)

## CMS overview

Common Management Services provides a foundation on which BMC Marimba Client Automation browser-based applications run, for example, the Report Center and Policy Manager applications. It provides the browser-based interface, or *console*, through which you use the applications. CMS lets you configure system settings, which apply to all the browser-based applications.

The CMS channel must be running on a tuner for the other application channels to run; the application channels must run on the same machine as the CMS channel. You can move among the applications. Usually, the CMS channel and the application channels start automatically when the tuner is started.

When the CMS channel is running on a machine, the CMS or console icon  usually appears in the task bar. You can right-click the icon and then do either of the following:

- Select **Launch Console Window** to open a browser window, log in to the console, and use the BMC Marimba Client Automation browser-based applications.
- Select **Exit** to stop the CMS channel and all the BMC Marimba Client Automation browser-based applications.

## Console and command-line interfaces

You can configure the following system settings through the console (browser-based interface) or the command-line interface:

- The port number used for accessing applications from a browser
- The bind address for the network interface for which you want the browser-based applications to accept requests
- The emergency administrator password
- The directory where the system-settings configuration files are stored
- The directory where the log files are stored
- The maximum number of simultaneous connections allowed by the HTTP server
- Whether SSL is enabled or disabled and the SSL certificate to use

All other system settings can be configured from the console only.

For a list of the command-line options, see the command-line section. The procedures provided in this document assume that you are using the console. For some procedures, the command-line options are provided.

## System settings overview

System settings let you provide information and set configurations that apply to all the applications. They are grouped in the following categories:

- **General settings.** These settings let you start, stop, and update applications. They include options for configuring the inactive user timeout, the browser access port number and host name, SSL, connections and timeouts, the location and the rollover policies for log files, email notifications, and Deployment Manager integration.
- **User authentication settings.** These settings determine how users are authenticated when they log in to use the applications. These include options for configuring the user authentication type, the local user database, user role mapping, and the emergency administrator password.
- **Data source settings.** These settings specify the sources where the applications get and store data. These include options for configuring the directory services, databases that you want the applications to use, and the LDAP-to-database synchronization service.
- **Access control settings.** These settings specify user permissions.
- **Action Request System settings.** These settings specify the sources for connecting to the Action Request System. These include configuring the connections to the AR System server, mid tier, and database.
- **Web services settings.** This page displays a list of the available web services. This includes an option to start or stop a service.

Usually, you want to configure the system settings immediately after installation and before you start using the applications.

## Configuring System Settings before using applications

It is recommended that you set the following system settings before using the applications:

**User authentication settings.** If many users access the applications, you might want to configure user authentication settings for several reasons:

- To give each user a user name and password for logging in to use the applications
- To assign roles to users and groups
- To give users and groups the appropriate permissions for performing tasks

You can use either a local user database or a directory service, such as Active Directory, Active Directory Application Mode (ADAM) / AD LDS, or Sun ONE Directory, to configure user authentication settings. For more information, see “Using a local user database or a directory service” on page 129.

For information about creating user and group accounts, see:

- “Selecting the user authentication type” on page 127
- “Adding users to the local user database” on page 130
- “Adding or editing a directory service” on page 144
- “Mapping roles to groups in a directory service” on page 136
- “Selecting the user authentication type” on page 127

**Database settings.** If you use applications that use a database to store information, such as Report Center, you should configure one or more databases so that they are available for use by applications. For information, see “Adding or editing a database” on page 156.

**Directory service settings.** If you use applications that use a directory service to store information, such as Policy Manager, you should configure directory service settings so that it is available for use by applications. For information, see “Managing directory services” on page 144. In addition, you might want to use the directory service for user authentication.

**Emergency administrator password.** When you first logged in to use applications, you used the user name `admin` with a blank password because the emergency administrator password was not set. You should set an emergency administrator password to prevent unauthorized users from logging in using the user name `admin`.

The emergency administrator password lets you and other users log in and use applications even if the directory service (or the local user database used for authenticating users) is not available. For information, see “Setting an emergency administrator password” on page 138.

**Action Request System settings.** If you are going to use the Action Request System, you should configure the ARS settings. For information, see “Action Request System settings” on page 185.



Chapter

# 5 Getting started with CMS and the console

This chapter discusses starting and using CMS and the console in your enterprise.

The following topics are provided:

- Logging in to the console for the first time (page 66)
- Logging out of the console (page 66)
- Console navigation (page 67)
- The Getting Started page (page 68)
- CMS and cookies (page 69)

## Logging in to the console for the first time

After you have installed CMS and other applications and the channels have started automatically, you log in for the first time.

### ► To log in for the first time

- 1 Open a browser and enter `http://<machine_name>:<port>`

where `<machine_name>` is the name of the machine where the applications are installed, and `<port>` is the browser access port number. The default port is 8888.

- 2 In the User name field, enter `admin`. Leave the Password field empty.

This is the emergency login name and password. You should later reset this for security. For more information, see “Setting an emergency administrator password” on page 138.

- 3 Click Log In.

On the Getting Started page, you can start using the console and applications by selecting from the Applications list.

## Logging out of the console

You can log out in two ways, automatically and manually.

### ► To log out automatically

For security, if you do not use the console for 60 minutes, you are automatically logged out. The next time you click a button, the login box prompts you to log in again. If you want to change the 60 minute setting, see “Setting the user timeout” on page 77.

### ► To log out manually

- Click Logout.

If you do not log out and then change the browser window, you are still logged in. For security, it is a good practice to log out and close the browser window.

# Console navigation

This section describes the navigational items that appear at the top of the console. The items appear in the same place regardless of the page you are in or application you are using.

- **Applications.** This list lets you go to the application that you want to use. If you are in one application, you can use the list to switch to another application. The system settings are in this list at Applications > Console > System Settings.
- **Status.** This link displays information about the currently logged-in user. For more information, see “Viewing status information” on page 68.
- **Toggle info Text.** This link lets you show or hide informational (info) text on the console pages. For example, new users can see the info text for guidance, while advanced users can hide the info text.
- **About.** This link opens a separate browser window that displays the available applications and their version numbers.
- **Logout.** This link lets you log out of the console. It brings you to the login page.
- **Help.** This link opens a separate browser window that displays context-sensitive help information.

---

Tip: To best view the console and applications, set the resolution on the monitor to 1024 x 768.

---

## Switching between applications

After logging in to the console, you can use the applications that are available to you.

### ► To switch between applications

- Click Applications and select an application from the list.

If an application is not yet running, use the Applications Manager page to start it. For information, see “Starting and stopping applications” on page 72.

If you want to configure settings that apply to the console and the applications, choose Applications > Console > System Settings.

## Viewing status information

Status information appears when you move the mouse pointer over the status information item  . Status information identifies:

- The application the user is in or system settings, as appropriate.
- The name of the user currently logged in.
- The role of the user currently logged in.

Viewing status information while using one of the applications lets you see additional application-specific information. For example, if you are using Policy Manager, you see the name of the directory service that Policy Manager is using to store and access information.

## The Getting Started page

The Getting Started page is the default entry page. Here you can set console preferences, read information about roles and system settings, and access Customer Support and documentation sites.

To return to the Getting Started page, choose Applications > Getting Started.

## Setting console preferences

You can set the following preferences for the console:

- The application that you want to start in when you log in to the console
- Whether informational (or info) text appears in the browser-based interface of the console and the applications

### ► To set console preferences

- 1 Choose Applications > Getting Started and go to the Your Preferences section.
- 2 In the Choose your starting application section, select the application that appears after login.

For example, you can select the application that you use most frequently. In addition, you can choose the Getting Started page (the default) or the System Settings page. The System Settings page lets you configure settings that apply to the console and the applications.

- 3 In the Toggle info text section, select Show info text or Hide info text.

For example, you can show info text if you are a new user and want to see introductory text and additional information for the pages in the different applications or you can hide info text if you are an advanced user.

- 4 Click Apply Preferences to save the changes.

## Roles and system settings information

**Roles.** The system currently supports three roles: primary administrator, administrator, and operator. These roles allow or limit access to product features. Depending on your role, certain pages or tabs might be hidden or unavailable to you. Configuration pages are reserved for primary administrators only. When you log in to the system, your role is assigned based on the user name and password you provide.

**System Settings.** System settings are used by all installed applications and can be accessed from the Applications list in the banner (Applications > Console > System Settings). Only a primary administrator or the person who installed the product can configure system settings.

## Customer support and documentation links

**Customer Support** gives the link to send an email to Customer Support.

## CMS and cookies

CMS stores information in a small text file, called a cookie, on the hard disk. CMS uses cookies to keep track of session information for users who log in to use the browser-based applications. For example, the cookie can include the user name that you used to log in and whether you want info text to be displayed on the browser-based GUI.

The browser you use should be configured to accept cookies. If the browser has been configured not to accept cookies, CMS and the applications that run on top of it might not function correctly.



# General settings

This section describes how to configure general system settings for the console and browser-based applications.

The following topics are provided:

- Managing applications (page 72)
- Setting the user timeout (page 77)
- Setting the browser access port and bind address (page 78)
- Configuring the console to use SSL (page 79)
- Working with performance settings (page 81)
- Managing log files (page 83)
- Configuring email notifications (page 85)
- Configuring FTP upload settings (page 86)
- Restarting CMS and the console (page 87)
- Updating CMS and the console (page 88)
- Configuring Deployment Manager Integration settings (page 88)

---

Note: You must be logged in as a primary administrator. To see the login status, place the mouse pointer over the Status icon.

You specify primary and standard administrators during installation and configuration. For more information, see “What are user roles?” on page 126.

---

# Managing applications

This section describes how you can manage the applications running on top of CMS.

This section contains the following topics:

- “Viewing information about applications” on page 72
- “Starting and stopping applications” on page 72
- “Updating applications” on page 73
- “Subscribing to new applications” on page 75
- “Removing applications” on page 76

## Viewing information about applications

You can find out which applications (and versions) you have from most pages in the browser-based applications.

### ► To view information about the applications

- At the top of the browser window, click About.

A browser window shows the applications you have installed and the version number for each one. If you want to see the status of each application, go to the Applications Manager page (see “Starting and stopping applications” on page 72).

## Starting and stopping applications

You can view which applications you have and what their current status is from the Applications Manager page. You can start and stop applications.

### ► To start or stop applications

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the Applications Manager link.

The Applications Manager page lists the applications that you have and shows their current status.

- 3 If you want to start an application that is not running, in the Actions column for the application, select Start.
- 4 If you want to stop an application that is currently running, in the Actions column for the application, select Stop.

The status changes from running to subscribed. The application is not available until you start it again.

The status changes from subscribed to running.

- 5 Click Refresh to display the latest status of the applications.
- 6 Click OK to return to the General Settings page.

## Updating applications

You can update applications from the Applications Manager page after you download a newer version from a transmitter. You can use the source transmitter or one from a different location, for example, after you move an application from one transmitter to another.

You can see the channel URL, including the transmitter, by holding the mouse pointer over the application name.

After you update a channel that is accessed through the IE browser, clear the IE browser Internet cache to make sure the cache gets the new content.

---

**WARNING:** If the applications that you select for the update are currently running, they are automatically restarted if any updates are found and installed. You might want to warn anyone currently using these applications before you start the update.

---

### ► To update an application from the source transmitter

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the Applications Manager link.

The Applications Manager page lists the applications that you have and shows their current status.

- 3 Locate the application, and under the Actions column, choose Update.

The application downloads and installs any updates from the source transmitter.

- 4 If you want to display the latest status of the applications, click Refresh.
- 5 Click OK.

This procedure only updates the application itself. You might need to perform other tasks specific to an application when updating to a newer version. For more information, see the upgrade section of the *BMC Marimba Client Automation Installation Guide*.

#### ► To update an application from a different URL

- 1 Choose Applications > Console > System Settings and then click the General tab.

- 2 Click the Applications Manager link.

The Applications Manager page lists the applications that you have and shows their current status.

- 3 Locate the application, and under the Actions column, select Stop.

- 4 Make sure the application has a Subscribed (not Running) status. If necessary, click Refresh.

- 5 Under the Actions column, select Update from.

You are prompted for the new URL. The current URL is usually displayed.

- 6 Enter the new URL for the application.

The application checks for an update from the URL you specified and downloads the update. If the URL is not valid, you get an error message and the console changes the URL back to the original URL.

- 7 Make sure the application has a Subscribed (not Updating) status. If necessary, click Refresh.

- 8 To restart the application, under the Actions column, select Start.

- 9 Click OK.

This procedure only updates the application itself. You might need to perform other tasks specific to an application when updating to a newer version. For more information, see the upgrade section of the *BMC Marimba Client Automation Installation Guide*.

## Subscribing to new applications

You can subscribe to new applications and add them to the console from the Applications Manager page. An application comes in the form of a channel.

Make sure that the channel you subscribe to is an application that was designed to run on the console, for example, Schema Manager, Infrastructure Administration, Patch Manager, Report Center, and Policy Manager. Although you can see other types of channels when you browse a transmitter, subscribing to those channels only subscribes them to the tuner and does not make them appear on the console.

Before you can subscribe to a new application, you must know either

- The URL for the application

For example, `http://server:5282/Marimba/Current/ReportCenter`.

- The host name and port number for the transmitter that hosts the application

For example, `http://server:5282`.

### ► To subscribe to a new application

1 Choose Applications > Console > System Settings and then click the General tab.

2 Click the Applications Manager link.

The Applications Manager page lists the applications that you have and shows their current status.

3 Click Subscribe to a New Application.

4 If you know the URL, in the Application URL field, enter the URL for the channel.

The URL usually consists of the host name of the machine on which the transmitter is running, the port number for the transmitter, the name of any folders, and the name of the channel, for example, `http://server:5282/Marimba/Current/ReportCenter`.

- 5 If you do not know the URL, you can browse for an application.
  - a Click Browse.
  - b In the Connect to field, enter the host name and port number for a transmitter, and click Go.
  - c Choose an application and click Select. The URL appears in the Application URL field.
- 6 If the application comes from a transmitter with restricted access, enter the subscribe user name and password.
- 7 Click Subscribe.

When the Applications Manager page refreshes, the application appears on the page with the status Running.
- 8 If the application does not automatically start running, under the Actions column, select Start.

The status changes from Subscribed to Running.
- 9 Make sure the application has a Subscribed (not Running) status. If necessary, click Refresh.
- 10 Click OK.

## Removing applications

You can remove applications from the console using the Applications Manager page.

Before you remove an application, make sure you have backed up the information you want to keep. Make sure you inform users who might be using the application before you remove it.

### ► To remove applications

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the Applications Manager link.

The Applications Manager page lists the applications that you have and shows their current status.

- 3 For the application, under the Actions column, select Stop.

When the Applications Manager page refreshes, the application has the status Subscribed.

- 4 For the application, under the Actions column, select Remove.

When the Applications Manager page refreshes, the application has the status Removed or Removed from the page.

- 5 Click OK.

## Setting the user timeout

You can configure applications to automatically log out users who have been inactive or idle for a certain amount of time. This helps prevent unauthorized access to applications. Users must log in again before they can continue using applications.

The user timeout that you set applies to all users who log in to access applications. You cannot specify a different timeout for different users.

If you change this setting, the new timeout does not apply to users who are already logged in, but takes effect the next time users log in.

### ► To set the timeout for users

- 1 Choose Applications > Console > System Settings and then click the General tab.

- 2 Click the User Timeout link.

- 3 In the field, enter the number of minutes you want to wait before logging out idle users. The default is 60 minutes.

It is recommended that you enter a value between 0 and 1000.

- 4 If you want to disable the timeout, enter 0.

- 5 Click OK.

# Setting the browser access port and bind address

This section contains the following topics:

- “What is the browser access port?” on page 78
- “What is the bind address?” on page 78
- “Changing the browser access port and bind address” on page 78

## What is the browser access port?

The browser access port is the port number to use for accessing applications through a browser. The default is 8888.

If you have any firewalls between applications and the target endpoints, make sure that the firewalls allow access to this port. The service channels on the target endpoints send data back to applications, so it is important that the target endpoints can resolve both the host name and the browser access port for applications.

## What is the bind address?

The bind address represents the network interface on which you want the browser-based applications to accept requests. You specify a bind address only if the machine on which you are running the applications has more than one network interface. You can specify one or all network interfaces.

For example, the machine on which you are running the applications has two network interfaces: one allows access from the intranet and the other allows access from the Internet. If you want to allow access to the applications only from the intranet, specify the bind address as the network interface that allows access from the intranet. If you want to allow access to the applications from both, select the “Bind to all interfaces” option.

## Changing the browser access port and bind address

You can change the browser access port and bind address from the console. For information on the specific topics, see “What is the bind address?” on page 78 and “What is the browser access port?” on page 78.

**Command-line.** For information, see the `-setPort`, `-getPort`, `-setBindAddress`, and `-getBindAddress` options in the command-line section of the *BMC Marimba Client Automation Reference Guide*.

## ► To change the browser access port and bind address

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the Browser Access Port and Bind Address link.
- 3 In the Bind address field, select one of the following options to allow access to the applications:
  - a From a specific network interface, select that interface.
  - b From all available network interfaces, select Bind to all interfaces.

You only need to specify a bind address if the machine has more than one network interface.

- 4 In the Browser access port field, change the port number as necessary.  
The default is 8888.
- 5 Click OK.
- 6 Confirm the changes and then click OK.  
If you selected “Bind to all interfaces,” the bind address appears as 0.0.0.0.  
The browser-based applications restart. This might take up to one minute.
- 7 After the restart, choose Applications > Getting Started to begin using the new settings.  
If you try to go to the Getting Started page before the restart is complete, you might get an error message. Refreshing the page usually solves the problem.

## Configuring the console to use SSL

If you want to encrypt communication between the browser and the console server, you must obtain and install a Secure Sockets Layer (SSL) certificate on the console server. The console server is the machine that hosts the tuner on which CMS and browser-based applications, such as Report Center, are running.

To request and install a certificate, use Certificate Manager. Information for requesting, installing, and importing certificates, and for setting the certificate to be trusted for SSL, appear in the Certificate Manager Help (click the Help button from within Certificate Manager). Certificate Manager might be limited to a group of users in your company, such as system administrators.

**Command-line.** For information, see the `-getSSLCert`, `-setNoSSL`, and `-setSSL` options in the command-line section of the *BMC Marimba Client Automation Reference Guide*.

#### ► To configure the console to use SSL

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the SSL Settings link.
- 3 Select Use SSL and then specify the SSL certificate and password.

If no SSL certificates appear on this page, you must install one on the machine running the console. Use Certificate Manager to install the certificate as described in Certificate Manager Help.

- 4 Click OK.

The URL for connecting to the console changes from http to https.

#### ► To configure the console to not use SSL

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the SSL Settings link.
- 3 Select Do not use SSL.
- 4 Click OK.

If you were using SSL, the URL for connecting to the console changes from https to http.

## Properties for supplying SSL client-certificate information

Use the following properties to supply the required SSL client-certificate information when you do not see the client-certificate dialog box.

For example, the tuner on which the CMS channel is running communicates with Active Directory through an SSL connection. Because you set the tuner to run in silent interaction mode, the client-certificate dialog box is suppressed. You must then supply the information using properties.

You can set the properties in Tuner Administrator (choose Applications > Infrastructure > Tuner Administration, log in and click Edit Settings, and then click the Custom Properties tab) or by manually editing the `prefs.txt` file.

- `marimba.security.sslcert`—Set to the Certificate Manager certID string (for example, `o4H7G0-Wf6FaW-0ljRib-pvsQ==`) for the tuner's default client certificate. When this property is set, the tuner always uses the corresponding certificate when client-certificate authentication is requested.
- `marimba.security.cert.password.timeout`—The number of seconds before client-certificate passwords time out. The default is 1 hour. Specify `-1` to indicate no timeout.
- `marimba.security.clientcertpw`—Set to the default base 64-encoded password (for example, `base64:bWFyaW1iYQ\=|=`) for the client certificate used by the tuner.

## Working with performance settings

CMS acts as an HTTP server that processes requests sent to it and the applications that run on top of it. The Performance page lets you configure settings that determine how CMS processes requests. There are two types of performance settings you can configure.

- **Maximum concurrent connections.** The maximum concurrent connections allowed by the HTTP server. You might want to increase the number of concurrent connections if you experience problems with users being refused connections.

- **Timeouts.** The amount of time (in seconds) that a connection can be idle during each state that CMS goes through while processing an HTTP connection before CMS drops the connection. Typically, an HTTP connection goes through three states:
  - **Reading state.** CMS reads and parses the request header.
  - **Writing state.** CMS generates a response to the request.
  - **Processing state.** CMS processes the request and dispatches it to the corresponding handler. Logic is invoked.

You might want to increase the read and write timeouts if you experience problems with dropped connections over slow links. You might want to increase the processing timeout if you experience problems with dropped connections while an application is handling a request.

### ► To change the performance settings

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the Performance Settings link.
- 3 If necessary, change the number of connections in the Maximum concurrent connections field. The default is 1024 connections.
- 4 As appropriate for each state, change the number of seconds that a connection can be idle before CMS drops the connection:
  - Read timeout. The default is 60 seconds.
  - Write timeout. The default is 60 seconds.
  - Processing timeout. The default is 120 seconds.
- 5 Click OK.

**Note:** If you are using Internet Explorer, leaving the “Check for newer versions of stored pages” option (Tools > Internet Options > General > Settings) at the default setting “Automatically” is recommended. Changing the setting to “Every visit to the page” generates many HTTP requests for pages, which might affect CMS performance.

# Managing log files

This section describes the log files and explains how you can manage them. It contains the following topics:

- “Log files for the applications” on page 83
- “Setting where log files are stored” on page 84
- “Setting the log file rolling policies” on page 85

## Log files for the applications

*History log files* record any errors that occur when you are using the browser-based interface or the command-line interface for applications. *Access logfiles* record the applications into which users are logging in. For information, see “History log files” on page 83 and “Access log files” on page 83.

### History log files

Like all other BMC Marimba Client Automation channels, the channels for the browser-based applications have a history log that records the events and errors that occur when you use the application. The events include starting, stopping, and updating the channel, and events that are specific to each application.

All the log messages for the BMC Marimba Client Automation browser-based applications are recorded in the log files maintained by CMS. For more information, see “Setting where log files are stored” on page 84 and “Setting the log file rolling policies” on page 85.

### Access log files

The access log files record which browser-based applications that users log in to when going through a browser. The access logs are contained in the logs maintained by CMS. For more information, see “Setting where log files are stored” on page 84 and “Setting the log file rolling policies” on page 85.

The following entries are examples from an access log:

```
123.45.6.789 - - [12/Nov/2005:14:11:01 -0800] "GET /shell/settings/appmgr.do 1001" 200 24701 477 1 0 "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)"  
123.45.6.789 - - [12/Nov/2005:14:11:01 -0800] "GET /shell/common-rsrc/js/table.js 1001" 304 83 457 1 0 "Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0)"
```

```
123.45.6.789 - - [12/Nov/2005:14:11:01 -0800] "GET /shell/common-
rsrc/css/main.css 1001" 200 32211 408 1 10 "Mozilla/4.0 (compatible;
MSIE 5.5; Windows NT 5.0)"
123.45.6.789 - - [12/Nov/2005:14:11:01 -0800] "GET /shell/common-
rsrc/css/tooltips.css 1001" 304 83 462 1 0 "Mozilla/4.0 (compatible;
MSIE 5.5; Windows NT 5.0)"
123.45.6.789 - - [12/Nov/2005:14:11:01 -0800] "GET /shell/common-
rsrc/images/arrow.gif 1001" 304 83 462 1 0 "Mozilla/4.0 (compatible;
MSIE 5.5; Windows NT 5.0)"
123.45.6.789 - - [12/Nov/2005:14:11:01 -0800] "GET /shell/common-
rsrc/images/blue/banner_top.gif 1001" 304 83 472 1 0 "Mozilla/4.0
(compatible; MSIE 5.5; Windows NT 5.0)"
123.45.6.789 - - [12/Nov/2005:14:11:01 -0800] "GET /shell/common-
rsrc/images/black_arrow_down.gif 1001" 304 83 473 1 0 "Mozilla/4.0
(compatible; MSIE 5.5; Windows NT 5.0)"
```

The IP address at the beginning of each line is the IP address of the machine that is accessing the browser-based application. It is followed by the date and time when the event occurred. The paths, such as /shell/settings/appmgr.do, indicate which page of the browser-based application is being accessed.

## Setting where log files are stored

Log files for applications are stored in the tuner workspace directory. You can see and change the path by looking on the Log Files page.

Log files are stored on the machine on which the tuner and the CMS channel are running. This machine might not be the machine on which you are viewing the console (browser-based graphical user interface).

**Command-line.** For information, see the `-setLogDir` and `-getLogDir` options in the command-line section of the *BMC Marimba Client Automation Reference Guide*.

### ► To set where log files are stored

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the Log Files link.
- 3 To see the path, look in the Location of log files field at the top of the page.
- 4 If you want to change the directory location, make any changes in this field.
- 5 Click OK if you made any changes; otherwise, click Cancel.

## Setting the log file rolling policies

The log file rolling policies for applications set how often to start a new log file and how many versions of log files to keep. You set the rolling policies individually for history log files and access log files.

### ► To set the log file rolling policies

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the Log Files link.
- 3 For the access log file, select a log file rolling policy.
  - Never roll
  - Roll <hourly, daily, weekly, monthly, yearly>
  - Roll when they reach this size: (enter the size in kilobytes)
- 4 Specify the number of log file versions that you want to keep.
- 5 For the history log file, select a log file rolling policy.
  - Never roll
  - Roll <hourly, daily, weekly, monthly, yearly>
  - Roll when they reach this size: (enter the size in kilobytes)
- 6 Specify the number of log file versions that you want to keep.
- 7 Click OK.

## Configuring email notifications

Applications that run on top of CMS, such as Report Center, can send email notifications with attachments after certain actions or events. To enable email notifications, you must configure these settings in the CMS console. You can also set the user name and password needed if your SMTP server requires authentication.

When you set email body and attachment sizes, remember that the actual sizes depend on network load considerations and the mail server capacity. For information, see the Simple Mail Transfer Protocol (SMTP) administrator.

## ► To configure email notifications

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the E-mail Notifications link.
- 3 In the Mail server field, enter the host name of the mail server. For example: smtp.company.com

This mail server is usually an SMTP server.
- 4 Enter the port number for the SMTP server. The default is 25.
- 5 If your SMTP server requires authentication, click the Use Authentication check box and enter the required user name and password for the SMTP server.
- 6 If you want to set the email body size, in the Maximum size of email body field, enter a size in MB. The default is 1 MB.
- 7 If you want to set the attachment size, in the Maximum size of email attachments field, enter a size in MB. The default is 5 MB.
- 8 Click OK.

Depending on the applications you have, you must specify additional information, such as the email address that you want to send notifications to and the events after which notifications are sent.

## Configuring FTP upload settings

In BMC Marimba Client Automation, some of the applications can upload data to an FTP server. For example, Report Center can upload query results to an FTP server.

The following task describes how to specify an FTP server in the CMS console to which participating applications can upload data.

## ► To configure FTP upload settings

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the FTP Upload Settings link.
- 3 From the FTP Upload Settings page, enter or select the appropriate values for the FTP Server Settings in the following fields:

- FTP Server (name or IP address)
  - Server Port (defaults to 21)
  - Connect Anonymously (click to allow anonymous FTP)
  - Username (for the FTP server; dimmed when “Connect Anonymously” is checked)
  - Password (for the FTP server; dimmed when “Connect Anonymously” is checked)
  - Upload Directory (where the uploaded data will reside on the FTP server)
- 4 To use a proxy, select the one of the following options:
- Do not communicate with the Server via proxy (default value)
  - Use the default proxy settings in the Tuner (click to use the tuner’s settings)
  - Use the following proxy settings (click to specify a proxy)
    - Proxy Server
    - Proxy Port
    - Connect Anonymously
    - Username (for the Proxy server; dimmed when “Connect Anonymously” is checked)
    - Password (for the Proxy server; dimmed when “Connect Anonymously” is checked)

## Restarting CMS and the console

You must restart CMS and the console after you change certain some settings; you are usually prompted to do so. You should warn users who are using the system before you restart CMS because this also restarts the browser-based applications that run on top of it.

### ► **To restart the console**

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the Restart the Console link.

You are prompted to confirm that you want to restart the console.

- 3 Click OK.

CMS and all the applications that run on top of it restart. Anyone using the console or the applications is automatically logged out and must log in again.

## Updating CMS and the console

When a new version of CMS and the console becomes available, you can use the Applications Manager page to update to the newer version. You should warn users who are using the system before you update CMS because this also restarts the console and the browser-based applications that run on top of it.

### ► To update CMS and the console

- 1 Make sure that the new version of CMS has been published to the transmitter in the same location where you subscribe to CMS.
- 2 Choose Applications > Console > System Settings and then click the General tab.
- 3 Click the Applications Manager link.

The Update the console section near the bottom of the page shows the current version of the console.

- 4 Click Update Console .

The console and all the applications that run on top of it restart. Anyone using the console or the applications is automatically logged out and must log in again.

## Configuring Deployment Manager Integration settings

You can configure the console to integrate with Deployment Manager. Applications that run on the console, such as Policy Manager, can then communicate with Deployment Manager.

### ► To configure Deployment Manager Integration settings

- 1 Choose Applications > Console > System Settings and then click the General tab.
- 2 Click the Deployment Manager Integration Settings link.

3 Complete the following Deployment Manager-related fields:

- **Tuner host name and port number**—Host name and port number for the tuner on which the Deployment Manager channel is running. The default is `http://localhost:7717`.
- **User name and password**—User name and password for accessing Deployment Manager. Deployment Manager must have been configured to give access to this user. The default user name is `admin`.
- **Console port number**—Port number used to access Deployment Manager. The default is 8000.
- **Active limit**—Maximum number of active endpoints in a group that can process the job at the same time. The default value is 50. If you have more than 50 endpoints in a group, it is recommended that you set this limit to 50. If this value is not set, the value set in Deployment Manager is used.
- **Quorum**—Percentage of endpoints in each deployment that must succeed for the deployment to report success. The default value is 0. When the quorum is set to 0, the deployment continues for all the endpoints in the group regardless of how many endpoints have already failed or succeeded. If this value is not set, the value set in Deployment Manager is used.

4 Complete the following endpoint-related fields:

- **Tuner user name and password**—Remote administration user name and password for the endpoint tuners to which Deployment Manager connects. The user name and password were assigned to the endpoint tuners either when creating the tuner installers or when connecting to the tuners using Tuner Administration.
- **Response timeout**—Number of minutes that Deployment Manager waits for communication from a target endpoint before assuming that the tuner on that endpoint is not responding. (In Deployment Manager, this is the server response timeout.) Deployment Service on each target server sends a “Server processing ...” message back to Deployment Manager at the intervals that you specify. The default is 5 minutes.

5 Click OK.



Chapter

# 7 Multi-Tenancy

The following topics are provided:

- Introduction (page 93)
  - What is a tenant? (page 93)
  - Key features (page 94)
  - Support for Multi-Forest (page 95)
  - Advantages of Multi-Tenancy (page 95)
  - Default environment in 9.0.00 (page 96)
  - What happens when you upgrade to 9.0.00? (page 96)
- Architecture of Multi-Tenancy (page 97)
  - How tenants are managed? (page 97)
  - How to use the Application Permissions tab to specify access permissions for tenant administrators to web application channels (page 97)
  - Different types of deploying Marimba infrastructure (page 98)
  - Tenant specific properties (page 99)
  - Using command-line to perform operations in a Multi-Tenant environment (page 100)
  - Using the database in a Multi-Tenant environment (page 100)

- Schema Manager Channel changes to support Multi-Tenancy (page 102)
- Multi-Tenancy changes in Infrastructure Administration (page 105)
- Different scenarios while deploying Marimba 9.00.00 (page 106)
  - Upgrading to 9.0.00 (page 106)
  - Using 9.0.00 for the first time - a fresh installation (page 107)
  - Deploying Marimba 9.0.00 on cloud (page 108)
- User Roles (page 112)
  - Role of Emergency Administrator or Super Administrator (page 112)
  - The role of Primary Administrator (page 113)
  - User roles in a Multi-Tenancy (page 114)
- Configuring a tenant (page 117)
  - Workflow of configuring a tenant (page 117)

# Introduction

In this era of mergers and acquisitions, there are many organizations which internally consist of more than one small organization. However, usually during and after the acquisition, all the IT infrastructure is controlled by a single command and control center which provides several advantages. Having a single command and control center for the whole organization is very effective as it leads to a lot of cost savings in terms of redundant efforts, and IT hardware and infrastructure. It is also leads to optimum use of Marimba Infrastructure, particularly if you are using Marimba 9.0.00.

In this scenario, one of the challenges for any IT infrastructure is to have a common command and control center from where you can control and monitor all the sub-organization's IT infrastructure.

Marimba's Multi-Tenancy feature in 9.0.00 provides administrators with a facility to have a common Marimba command and control center from where they can control the whole organization's IT infrastructure.

The Multi-Tenancy feature allows you to control more than one organization's infrastructure using a single CMS console. This feature also helps any Marimba service provider control infrastructure of different organizations using a single CMS.

Note:

By default, Marimba 9.0 is in Single Tenant model. For more information refer Upgrading to 9.0.00 (page 107).

## What is a tenant?

Any organization which wants to manage their infrastructure with this Multi-Tenant capable CMS feature is referred to as Tenant. The tenant can also refer to any sub-organizations within an organization.

## Who can create a tenant?

Only a Super Administrator can create a tenant.

## Who is a Super Administrator?

The super administrator is the term given to the administrator who can access the console when CMS is installed or updated. The Super Administrator has the primary responsibility of creating, editing or removing tenants. This responsibility involves tasks such as creating tenant-specific rights to applications in the console, configuring a database for the exclusive use of the tenant, and customizing console properties. The Super Administrator also creates the initial credentials for a tenant's administrator so that the tenant's administrator can access his specific view of the console.

The Super Administrator's default role is restricted to only tenant management as described above. However, for some scenarios configuration changes can be made to allow the primary administrator access to system setting related pages and to access CMS web applications.

---

Note: When managing multiple tenants using the same console, it is necessary to ensure that all tenants are on the same Marimba version.

---

The Super Administrator performs the role of Emergency Administrator but has the additional privileges to create, and activate or deactivate, tenant and also configure settings such as the database for each tenant.

### Best practice

It is recommended to plan for upgrade of all tenants at the same time.

## Key features

The key features of Multi-Tenancy are:

- Marimba IT infrastructure service provider can control several tenants using the same CMS.
- The Multi-Tenant feature is completely cloud compatible.
- In a cloud environment, this feature can support separate database servers per tenant. It can also support a single database server hosting multiple tenant-specific database instances.
- Cloud environments can also support hosting tenant specific folders in the same server Transmitter; configuring tenant specific authentication to lock content from other customers tenants is also supported.

- Most CMS applications and services like Report Center, Policy Manager now support multi-tenancy use cases such as tenant specific LDAPs, databases, and permissions, etc.

## Support for Multi-Forest

Multi-Tenancy supports multi-forest. You can configure each forest as a separate tenant and you can configure the database server which can be same with different instance names (database servers provides options to create different instances in a single server). This model helps achieve security over different forests' machines and is also cost effective since you use only a single database server. In this scenario you also have the flexibility for e-mail and FTP server could be same or different servers, since multi-forest environment is when there is acquiring or merging of organizations, it will be different server at initial stage and could be same later.

### If you want to manage the infrastructure of a newly acquired organization at a later time

At a later time if your organization acquires another company, and you want to manage the infrastructure of the newly acquired company, then you can create a separate tenant for the new organization. Once you have created another tenant and specified the primary administrators for the acquired organization, you can configure the settings like database and LDAP for the new tenant created.

## Advantages of Multi-Tenancy

The advantages of Multi-Tenancy feature are:

- Use only one CMS console to manage multiple infrastructures.
- Substantial cost savings in the cost of IT hardware and software such as using single database infrastructure.
- The infrastructure for all tenants can be upgraded at the same time.
- You need not apply the same hotfix or patch multiple times.
- You can deploy Marimba infrastructure on cloud to make use of the Multi-Tenancy feature to manage different customer organizations as tenants in a single cloud-based CMS.
- Enables you to share hardware and software infrastructure.

- Achieves significant cost reduction due to economies of scale.

## Default environment in 9.0.00

In Marimba 9.0.00, all environments are treated as multi-tenant. Even a single infrastructure model is treated as a tenant.

## What happens when you upgrade to 9.0.00?

Once you upgraded to 9.0, “Default-Tenant” will be created internally and all the existing server configurations will be mapped to it. You can see the tenant name as “Default-Tenant” in Status tip for the primary admin log into CMS.

---

Note: While upgrading to 9.0.00, ensure that you first upgrade the tuner and then upgrade other modules like CMS and Report Center.

---

## Change in access permissions for Super Administrator and Primary Administrator in 9.0.00

In 9.0.00, by default the Super Administrator cannot access web applications like the Report Center. The primary role of a Super Administrator is to create tenants in the Tenant Management page and configure settings such as the database for each database. The Primary Administrator does not have the required permissions to access the Tenant Management page and create tenants. The Primary Administer can only configure the schema settings of a tenant to which he/she belongs.

# Architecture of Multi-Tenancy

## How tenants are managed?

The Super Administrator can create configure and manage tenants. In the Tenant Management page, the Super Administrator can create, modify, and delete tenants. For each tenant the Super Administrator can specify details such as:

- General
- LDAP Server
- Database Server
- FTP Server
- E-mail Server
- DM Server
- Application Permissions
- Properties

## How to use the Application Permissions tab to specify access permissions for tenant administrators to web application channels

The Super Administrator can specify the list of web application channels running on the CMS console (Policy Manager, ISM, Report Center and etc. and also custom channels if any) which each tenant can access. While each tenant logs into CMS console, the Applications menu contains the web application channels chosen for that tenant.

---

Note: Custom web applications running on Multi-Tenant mode of CMS must capable of Multi-Tenancy support to work properly.

---

For each tenant, a specific directory is created using that tenant name inside each web application channel's data directory. This directory is also known as tenant directory of that web application channel. This tenant directory is created to keep the files, properties used by the respective tenants. The msf.txt file of CMS channel directory is created for each tenant to hold each tenant's settings, and this file is located inside each tenant's directory.

Note:

- Each tenant can have only one active configuration.
- Each tenant user has access to view or manage their own set of configurations.
- Each tenant user can manage only their own infrastructure.
- The Master, Mirror, Repeaters, Application Packager and other plugins like Policy Service and Inventory Service must reside inside each tenant's infrastructure.
- Each tenant will have one or more dedicated transmitter.
- For Default-Tenant, the files in the property are resides in the same location.

## Different types of deploying Marimba infrastructure

There are four different ways in which you can deploy Marimba multi-tenant enabled infrastructure:

- All the Marimba related infrastructure such as LDAP, database, e-mail and FTP servers are deployed in the tenant's location.
- All the Marimba related infrastructure such as LDAP, database, and e-mail, except FTP servers are deployed in the tenant's location. In this scenario the AR server is configured.
- All the Marimba related infrastructure such as LDAP, and e-mail except the database are deployed in the tenant's location. The database can be deployed on a cloud or in any service providers environment.

- All the Marimba related infrastructure such as LDAP except the e-mail and database are deployed in the tenant's location. The database can be deployed on a cloud or in any service providers environment.

## Tenant specific properties

The following list of CMS properties are tenant specific and reside inside each tenant's directory from 9.0.00 onwards. For upgrade environments, these properties are moved from prefs.txt to msf.txt file.

- marimba.ldap.preferreddc
- marimba.ldap.admanagementdomain
- marimba.ldap.srvdnsserver
- marimba.ldap.adsite
- marimba.ldap.querytimeout
- marimba.ldap.connectiontimeout
- marimba.ldap.queryresultsize
- marimba.wow.wakeup.strategy
- marimba.wow.filter.subnets
- marimba.wow.ping.timeout
- marimba.wow.ping.useapi
- marimba.wow.ping.retrycount
- marimba.rc.fdcc.enable

The following properties are moved from prefs.txt to cms-config.txt under CMS data directory.

- marimba.task.distribution.port
- marimba.task.distribution.enabled
- marimba.task.distribution.password
- marimba.task.distribution.groupname
- marimba.task.distribution.port.autoincrement
- marimba.task.distribution.multicast.port
- marimba.task.distribution.multicast.address

- marimba.task.distribution.tcpip.enabled
- marimba.task.distribution.tcpip.members

## Using command-line to perform operations in a Multi-Tenant environment

Starting from 8.5.00, in a multi-tenant environment, whenever you perform any actions using the command-line, you must specify the tenant name in the command argument.

For example:

- runchannel <CMS\_URL> -user <user\_name> -password <password> <option> -tenant <tenantName>
- runchannel <Policy Manager\_URL> -user <user\_name> -password <password> <option> -tenant <tenantName>
- runchannel <Report Center\_URL> -user <user\_name> -password <password> <option> -tenant <tenantName>

If you do not specify the tenant name in the command line argument, then the command fails and an exception message is displayed.

### A scenario where you need not specify the tenant name in command line argument

If you have upgraded Marimba infrastructure to 9.0.00 and you operate only a default-tenant environment (there is only one tenant which is the Default-Tenant), and the Super Administrator has the privileges of a Primary Administrator, then you (the Super Administrator and the Primary Administrator) need not specify the tenant name in the command line argument. If you do not specify the tenant name in the command, then the command is implemented for the Default-Tenant in this scenario.

## Using the database in a Multi-Tenant environment

You can deploy all of the multi-tenant capable CMS and related Marimba infrastructure within your environment. Alternatively you can also deploy on an external or internal cloud or use a service provider's environment. Wherever you deploy the database servers or any other Marimba related server, ensure that the CMS machine can access these server settings:

The cloud-enabled Multi-Tenant architecture allows you to:

- Host the database server in the tenant's location
- Host the database server on a Service Provider's environment

Note: You can use a single database server for more than one tenant by having different instances.

## Deploying SQL Server in a Multi-Tenant environment (cloud environment)

There are two different ways you can deploy and use SQL Server in a Multi-Tenant environment. The two different ways are:

- Deploy a single SQL Server

Create a separate database within the same SQL Server for each tenant. You can use multiple tenant specific databases on the same SQL Server machine. In this scenario, only the Super Administrator can install, uninstall, re-install, or update the schema. The Primary Administrator can only run maintenance scripts for the tenant to which they belong.

Super Administrator must set the following property for each tenant after installing schema and database configuration under using Tenant Management Properties:

```
marimba.tunercloud.tenantdb.system.password=marimba123$
```

Note: For SQL Server database "sa" password and for Oracle database "system" password should be set value for this property.

This property must be mandatorily set by Super Administrator for each tenant for Primary Administrator to get the access to Schema Manager page to run the Schema maintenance task.

- Deploy multiple SQL Servers and use a separate SQL Server for each tenant

In this scenario, only the Super Administrator can install, uninstall, re-install, and update the schema. The Primary Administrators can only run maintenance scripts.

Note:

- In both the preceding scenarios a Primary Administrator cannot view the database details of other tenants.

- A Primary Administrator need not know any database details such as database name and reporting and inventory connection user credentials when attempting to run maintenance scripts in their assigned database.
- In a Default-Tenant environment, a Primary Administrator can perform schema installation, upgrade, and maintenance activities.
- In a cloud environment, the Super Administrator cannot perform simultaneous installation of schemas from different browsers for different tenants.

Note:

For Multi-Tenant model (non-cloud environment)- In Multi-Tenant model, Deploy multiple SQL Servers and use a separate SQL Server machine for each tenant. Here, only the Primary Administrator can install, uninstall, re-install, or update the schema of his own tenant. Super Administrator does not have access to manage the tenant specific data base.

## Schema Manager Channel changes to support Multi-Tenancy

### Schema in Multi-Tenancy

All versions prior to Schema Manager 9.0.00 can connect to any instance name in Oracle, however Schema Manager can connect to only invdb database name in SQL Server for each tenant in different database machines. The invdb database name is the default database name in SQL Sever. With Schema Manager 8.5.00, you can choose any instance name to connect to Oracle and use any database.

You can use SQL Server database in a multi-tenant or multi-forest scenario. In this scenario, you can use either only one SQL Server Machine or multiple SQL Server Machines.

- Single SQL Server Machine

Each tenant or forest is mapped to a different database. A single database supports a maximum of 200,000 endpoints.

For example:

- Database Name: invdb\_tenant\_1 supports 50,000 endpoints
- Database Name: invdb\_tenant\_2 supports 50,000 endpoints
- Database Name: invdb\_tenant\_3 supports 50,000 endpoints

- Database Name: invdb\_tenant\_4 supports 50,000 endpoints
- Multiple SQL Server Machines

You must use multiple databases if the total number of end points exceeds 200,000 endpoints.

---

Note: Multiple DB instances are supported both in SQL and Oracle for a tenant.

---

Multi-Tenancy 9.0.00 supports:

- Multiple instances of Oracle on a single Oracle installation.
- Multiple databases on a single SQL Server instance running on a database server.

On Oracle, for each tenant you can create a separate Oracle instance on the same Oracle installation. On SQL Server, for each tenant you can create a separate database on the same SQL Server instance. On SQL Server, the default database name created is invdb but you can change this name during installation.

On command-line

On Oracle, on the command-line there are no changes made over the previous version. You can use the same steps used prior to 9.0.00 to create the database schemas on a single Oracle instance to support a single tenant environment or on multiple Oracle database instances running on a single Oracle installation to support Multi-Tenancy feature.

Starting from 9.0.00, on SQL Server, the `osql` SQL Server utility is replaced with `sqlcmd` utility.

Microsoft introduced the new command-line utility, `SQLCMD`, as a replacement for `osql` and `isql`. The `sqlcmd` utility is used to run ad-hoc queries interactively from a command prompt window, or can be used to execute a script containing T-SQL statements. The `sqlcmd` utility is a great improvement over `osql` and `isql` of older releases of SQL Server.

Migration from `OSQL` to `SQLCMD` is very simple because most of the command line switches are similar. The only difference is that `SQLCMD` support additional switches. To see the difference between them type `OSQL /?` and `SQLCMD /?` at the command prompt.

The following examples show how the related changes are effected on our command-line scripts to create multiple databases over and above the `invdb` default database name to support Multi-Tenancy.

The old command line entry with OSQL utility:

```
osql -Usa -icmd_install_inventory.sql -oinstall_inventory.log
```

The new command line entry with SQLCMD utility:

```
Sqlcmd -S <server> -v MRBA_inv_dbname="invdb"  
MRBA_hm_dbname="invdb" -U sa -P <password> -i <install/reinstall/  
uninstall sql file> -o <install/reinstall/uninstall log file>
```

Note: On the new command-line entry, a new `-v` switch is introduced to help pass the preferred database name. In this sample, we have used the default database name `invdb`.

Note:

In command-line schema installation you can only use the database name as `invdb`.

#### On Schema Manager GUI

All versions prior to Schema Manager 9.0.00 can connect to any instance name in Oracle, however Schema Manager can connect to only `invdb` database name in SQL Server for each tenant in different database machines.

From Schema Manager 9.0.00, you can choose any instance name to connect to Oracle and also use any database name to connect to SQL Server. You can change the default `invdb` name for each database name. This new feature of Schema Manager 9.0.00 allows it to work in both single and multi-tenant environments.

In both multi-tenant and single-tenant environments, each tenant supports the same number of endpoints.

Note:

Ensure to add the required CPU power, memory, and disk space to the database server if you make a change from single tenant-mode to multi-tenant mode. You can calculate the required resources based on the number of databases planned to add. For each tenant, Multi-Tenancy supports up to 200,000 endpoints.

## Multi-Tenancy changes in Infrastructure Administration

Options now exist that may not be useful to all administrators, but provide a way to take advantage of Multi-Tenancy feature. One such use case in a cloud environment where it may be required to host content of individual customers into individual folders on the same Transmitter while giving those customers the ability to set their own permissions on these folders.

The following scenario along with information how to achieve the required functionality describes how to make use of the multi-tenancy changes in Infrastructure Administration:

- The Super Administrator wishes to protect his Transmitter at the base folder level, preventing any customer from directly accessing the base folder contents.
- The super administrator can use Local User Database user with Primary Administrator access to lock down subscribe, publish, and replicate permissions on the base folder.
- The super administrator (in the process of enrolling a customer into the cloud), decides to provide a folder within the Transmitter; this becomes the single repository for any content, applications, etc., which the customer wishes to host.
- In this case, the super administrator can create a Local User Database user for the specific customer's tenant. This can then be used to lock down the tenant folder with separate credentials.
- Once the tenant administrator has got access to the cloud, they may want to associate their own public LDAP with the CMS console. They use the required CMS options to do this.
- Once this is done, the tenant administrator can connect to the Transmitter, modify their folder's authentication mechanism to use their LDAP. Once they do this, they can modify the subscribe, publish, or replication credentials of their folder to specific user or groups, or all users in their LDAP.
- The tenant's folder is now accessible only to the tenant administrator and designated users/groups in his LDAP. Similarly, every tenant who is hosting a folder on that Transmitter can roll their own LDAP-based authentication mechanism. They are only allowed to change the authentication mechanism in their own designated tenant folder.

## Different scenarios while deploying Marimba 9.0.00

The different scenarios which you may use while deploying Marimba 9.0.00 is as follows:

- Upgrading from pre-8.5.00 to 9.0.00
- Fresh Marimba 9.0.00 infrastructure deployment
- Marimba 9.0.00 on cloud

The above scenarios are explained in detail in the following topics.

## Upgrading to 9.0.00

When you upgrade to 9.0, the upgraded customer will be in Single tenant mode by default.“Default-Tenant” will be created internally and all the existing server configurations will be mapped to it.You can see the tenant name as “Default-Tenant” in Status tip for the primary admin login into CMS.

---

**Note:** While upgrading to 9.0.00, ensure that you first upgrade the tuner and then upgrade other modules like CMS and Report Center.

---

Later, if he wants to migrate to Multi tenant mode, the following property should be set in prefs.txt in CMS tuner.

***marimba.cms.mode =tenancy***

The value “tenancy” refers that the cms runs in “Multi-Tenant” mode where Schema Manager and Infra Admin are not listed for “admin” user and “admin” user can not have any functional access apart from few System Settings server configuration links.

## At a later time - if you want to manage the infrastructure of a newly acquired organization

At a later time if your organization acquires another company, and you want to manage the infrastructure of the newly acquired company, then you can create a separate tenant for the new organization. Once you have created another tenant and specified the primary administrators for the acquired organization, you can configure the settings like database and LDAP for the new tenant created. For more information, refer “User roles in a Multi-Tenancy” on page 115.

## Using 9.0.00 for the first time - a fresh installation

Consider a scenario where you are deploying Marimba 9.0.00 infrastructure for the first time. In this scenario, when the Super Administrator logs on to CMS for the first time, there is no Default-Tenant created in the Tenant Management page because this is not an upgrade scenario.

In a cloud environment, it is mandatory to assign a common password like inventory, user\_view, dbtree, madman, humuser, in a single database machine environment for installing multiple tenant database during schema installations. However, this is not applicable when the Super Administrator uses separate database machines for each tenant.

Note: At a later stage the super administrator can change the passwords in the database. If you change the passwords in database then you must update wherever in respective modules such as Report center, Logging Plugin configurations, each tenant CMS data source DB configurations etc.

Once you have deployed Marimba 9.0.00 infrastructure, you have two options:

- Use Marimba 9.0.00 infrastructure to manage a single tenant
- Use Marimba 9.0.00 infrastructure to manage multiple tenants

## Using Marimba 9.0.00 infrastructure to manage a single tenant

The workflow for deploying Marimba 9.0.00 for a single tenant is as follows:

- 1 Deploy Marimba 9.0.00 infrastructure.

- 2 Configure all settings such as database and LDAP .

For more information, refer “User roles in a Multi-Tenancy” on page 115.

## Using Marimba 9.0.00 infrastructure to manage multiple tenants

The workflow for deploying Marimba 9.0.00 for a single tenant is as follows:

- 1 Deploy Marimba 9.0.00 infrastructure.
- 2 Create multiple tenants as per the requirement.
- 3 Specify the Primary Administrators for each tenant.
- 4 Configure all settings such as database and LDAP for each tenant which you have created.

For more information, refer “User roles in a Multi-Tenancy” on page 35.

## Deploying Marimba 9.0.00 on cloud

The Multi-Tenant feature of Marimba 9.0.00 is completely cloud capable which means that you can deploy the Marimba 9.0.00 infrastructure on a cloud provided by cloud service providers such as Amazon and Microsoft.

You can deploy Marimba 9.0.00 on cloud for the following two scenarios:

- Deploy Marimba 9.0.00 on cloud to manage only a single tenant
- Deploy Marimba 9.0.00 on cloud to manage multiple tenants

## Enabling Cloud-based Multi-Tenant feature

Marimba 9.0.00 is completely cloud-enabled. You can deploy Marimba 9.0.00 on a cloud and manage your organization's infrastructure. If you want to deploy Marimba 9.0.00 on a cloud, you must specify a property.

### ► To enable Marimba 9.0.00 on cloud

- 1 Deploy Marimba 9.0.00 infrastructure on the cloud.
- 2 Once CMS is running on cloud, set the following property in the prefs.txt file:  
`marimba.cms.mode=cloud`
- 3 Restart CMS.

Marimba 9.0.00 is now cloud enabled.

#### Access restriction

- In CMS, a Tenant user will able to view configured DB details only.
- In Report Center, Tenant will not able modify DB details in all Plugin configuration page.

## Deploy Marimba 9.0.00 on cloud to manage only a single tenant

The workflow for deploying Marimba 9.0.00 for a single tenant is as follows:

- 1 Deploy Marimba 9.0.00 infrastructure on cloud.
- 2 Enable Marimba 9.0.00 on cloud using the `marimba.cms.mode=cloud` property.
- 3 Create a single tenant.

- 4 Configure all settings such as database and LDAP for the tenant which you have created.

## Deploy Marimba 9.0.00 on cloud to manage multiple tenants

The workflow for deploying Marimba 9.0.00 for multiple tenants is as follows:

- 1 Deploy Marimba 9.0.00 infrastructure on cloud.
- 2 Enable Marimba 9.0.00 on cloud using the *marimba.cms.mode=cloud* property.
- 3 Create the required tenants.
- 4 Specify the Primary Administrators
- 5 Configure all settings such as database and LDAP for the tenants which you have created. Either the Super Administrator or the Primary Administrator can configure the settings. For more information, refer “User roles in a Multi-Tenancy” on page 35.

---

**Note:** In a cloud environment, the Super Administrator cannot perform simultaneous installation of schemas from different browsers for different tenants.

---

## Logging on to CMS Console in Marimba 9.0.00

From 9.0.00 onwards, in multi-tenant and cloud environment the log-in user name should be prefixed with the tenant name that he/she belongs to. For customers who upgraded from previous version can log-in with user name alone since CMS considers logged-in user from "Default-Tenant" that was created automatically on upgrade.

For example:

■ Scenario 1: **Just upgraded to 9.0.00**

< user name>

or

Default-Tenant\<user name>

■ Scenario 2: **Multiple tenants or cloud environment**

<Tenant name>\<your user name>

Note:

If in case, Default-Tenant is removed or created with other name, then tenant name should be given while login to CMS Console.

All these options are available through the Transmitter Administration section of the Infrastructure Administration web application in CMS.

# User Roles

## Role of Emergency Administrator or Super Administrator

In Marimba 9.0.00, the Super Administrator performs the role of Emergency Administrator. In addition to performing the role of a Emergency Administrator, the Super Administrator can create a tenant and configure settings like database for each tenant. The Super Administrator can access the Systems Settings page where configuration of servers and other related settings can be performed. By default, the Super Administrator cannot access other Web applications like Report Center, Patch Manager.

For detailed information what pages the Super Administrator can access, refer User roles in a Multi-Tenancy (page 115).

---

**Note:** From 9.0 onwards , upgraded or fresh customer will be in Single Tenant mode by default and can perform the operations like prior to 8.5.x irrespective of any role like Emergency admin or primary admin.

---

## Creating a tenant

One of the important tasks of a Super Administrator is creating the tenants in a Multi-tenant environment. Only the Super Administrator has the access to create a tenant. To create a tenant, you can use the Tenant Management tab in the Settings page of CMS.

When a Super Administrator performs a any task on pages which he can access such as User Roles or Database page, the Super Administrator can perform the task only specific to a tenant. All the tasks performed in such pages are linked to a specific tenant. The Super Administrator must select the tenant in such pages prior to performing any action.

If no tenant is configured then CMS displays the following error message in red color on the page:

Before proceeding, correct the following:

There is no tenant configured, make sure at least one tenant is configured.

## The role of Primary Administrator

Prior to 9.0.00, the Primary Administrator did not have any restriction on access to any page of Web application channels or the System Settings page.

However, from 9.0.00 the Primary Administrator will have access to system settings page with restricted permission on only some features as specified in “User roles in a Multi-Tenancy” on page 115.

## Providing full access restrictions to the Primary Administrator

If the property marimba.cms.mode=default is set in the prefs.txt, can consider the infrastructure in single tenant mode. Here, Primary admin will not have any restriction on accessing the web app channels.

- Note:**
- Do not set this property if there are multiple tenants configured.
  - You also cannot use set this property if Marimba 9.0.00 is deployed on a cloud.

## User roles in a Multi-Tenancy

The following are the new roles for different types of administrators:

- Super Administrator

The Super Administrator can create and edit tenants and assign primary and secondary administrators to the tenants.

**Note:**

You cannot remove an active tenant. To remove a tenant, you must first deactivate or disable the tenant and then you can remove the tenant.

Each tenant can configure any number of LDAP servers, but can set at the maximum of one as active. In the same way, Reporting, Inventory, HM Read and HM Admin connections can be at the max of one in active per tenant. Other servers like DM, FTP, E-mail and AR are at the max of one can be configured for any tenant.

- Primary Administrator

The primary administrator cannot access the following pages and functions:

- Restart console
- Configuration of SSL/non-SSL mode
- Logged in user timeout
- Applications Manager
- Performance Settings
- Browser Access Port and Bind Address
- Emergency Administrator Password

The following table shows the matrix between the links that various types of administrators can access in Marimba:

Links	Emergency Admin	Primary Admin	Secondary Admin	Operator
<b>General tab</b>				
Log Files	✓	✓	✗	✗
SSL Settings	✓	✗	✗	✗
User Timeout	✓	✗	✗	✗
Channel Store	✓	✗	✗	✗
Logged-in users	✓	✓	✗	✗
Empirum Settings	✗	✗	✗	✗
E-mail Notifications	✓	✓	✗	✗
Restart the Console	✓	✗	✗	✗
FTP Upload Settings	✓	✓	✗	✗
Applications Manager	✓	✗	✗	✗
Performance Settings	✓	✗	✗	✗
Browser access port and bind settings	✓	✗	✗	✗
Deployment Manager Integration Settings	✓	✓	✗	✗
<b>User Authentication tab</b>				
User roles	✓	✓	✗	✗

Links	Emergency Admin	Primary Admin	Secondary Admin	Operator
Smartcard Settings	✓	✓	✗	✗
Local User Database	✓	✓	✗	✗
Emergency Administrator Password	✓	✗	✗	✗
<b>Data Sources Tab</b>				
Database	✓	✓	✗	✗
NAP database	✓	✓	✗	✗
Directory service	✓	✓	✗	✗
LDAP-to-database synchronization service	✗	✓	✗	✗
<b>Access Control tab</b>				
Access Control tab	✗	✓	✗	✗
<b>AR Settings</b>				
AR Server	✓	✓	✗	✗
AR Database	✓	✓	✗	✗
<b>Web Services tab</b>				
Web Services	✓	✓	✗	✗
Publish Web Services	✓	✓	✗	✗
<b>Tenant Management tab</b>				
Talent Management tab	✓	✗	✗	✗

## Configuring a tenant

The Super Administrator can access and view the Tenant Management tab in the Systems Settings page of CMS. In this tab, the Super Administrator can perform the following tasks:

- Add or remove a tenant
- Activate or deactivate a tenant
- Configure a tenant
- Configure the server properties of tenants

For each tenant, the Super Administrator can perform the following configurations:

- Configure the database
- Configure the Directory Service
- Configure the FTP server
- Configure the E-mail server
- Configure the AR server
- Configure the Deployment Manager server
- Configure Application permissions
- Configure properties

## Workflow of configuring a tenant

The workflow of configuring a tenant includes the following steps:

- 1 Create a tenant
- 2 Specify the access permissions for a Primary Administrator.
- 3 Specify the common properties of tenants.
- 4 Specify the properties of the tenant
- 5 Configure the database, directory service, FTP server, AR server, e-mail server, and Deployment Settings for the tenant.
- 6 Activate the tenant

The Super Administrator can add, configure, delete, deactivate a tenant from the Tenant Management tab in CMS. You can also edit the details of the tenant from the Tenant Management tab.

To delete a tenant, select the tenant which you want to delete and then click Remove button. Before you can delete a tenant, you must deactivate the tenant.

Note: Only the Super Administrators can view the Tenant Management tab in CMS.

## ► To add a new tenant

1. Log-in to CMS as Super Administrator
2. Navigate to System Settings - > Tenant Management tab
3. Click Add tenant button
4. Tenant Configuration page appears
5. Provide the following tenant details under General tab
  - tenant status (By default, tenant is de-activated)
  - tenant name
  - tenant description

-specify the required details to connect LDAP in auto-discovery mode.

Refer installation guide for creating new Active directory with auto-discovery mode.

AD Management Domain

DNS Server

Preferred DC's

AD Site

6. Add the following settings if required on each tab

- LDAP settings
- DB settings
- FTP settings
- E-Mail settings
- DM settings

7. Select required applications permissions can be accessed by tenant users
8. Set required tenant specific properties
9. Save the tenant

## Removing a tenant

### ► To remove a new tenant:

1. Log-in to CMS as Super Administrator
2. Navigate to System Settings - > Tenant Management tab
3. Ensure tenants are de-activated for removal.
4. Select tenant(s) and click Remove button
5. Confirm the removal

## Configuring the server tenant properties

Super Administrator can perform the following actions for configuration of server tenant properties:

- Add a property
- Remove a property
- Edit a property

### ► To configure server tenant properties

1. **Log-in** to CMS as Super Administrator
2. Navigate to **System Settings - > Tenant Management tab**
3. **Click** Property button  
The Server Properties dialogue appears.
4. **To add** a property, **Click Add**.
5. **To add** a property, **Click Add**.
6. **To delete** a property, select the required property and click **Remove**.
7. **To edit** a property, click on the required property and make the changes.
8. Click **Revert Changes** button to cancel the changes.
9. Once you have made the changes required, click **Save Changes**.

The changes you have made are saved.

## Editing the properties of a specific tenant

### ► To edit the properties of a tenant

- 1 Logon to CMS using your Super Administrator credentials.
- 2 Navigate to Applications > System Settings.  
The System Settings page appears.
- 3 Click Tenant Management tab in CMS.  
The Tenant Management tab appears.
- 4 Select the tenant for which you want to edit the properties.
- 5 Click Edit button.  
The Edit Tenant page appears.
- 6 Click Properties link on the left hand side menu.  
The Edit Properties page appears.
- 7 To add a property, click Add button.  
A new blank row appears where you can type the property and the value of property.
- 8 Click Save Changes to save the changes.
- 9 Click Revert Changes button to cancel the changes.
- 10 To remove a common property, select the property which you want to remove and click Remove button.

## Activating or Deactivating a tenant

Once you create a tenant, you have to activate it after making the required configuration settings.

### ► To activate or deactivate a tenant:

- 1 Logon to CMS using your Super Administrator credentials.
- 2 Navigate to Applications > System Settings.  
The System Settings page appears.

- 3 Click Tenant Management tab in CMS.  
The Tenant Management tab appears.
- 4 Select the tenant for which you want to activate or deactivate.
- 5 Click **Edit** button.  
The Edit Tenant page appears.
- 6 Click General link in the left side menu.
- 7 To activate the tenant, select **Activate**.
- 8 To deactivate the tenant, select **Deactivate**.
- 9 Click **Save**.

## Specifying access permissions to application

Super Administrator can choose applications permissions which can be accessed by tenant users.

### ► To specify access permissions for tenant users

- 1 Logon to CMS as Super Administrator.
- 2 Navigate to Applications > System Settings.  
The System Settings page appears.
- 3 Click Tenant Management tab in CMS.  
The Tenant Management tab appears.
- 4 Select the tenant for which you want to specify access permissions.
- 5 Click **Edit** button.  
The Edit Tenant page appears.
- 6 Click Application Permissions link in the left hand side menu.  
The Application Permissions tab appears.
- 7 Select the applications for which you want to give access permissions to the tenant user.
- 8 Click **Save** button.

## Configuring the database, LDAP, DM, AR, FTP and e-mail server settings for a tenant.

The Super Administrator can configure the database, LDAP, DM, AR, FTP and e-mail server settings for a tenant in the following two ways:

- From the Tenant Management page
- From individual pages of CMS

---

Note: If no tenant is configured and activated, then the Super Administrator cannot perform any tasks in the Schema Manager page.

---

## Configuring the database, LDAP, DM, AR, FTP and e-mail server settings for a tenant using the Tenant Management tab

- 1 Logon to CMS using your Super Administrator credentials.
- 2 Navigate to Applications > System Settings.  
The System Settings page appears.
- 3 Click Tenant Management tab in CMS.  
The Tenant Management tab appears.
- 4 Select the tenant for which you want to configure settings.
- 5 Click Edit button.  
The Edit Tenant page appears.
- 6 If you want to configure Directory Services, click the Directory Services link.  
The Directory Service page appears.
- 7 Proceed to configure the Directory Service.
- 8 Once you have completed specifying the Directory Service settings, click **Save**.  
For more information on configuring the Directory Service, refer CMS and Tuner Guide.
- 9 If you want to configure Database, click the Database link.  
The Database configuration page appears.
- 10 Proceed to configure the Database settings.  
For more information, refer CMS and Tuner Guide.

- 11 Once you have completed specifying the Database settings, click **Save**.
- 12 If you want to configure FTP settings, click the **FTP** link.  
The FTP configuration page appears.
- 13 Proceed to configure the FTP settings.  
For more information, refer CMS and Tuner Guide.
- 14 Once you have completed specifying the FTP settings, click **Save**.
- 15 If you want to configure E-mail click the **E-mail** link.  
The E-mail configuration page appears.
- 16 Proceed to configure the E-mail settings.  
For more information, refer CMS and Tuner Guide.
- 17 Once you have completed specifying the E-mail settings, click **Save**.
- 18 If you want to configure AR settings, click the **AR** link.  
The AR configuration page appears.
- 19 Proceed to configure the AR settings.  
For more information, refer CMS and Tuner Guide.
- 20 Once you have completed specifying the AR settings, click **Save**.
- 21 If you want to configure DM settings, click the **DM** link.  
The Deployment Manager configuration page appears.
- 22 Proceed to configure the DM settings.  
For more information, refer CMS and Tuner Guide.
- 23 Once you have completed specifying the DM settings, click **Save**.

Matrix showing the applicability of properties for Super Administrator and Primary Administrator in different environments:

Environment	Property	Super Administrator	Primary Administrator	Supported database
Multi tenant		Access only to CMS system setting page	Database installed by Tenant Primary Administrator	SQL Server or Oracle SQL Server - One DB for one Tenant
On Cloud	<p>This property is mandatory for cloud in CMS Tenant Management ? Properties (SQL &amp; Oracle db system password) &amp; tuner property respectively:</p> <ul style="list-style-type: none"> <li>■ marimba.tunercloud.tenant db.system.password=marimba123\$</li> <li>■ marimba.cms.mode=cloud</li> </ul>	Database installed by super administrator	Primary Administrator can perform only Schema maintenance activities.	SQL Server or Oracle SQL server - support for multiple custom invdb instances in one SQL server
Single tenant	<p>This property is not mandatory and applicable if Super Administrator user needs access to all the links.</p> <p>marimba.emergency.admin.role =PrimaryAdmin</p>	Can access CMS Web applications	Can access CMS Web applications	SQL Server or Oracle SQL Server - similar to prior to 8.5.00
Single tenant	All the links applicable only to default tenant primary admin user like pre-8.5.00	Access only to CMS system setting page.	Can access CMS Web applications.	SQL Server or Oracle SQL Server - similar to pre-8.5.00

Chapter

# 8

# User authentication and roles

This chapter describes the user authentication settings that you use to determine who can log in to the console and use the BMC Marimba Client Automation browser-based applications.

The following topics are provided:

- User authentication overview (page 127)
- What are user roles? (page 127)
- Selecting the user authentication type (page 128)
- Managing the local user database (page 130)
- Using smartcard authentication for CMS (page 130)
- Mapping roles to groups in a directory service (page 137)
- Setting an emergency administrator password (page 139)

## User authentication overview

The user authentication settings determine who can log in to the console and use the browser-based applications. You might want to configure user authentication settings for several reasons:

- To give each user a user name and password for logging in to use applications
- To assign roles to users and groups
- To give users and groups the appropriate permissions for performing tasks

You can use either a local user database or a directory service, such as Active Directory, ADAM / AD LDS, or Sun ONE Directory, for user authentication. For more information, see “Using a local user database or a directory service” on page 129.

To change the system settings, you must be logged in as a primary administrator. To check, place the mouse pointer over the Status icon.

## What are user roles?

User roles determine the capabilities of users when they log in to use the browser-based applications. When users log in to the system, their roles are assigned based on the user name and password they provide. The following roles are available:

- **Primary administrator.** Primary administrators have access to all product features available in the applications, including the system settings and configuration pages for applications. Primary administrators can set the user access to applications.

Depending on each application, primary administrators can perform certain tasks that are not available to other users. For example, the Configuration page in Report Center and the Plug-in Configuration page in Policy Manager are only available to primary administrators.

- **Administrator.** By default, Administrators can log in to the applications and have access to all product features except those reserved for primary administrators.

For example, the Configuration page in Report Center and the Plug-in Configuration page in Policy Manager are not available to standard administrators.

Standard administrators cannot modify most system settings, so they cannot perform tasks such as updating applications or configuring directory service settings. However, if a primary administrator has set up permissions for access control lists, standard administrators can assign permissions to other users on the Access Control tab (Applications > Console > System Settings).

You can also restrict which applications Administrators can access.

- **Operator.** Operators can log in to the applications and perform certain tasks, but they cannot make changes or save any changes in the applications. They generally have read-only access to the applications.

For example, in Report Center, operators can create new queries through the Query Builder but not by entering raw SQL. They cannot save queries.

Operators do not have access to Policy Manager. You can also restrict Operator access from any of the other applications.

See “Mapping roles to groups in a directory service” on page 136 for more information. For more information about what the roles mean for a specific application, see the online help for the application.

## Selecting the user authentication type

The user authentication type determines the source when authenticating users. You can choose from the following types:

- Directory service
- Local user database

You cannot use both types at the same time. You must use the directory service’s administration utility (not the System Settings pages) to perform operations on the directory service, for example, creating and removing users and groups, changing the group membership, and changing user passwords. Policy Manager requires that you use a directory service.

For more information, see “Using a local user database or a directory service” on page 129.

If you change the user authentication type, any users who are currently logged in are asked to log in again. You might want to warn users who are currently using the system before you change the user authentication type.

## ► To select the user authentication type

- 1 Choose Applications > Console > System Settings and then click the User Authentication tab.
- 2 Click the User Authentication Type link.
- 3 Select a type.
- 4 If you selected directory service, select one from the list.

If the directory service is not on the list, you must add the directory service first. See “Adding or editing a directory service” on page 144.

- 5 Click OK.

To use the new user authentication type, you are asked to log in again.

- 6 Depending on which type you choose, you must provide more information for user authentication.

If you selected a directory service, you must do the following:

- Provide information for connecting to the directory service. For information, see “Adding or editing a directory service” on page 144.
- Specify the groups in the directory service that you want to give access to applications and specify their roles. For information, see “Mapping roles to groups in a directory service” on page 136.

If you selected the local user database, you must add users and provide information for them. For information, see “Adding users to the local user database” on page 130.

**Adding users.** If you are using Active Directory, make sure new users belong to groups that were assigned user roles in the console system settings.

**Cache information.** If a new user logs in and sees You do not have privileges to access this server, CMS is using cached information to authenticate users and does not recognize the newly added users; this lasts until the cache expires and CMS contacts Active Directory. You can force CMS to refresh its cache immediately by restarting CMS. For more information, see “Restarting CMS and the console” on page 87. Using the cache happens because CMS has caching turned on by default when you configure a directory service to work with CMS. For more information, see the caching options described in “Advanced settings for the directory service” on page 151.

# Managing the local user database

This section describes the local user database and explains how you can add, edit, or remove users from it. It contains the following topics:

- “Using a local user database or a directory service” on page 129
- “Adding users to the local user database” on page 130
- “Changing passwords for users in the local user database” on page 131
- “Searching for users in the local user database” on page 130
- “Changing roles for users in the local user database” on page 132
- “Removing users from the local user database” on page 132

## Using a local user database or a directory service

If you do not want to use a directory service as the source for user accounts, you can store user accounts in a *local user database*. The local user database is stored on the machine where the applications are installed. In contrast, a directory service (such as Active Directory, ADAM / AD LDS, or Sun ONE Directory) is stored on a server, usually one different than the one on which the applications are installed. You can use either the local user database or a directory service, but not both at the same time.

When you use the local user database, you can:

- Add users to the database.
- Remove users from the database.
- Change user passwords.
- Assign and change roles for users.
- View whether users are logged in, when they logged in, and the IP address from which users are accessing the application.

When you use a directory service, you can:

- Provide access to users and groups that are already defined in a directory service.

- Assign and change the roles for users and groups that are already defined in a directory service.
- Use Policy Manager, which stores policies and other data in the directory service.

## Adding users to the local user database

You can use the local user database to store information for users so that they can access the applications. You can view the list of users who are currently allowed to access and use the applications.

### ► To add a user to the local user database

- 1 Choose Applications > Console > System Settings and then click the User Authentication tab.
- 2 Click the Local User Database link.
- 3 Click Add a User.
- 4 Enter a user name.

You cannot enter `admin` because it is reserved for use with the emergency administrator password. For more information, see “Setting an emergency administrator password” on page 138.

- 5 Select a user role.

For more information, see “What are user roles?” on page 126.

- 6 Enter a password. Confirm the password by entering it again.
- 7 Click Save to List to add the user to the database.  
The user you added appears in the list of users.
- 8 Click OK.

## Searching for users in the local user database

You can look up a specific user by entering the user name.

### ► To look up a specific user

- 1 Choose Applications > Console > System Settings and then click the User Authentication tab.

2 Click the Local User Database link.

The local user database lists the users. The Role column shows the role assigned to each user. The Logged in Since column shows:

- Whether users are logged in.
- The date and time when users logged in.
- The IP address from which users are accessing the application.

If there are more than 25 users, you can page through the list of users.

3 In the Look up user field, enter a user name and click Go.

The user name is case-sensitive and must match exactly.

The information for the user appears. To make changes, see “Changing passwords for users in the local user database” on page 131 and “Changing roles for users in the local user database” on page 132.

## Changing passwords for users in the local user database

As a primary administrator, you can change the password for any user in the local user database.

### ► To change a user password

1 Choose Applications > Console > System Settings and then click the User Authentication tab.

2 Click the Local User Database link.

If there are more than 25 users, you can page through the list of users.

3 Select a user and click Edit.

4 In the Password field, enter a new password. Confirm the password by entering it again.

5 Click Save to List.

6 Click OK.

The next time the user logs in, the user must use the new password.

## Changing roles for users in the local user database

You can change the roles specified for users in the local user database. For information about user roles, see “What are user roles?” on page 126.

### ► To change a user role

- 1 Choose Applications > Console > System Settings and then click the User Authentication tab.
- 2 Click the Local User Database link.

The Role column lets you see the role assigned to each user. If there are more than 25 users, you can page through the list of users.

- 3 Select a user and click Edit.
- 4 In the User role field, select a role.
- 5 Click Save to List.
- 6 Click OK.

The next time the user logs in, the user has the role that you specified.

## Removing users from the local user database

You can remove users from the local user database. After removal, users cannot log in and access the applications.

### ► To remove a user from the local user database

- 1 Choose Applications > Console > System Settings and then click the User Authentication tab.
- 2 Click the Local User Database link.

If there are more than 25 users, you can page through the list of users.

- 3 Select a user and click Remove.

The user you removed no longer appears in the list of users.

- 4 Click OK.

## Finding logged in users in the local user database

The Local User Database page lets you view whether users are logged in, when they logged in, and the IP address from which users are accessing the application.

### ► To find out which users from the local user database are logged in

- 1 Choose Applications > Console > System Settings and then click the User Authentication tab.
- 2 Click the Local User Database link.

The Logged in Since column lets you view:

- Whether users are logged in.
- The date and time when users logged in.
- The IP address from which users are accessing the application.

If there are more than 25 users, you can page through the list of users.

- 3 Click OK.

## Using smartcard authentication for CMS

You can enable users to log in to the console using a smartcard so that they are not required to enter a username and password. Authentication is achieved using the client certificate stored in the smartcard.

SSL must be enabled in CMS before you enable smartcard authentication.

Smartcard authentication requires the smartcard issuer to be registered before using a smartcard. The issuer can be registered by the root certificate received from the issuer, and it can be imported into the tuner Certificate Database using Certificate Manager. The imported issuers can be registered using the Issuer registration page from Smartcard Settings > Smart Card Issuer List > Add an Issuer link.

---

Note: The issue certificate should be the immediate root of the smartcard certificate. The smartcard certificate issuer comparison checks only the immediate parent not the chain of parents.

---

## Requirements

Before using this feature, you must register the smartcard in the CMS console, configure the directory service (LDAP) and enable Secure Sockets Layer (SSL) in the console. You can use smartcard authentication with the following directory services:

- Sun One
- ADAM
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory (AD)

Users must use the FQDN (Fully Qualified Domain Name) to access CMS. Otherwise, SSL handshaking fails and the user is directed to the login page.

## To enable smartcard authentication

- 1 Import smartcard issuer (root) certificate.
  - a Obtain the smartcard issuer certificate from the smartcard vendor and use Certificate Manager to import it to the CMS Tuner.
  - b In the CMS console, go to the System Settings=>User Authentication=> Smartcard Setting=>Smartcard Issuer List page and select the issuer certificate that you want to register as a trusted issuer.
- Only the smartcards issued by the trusted issuer are allowed to log in to the CMS console. The smartcard issuer must be the immediate root of the smartcard certificate.
- 2 Register the smartcard certificate.
  - a Using a browser, export the public certificate from the smartcard to a file. For example, using Internet Explorer, select the Tools=>Internet Setting=> Contents =>Certificates menu, select the certificate to export, and save it as a file.
  - b In the CMS Console, go to the System Settings=>User Authentication=> Smartcard Setting=>Smartcard User Registration page and select the smartcard certificate file.
  - c Map the smartcard certificate to a valid user in LDAP.

---

Note: Users can use a smartcard that is not registered but is issued by a valid issuer. On the first login, the smartcard user is prompted for a user name and password. This user is then mapped to the smartcard certificate. For subsequent logins, the user name and password are not required.

---

- 3 Enable smartcard authentication.
  - a From the CMS console, make sure that SSL is enabled on the System Settings=>General=>SSL Settings page.
  - b From the CMS console, go to System Settings=>Authentication=>Smartcard Setting>Smartcard Authentication and select the “Enable Smartcard Authentication” option.
  - c If you need both the normal login and the smartcard login, select the “Allow simple authentication” option.
  - d To provide smartcard authentication for tuner and transmitter administration, select “Allow remote admin access for smartcard users.”

---

Note: If you provide smartcard authentication for the tuner and transmitter administration, configure the same LDAP for authentication that is configured for CMS authentication.

---

When you enable smartcard authentication, the following channel property is set in the `msf.txt` file: `smartcard.enabled=true`

## To use smartcard authentication

- 1 Insert the smartcard.
- 2 Access the CMS login page.

---

Note: FireFox users must change their Firefox browser settings when using a smartcard to access the CMS. In the Firefox Advanced Options dialog, click the Encryption tab and enable “Ask me every time.”

---

- 3 When prompted, select the appropriate client certificate for login.

- 4 When prompted, enter the smartcard PIN.

If the certificate is valid, you are directed to the CMS getting started page. Otherwise, you are directed to the standard CMS login page if the option “Allow simple authentication” is enabled.

## Mapping roles to groups in a directory service

If you are using a directory service, users must belong to a group in the directory service and have a password to log in and use the applications.

- If you are using Active Directory, users can be in any group type. If the users do not belong to a group, you might want to create a global security group and assign the users as members.
- If you are using Active Directory Application Mode (ADAM) or AD LDS, users must belong to a global security group. Set the group type attribute to the global security group (-2147483646).

You must use the directory service’s administration utility (not the System Settings pages) to perform operations on the directory service. For example, creating and removing users and groups, changing the group membership, and changing user passwords.

For information on user roles, see “What are user roles?” on page 126.

### ► To map the Primary Administrator role to groups in a directory service

- 1 Choose Applications > Console > System Settings and then click the User Authentication tab.
- 2 Click the User Roles link.
- 3 In the Primary Administrator Groups field, enter the names of the groups to which you want to assign the primary administrator role as described in “Entering group names when mapping roles to groups” on page 137.
- 4 Click Save.

---

Note: You must select All Applications from the Applications drop-down before you can add or change Primary Administrator groups. Otherwise, the input field for Primary Administrator groups is inactive.

---

## ► To map the Administrator and Operator roles to groups in a directory service

You can restrict users in the administrator or operator groups to specific applications or give them access to all applications.

- 1 Click the Application drop-down and select an application to which access will be allowed for the groups you specify.  
Select All Applications if you do not want to restrict access to any applications for the groups you are entering.
- 2 In the Administrator groups and Operator groups fields, enter the names of the groups to which you want to assign the roles for the selected application described in “Entering group names when mapping roles to groups.”

---

Note: A group can have the administrator role for some applications and the operator role for other applications. Users in primary administrator groups have access to all applications.

---

- 3 Click Save.

You can enable access to other applications for the same groups by selecting another application and entering the names of the groups again for the newly selected application.

### Entering group names when mapping roles to groups

For each role, you can enter one or more group names. To specify multiple groups, enter a comma-separated list of groups for each role.

Use the following syntax for specifying group names:

- common names (CNs)  
For example, group1 or group1,group2,group3
- distinguished names (DNs)  
For example, “cn=group1,ou=groups,dc=company,dc=com” or  
“cn=group1,ou=groups,dc=company,dc=com”,  
“cn=group2,ou=groups,dc=company,dc=com”,  
“cn=group3,ou=groups,dc=company,dc=com”

Both commas and spaces are valid separators. If a group name contains either a comma or a space, the name must be enclosed in double quotation marks. If a group name contains double quotation marks, the quotation marks must be escaped using a backslash.

If there are groups with the same name in different domains within your enterprise, use fully qualified distinguished names. Otherwise, the CMS cannot authenticate users in those groups.

## Setting an emergency administrator password

The emergency administrator password lets you and other users log in and use the applications even if the directory service or the local user database used for authenticating users is not available.

You must log in with the user name `admin` when using the emergency password, but you can set the emergency administrator password.

**Command-line.** For information, see `-setAdminPassword` in the command-line section of the *BMC Marimba Client Automation Reference Guide*.

### ► To set an emergency administrator password

- 1 Choose Applications > Console > System Settings and then click the User Authentication tab.
- 2 Click the Emergency Administrator Password link.
- 3 Enter an emergency administrator password. Confirm the password by entering it again.

The maximum length for the emergency password is 40 characters.

- 4 Click OK.

Before you can use the BMC Marimba Client Automation browser-based applications, you must specify the sources—directory services and databases—where the applications get and store data. This chapter explains how to add directory services and databases to CMS so they are available for applications to use, and discusses synchronizing the data between the sources.

The following topics are provided:

- About the Java Kerberos system (page 141)
- Managing directory services (page 145)
- Managing databases (page 157)
- Synchronizing data from the directory service with the database (page 160)
- Configuring the CMS for integration with a NAP database (page 162)

To change the system settings, you must be logged in as a primary administrator. To check, place the mouse pointer over the Status icon.

# About the Java Kerberos system

You can enable Kerberos authentication to log on to SMCA and for communication within SMCA products.

A Kerberos server is a trusted third party that brokers communication requests of its clients. This Kerberos communication protocol uses secret keys and the Kerberos client uses the secret key which is known only to itself and the Kerberos server. The clients use the secret key to authenticate themselves to the Kerberos server and to set up secure connections with other clients. The Java Kerberos system secures all communications between the SMCA products and the LDAP Server. All SMCA applications are Kerberos clients. The CMS Console user login system is also a Kerberos client which authenticates the logged on users, and authenticates all LDAP operations using Kerberos technology.

The Java Kerberos system consists of the following components:

- Key Distribution Center (KDC)

KDC maintains a database of Kerberos Clients and Application Servers within its realm. It consists of an Authentication Server (AS) and a Ticket Granting Server (TGS), which run on the same machine. However, the Kerberos Clients and the Application Servers can be distributed across the network. It also provides Kerberos Ticket Granting Tickets (TGT) to its clients.

- Kerberos Client

- Application Server

---

Note: Application Server denotes the LDAP Server like Active Directory.

---

The workflow of the Java Kerberos system is as follows:

- 1 The Kerberos client logs on and receives TGT from the KDC.
- 2 The Kerberos client presents the TGT to KDC and obtains the session ticket to access Directory Server.
- 3 The Kerberos client connects to the required application and presents the session ticket.

## Prerequisite

You must configure the Service Principal Name (SPN) for LDAP connection. You must configure the krb5 configuration file for the Kerberos environment and place it in the c:\windows directory, which the Kerberos authentication module accesses.

### Configuring the SPN

To register the SPN manually, you must use the Setspn.exe tool provided with the Microsoft Windows Server 2003 Support Tools.

Setspn.exe is a command line tool that allows you to read, modify, and delete the SPN directory property. This tool enables you to view the current SPNs, reset the account's default SPNs, and add or delete supplemental SPNs.

For example, to manually register an SPN for a TCP/IP connection, you can use the following syntax:

```
setspn.exe -A LDAP/myhost.mydomain.com account-name
```

---

Note: By default, a SPN name is created with the Active Directory machine name. If SPN is not available for the domain, you can configure the SPN using the setspn command with the -D switch.

---

### Configuring the krb5 file

You can use the krb5.conf or krb5.ini file to locate the default realm and KDC server for a Kerberos environment. You must create and place the krb5.ini or krb5.conf file in a specified directory. This file is loaded during runtime and is cached until the tuner restarts.

For a Windows operating systems, you must place the krb5.ini file in the c:\windows directory.

An example of a krb5.conf file with a single domain controller:

```
[libdefaults]
default_realm = MYDOMAIN.COM
[domain_realm]
.mydomain.com = MYDOMAIN.COM
[realms]
MYDOMAIN.COM = {
kdc = MYPDC.MYDOMAIN.COM.COM
}
```

An example of a krb5.conf file with multiple Domain controller:

```
[libdefaults]
default_realm = MYDOMAIN.COM
[domain_realm]
.mydomain.com = MYDOMAIN.COM
[realms]
MYDOMAIN.COM = {
kdc = MYPDC.MYDOMAIN.COM.COM
kdc = MYBDC1.MYDOMAIN.COM.COM
admin_server = MYPDC.MYDOMAIN.COM.COM
default_domain = MYDOMAIN.COM
}
```

---

Note: After you make any changes to the krb5.ini or krb.conf file, restart the tuner.

---

After you have configured Kerberos authentication, if you see the Final handshake failed [Caused by GSSEException: Token had invalid integrity check (Mechanism level: Corrupt checksum in Wrap token)] exception message in the CMS history log, then add the following properties to the krb5.ini file:

```
default_tkt_enctypes = arcfour-hmac-md5
default_tgs_enctypes = arcfour-hmac-md5
permitted_enctypes = arcfour-hmac-md5
```

---

Note: After you add the preceding properties to the krb5.ini or krb.conf file, restart the CMS.

---

---

Note: The Kerberos authentication intern uses Java JCE (Java Cryptography Extension) for encrypted message exchange. Due to restrictions on import control in some countries, the version of the JCE policy files that are bundled with Infrastructure Service channel allow "strong" but limited cryptography. To enable unlimited strength, users need to accept the license agreement available on the profile page under Security\Kerberos tab. The same option is available in tuner administration as well. When users accept the licence, the tuner property "marimba.tuner.jce.unlimitedstrength=true" is added to profile. This property enables unlimited strength cryptography during the Kerberos authentication. This option is applicable to all the profile types.

---

---

Note: For Kerberos authentication, the CMS time and Transmitter time needs to be synchronized with the Kerberos server clock. The default configuration allows only 5 minutes of difference between the CMS time and Transmitter time. When Kerberos token expires, CMS automatically renews the token without user re-login. The Kerberos token expiry is also applicable to the service account that the policy plugin and scheduled tasks use.

---

---

Note: The authenticated Kerberos token is stored in the application layer cache until the token expires. The cache storage avoids frequent communication with KDC for authentication.

---

# Managing directory services

This section describes how you can add, edit, or remove directory services from the list available for use by the applications. CMS and browser-based applications can use a directory service to authenticate users when they log in (see “Selecting the user authentication type” on page 127). Applications such as Policy Manager can use a directory service to store information.

This section contains the following topics:

- “Adding or editing a directory service” on page 144
- “Removing a directory service” on page 148
- “Using automatic discovery for Active Directory” on page 150
- “Advanced settings for the directory service” on page 151
- “Using the base DN and bind DN” on page 152
- “Permissions required for the bind DN” on page 154
- “Setting up multiple directory services for failover” on page 155

## Adding or editing a directory service

You can add directory services and make them available for use by applications. You can edit information for a directory service that is already in the list.

When you change the directory service settings, the following happens:

- Users who are currently logged in are asked to log in again.  
You might want to warn users who are currently using the console or any applications before you change the directory service settings.
- The CMS channel must be restarted for the new properties to take effect. New properties includes everything except the description.

**Best practice.** If you do not want to restart CMS, add a new directory service with the properties and set that as active. This has an immediate effect and you do not have to restart CMS.

The base distinguished name (DN) and bind DN are only used when authenticating users who log in to use the console and applications that run on it, such as Patch Manager or Report Center. After users log in, authentication occurs in two steps: user authentication and role identification. Both steps require that the directory service be searched, and this is when the base DN and bind DN are used. For more information, see “Using the base DN and bind DN” on page 152.

---

**Tip:** If you want to use a new directory service for user authentication, add a new directory service instead of editing an existing one, especially if the new directory service is a different type (for example, Sun ONE Directory instead of Active Directory). You can then specify that the directory service be used for user authentication and map user groups to roles.

---

## ► To add or edit directory services

- 1 Choose Applications > Console > System Settings and then click the Data Source tab.
- 2 Click the Directory Service link.
- 3 If you are adding a directory service, click Add a Directory Service and then fill in the Directory service name and Description fields.

The name and description are added to the list of directory services.

For backward-compatibility reasons, you cannot use local or LDAP for the name of the directory service.

- 4 If you are editing a directory service, select the directory service from the list and then click Edit.
- 5 In the Directory service type field, select a type.
- 6 If you select Active Directory and want to use automatic discovery to find the Active Directory domain, select the Auto-discover check box.

CMS automatically discovers the Active Directory domain, site, global catalog, and domain controller. CMS uses the SRV records in the DNS server to discover the domain and then connects to the domain controller in the domain with the lowest load. For more information, see “Using automatic discovery for Active Directory” on page 150.

You do not have to enter a host name, port number, and base DN; go to step 10.

- 7 Enter the host name and port number (for example, Directory\_Service:389 or 176.16.2.162:389).
- 8 Enter the base DN for the directory service connection, usually equivalent to the directory suffix. For example:

For Active Directory, Active Directory Application Mode (ADAM) / Active Directory Lightweight Directory Services (AD LDS), or Sun ONE Directory, use the following format:

dc=company,dc=com

- 9 If you select Active Directory but not automatic discovery, and want CMS to verify the connection before saving the directory service settings, select the Validate connection check box.

You might choose to clear this check box if the directory service does not have to be accessible from the computer on which CMS is installed. For example, the directory service is being used by tuners and transmitters in another domain.

- 10 If the selected directory service is set up to use Secure Sockets Layer (SSL), select the Use SSL check box for secure transactions. In the Authentication type list, select Simple Bind. If you want to use Kerberos protocol for authentication, select Kerberos Protocol.

**Note:**

- When you select Kerberos authentication, you must provide the bind user name in the username@REALM format. If you have pre-defined the default realm in the krb5.ini file, then you need not specify the realm.
- You must configure the Service Principle Name (SPN) for LDAP connection. You must configure the krb5 configuration file for the Kerberos environment and place it in the c:\winnt or c:\windows directory, which the Kerberos authentication module accesses.
- By default, a SPN name is created with the Active Directory machine name.

For more information, see “Properties for supplying SSL client-certificate information” on page 81.

**Note:** After you set this, if you log in to the console and clear the check box, logging out and back in to the console does not turn off SSL. You must restart the console.

- 1 Enter the bind DN and password for a user with read and write permissions in the selected directory service.

For Active Directory or ADAM / AD LDS, use either of the following formats:

- The full distinguished name, for example,  
cn=Administrator,cn=Users,dc=company,dc=com
- The user principal name (UPN), for example,  
Administrator@company.com

If you want to use the built-in administrator account created by Active Directory using the UPN format (for example, administrator@company.com), you must set up the UPN attribute for the administrator account using the Microsoft Management Console (MMC). By default, no UPN attribute is assigned to the administrator account. If the UPN attribute cannot be found for an account, the user cannot log in; this scenario is true even when an account with the same user name has been set up with a UPN attribute in one domain but not another (for example, administrator@root1.com has a UPN attribute, while administrator@east.root1.com does not).

For Sun ONE Directory, use either of the following formats:

- The full distinguished name, for example,  
uid=Administrator,ou=People,dc=company,dc=com
  - The common name for the directory administrator, for example,  
cn=Directory Manager
- 2 If you want to use the directory service to authenticate users logging in to the console, select the Use this directory service to authenticate users check box.
  - 3 If you want to specify advanced settings for the directory service, do the following steps:
    - a From the Show advanced settings list, choose Yes.
    - b If you want to automatically enter the default information for the directory service type, click Set Directory Service Defaults. You can then change only the specific settings that you need for the directory service.
    - c Enter the information for the directory service you are using.  
The directory service administrator can provide you with the values. For more information, see “Advanced settings for the directory service” on page 151.
  - 4 Click OK.

You return to the Directory Services page, and the directory service you added or edited appears in the list.

- 5 Click OK.
- 6 Choose one of the following options:
  - Change the user roles before logging out.
  - Log out without changing user roles.

Either option requires you to log in again to use the new directory service settings.

When you use a directory service, you must select the directory service as the source for user authentication and to specify which groups in the directory service you want to give access to the applications by mapping roles. For information, see “Selecting the user authentication type” on page 127 and “Mapping roles to groups in a directory service” on page 136.

**Note:** Before this directory service can be used by an application, you might have to select it in the application. For example, in Policy Manager, you must use the Configuration > Plug-in Configuration page to select the directory service you just added.

## LDAP Properties

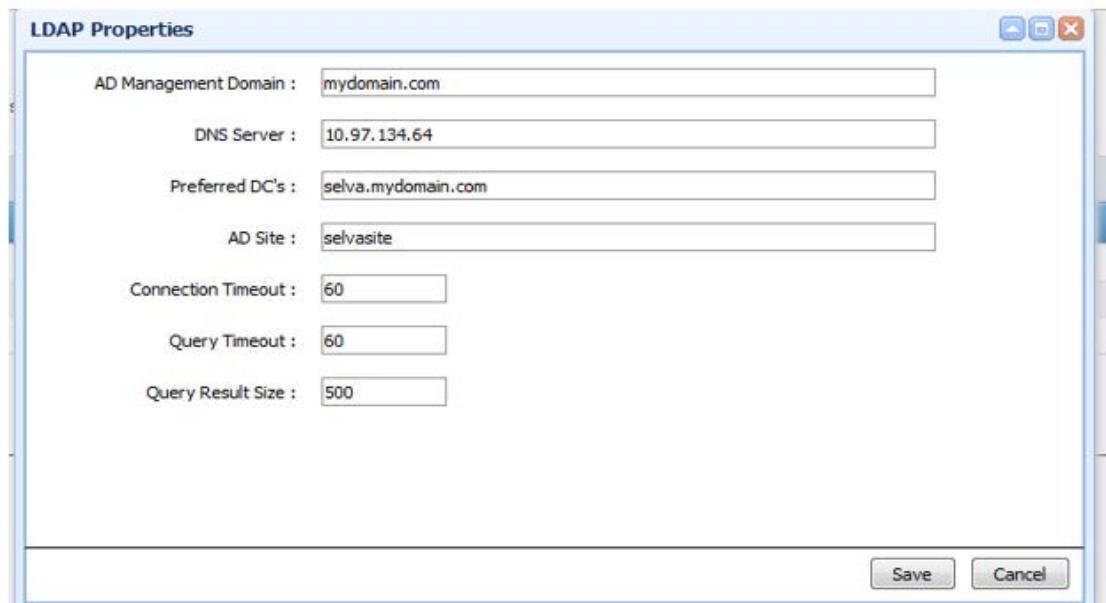
Below is the list of LDAP properties:

- "marimba.ldap.adsite"
- "marimba.ldap.preferreddcsc"
- "marimba.ldap.srvdnsserver"
- "marimba.ldap.querytimeout"
- "marimba.ldap.queryresultsiz"
- "marimba.ldap.admanagementdomain"
- "marimba.ldap.connectiontimeout"

**Permission :** Not applicable for Cloud.

**Location:** System Settings -> Data Source -> Click “Properties” button in directory service list page.

**Screen Shot:**



## Removing a directory service

When you remove a directory service from the list, the directory service is no longer available for use by BMC Marimba Client Automation applications.

If you are using the directory service for user authentication, you must first specify a different source for user authentication (User Authentication tab, then User Authentication Type link). You are prompted to log out after you change the user authentication source; you can then temporarily log in using the emergency administrator name (admin) and password to remove the directory service. For more information, see “Selecting the user authentication type” on page 127.

### ► To remove a directory service

- 1 Choose Applications > Console > System Settings and then click the Data Source tab.
- 2 Click the Directory Service link.
- 3 Select the directory service and click Remove.  
The directory service no longer appears in the list.
- 4 Click OK.

## Using automatic discovery for Active Directory

If you select Active Directory for the directory type, you have the option of using automatic discovery to find the Active Directory domain, site, global catalog, and domain controller using DNS information.

If you use Active Directory with multiple domains, you must use automatic discovery. With a single domain, you can choose whether to use automatic discovery.

If you use automatic discovery and Policy Manager, policies have to replicate to the global catalogs of the plug-in. Depending on how Active Directory is configured in your enterprise, it might take time before policies are available to endpoints in remote sites.

### When to use automatic discovery

Using automatic discovery has the following advantages:

- The console, Policy Manager, and the Policy Service plug-in connect to the domain controller and global catalog from the same site as the machine where they are running.
- You automatically get load balancing for the domain controllers in a particular site.
- Users from other domains can log in to the console and use applications (if they are given the appropriate role and access).
- When using Policy Manager, users can assign policies to targets across domains.
- When using Policy Manager, users do not have to create an `ldapservers.txt` file to map the Policy Service plug-in to the closest Active Directory server.

### When not to use automatic discovery

Do not use automatic discovery when connecting to Active Directory in the following cases:

**Administration tools.** Do not use automatic discovery if you are using Active Directory as the source for users who you want to give remote administration access for the administration tools (such as Tuner Administration and Transmitter Administration). The administration tools require that you explicitly enter the host name, port number, and base DN for Active Directory.

**Policy Manager and user authentication.** When using Active Directory with Policy Manager and for user authentication when logging in to the console, *not* using automatic discovery has the following advantages:

- When DNS is not set up with Active Directory information (for example, in a test environment or during a demonstration), you can configure the console and Policy Manager to connect directly to an Active Directory server.
- If you do not want the plug-in to go to the global catalog closest to it and accept the network traffic that might be generated, you can configure the plug-in so that it goes directly to the same Active Directory server used by Policy Manager. This allows policy changes to happen immediately without having to wait for the global catalog to replicate.

## Advanced settings for the directory service

Advanced settings depend on the directory service you are using; usually, you can use the defaults. However, if you have to modify particular advanced directory service settings for your environment, you can change the following settings.

### Containment Model

- **Group class name** – Enter object class names for groups. This can be a comma-separated list.

For example, groupOfNames, groupOfUniqueNames for Oracle Directory Server or group for Active Directory.

- **Group name attribute** – Enter an attribute used to name groups.

For example, cn.

- **Group member attribute** – Enter an attribute name used to define group members. This can be a comma-separated list.

For example, member , uniquemember for Oracle Directory Server or member for Active Directory.

## Users

- **Object class for a person** – Enter an object class used to represent a person. For example, `inetorgperson` for Oracle Directory Server or `user` for Active Directory.
- **Attribute name for a person** – Enter an attribute name used to identify users.  
For example, `uid` for Oracle Directory Server or `sAMAccountName` for Active Directory.

## Miscellaneous

- **Connection pool size** – Enter the number of open directory service connections shared by all authentication requests. The default is 16.
- **Maximum number of objects returned by a query** – Enter the maximum number of entries to return when opening folders or searching. The default is 500.
- **Use caching** – Select this check box and enter the number of minutes in the Cache expiration time in minutes field if you want directory service information to be cached for a specified amount of time only. By default, the check box is selected and cache expiration time is set to 10 minutes.  
If you clear the check box, CMS does not cache directory service information and connects to the directory service when information is required.

## Using the base DN and bind DN

The base DN and bind DN are only used when CMS authenticates users who log in to use the browser-based applications. Authentication occurs in two steps, user identification and role identification. Both steps require that the directory service is searched; this is when the base DN and bind DN are used.

**User Identification.** User identification requires searching the directory for the `<person object>` that represents the user identified by the user name provided. When using the user name (`sAMAccountName` for Active Directory or `uid` for Oracle Directory Server), Policy Manager must search the directory for the full distinguished name of the object that represents the user.

Searching the directory requires the following items:

- The base DN, which is the starting point for the search in the directory tree.
- The DN of a user object to connect to the directory service for a search (the same as the bind DN).

The *<person object>* identified by the bind DN must have read permission for the container (under the base DN) where the *<person object>* of users trying to log in are stored in the directory. For Active Directory, this is typically the `cn=users` container; for Oracle Directory Server, this is typically the `ou=people` container. The *<person object>* that the bind DN refers to must have read permissions on the container where the user group objects that define the user roles reside. This can be any container, but it is typically the same container where users are stored.

During the search, Policy looks for the object class *<person object>* that has the attribute name for *<object name>* set to the user name provided when the user logged in. The exact *<person object>* class and *<object name>* attribute within that class are different in Active Directory and in Oracle Directory Server. They can be found in the advanced settings section on the Add Directory Service page or the Edit Directory Service page (System Settings > Data Source > Directory Service link).

**Role Identification.** After the full DN of the user is found, Policy gets the groups to which the user belongs. One of the groups must be mapped to a user role in the User Roles page (System Settings > User Authentication > User Roles link).

Groups are identified by their common names on the User Roles page, so Policy searches for the full DN of the group in the directory. As described in the previous step, searching the directory requires the base DN and the bind DN. The *<person object>* identified by the bind DN must have read permission for the container where the user groups are found. The object class that represents the user group are different in Active Directory and in Oracle Directory Server. They can be found in the directory service page (System Settings > Data Source > Directory Service), under advanced settings.

## Permissions required for the bind DN

The administrator name and password used for the bind DN must have read permissions for users and groups for all membership information that must be retrieved (for example, to authenticate users logging in to the console).

If you are using Active Directory, it is recommended that you have the administrator name and password used for the bind DN be members of a universal group with the appropriate permissions for all the mentioned objects. This is because the member-of attribute of domain local groups and global groups is not replicated to the global catalog outside the groups' domain.

In addition, the administrator name and password used for the bind DN must

- Belong to at least one group besides the Domain User group.
- Have the appropriate permissions to read the member-of attribute of groups from the global catalog to which the Policy Service plug-in connects.
- To use the access control lists (ACLs) feature of Policy Manager, have read and write permissions to the container where ACLs are stored (for example, ou=ACL,dc=company,dc=com).

## Changing the bind DN password

When the bind DN user password is changed, you must also change the bind password in the CMS. You must also apply the password on endpoints if authentication permission is set for tuners using Tuner Administration.

### ► To change the bind DN password in the CMS

- 1 In the CMS console, access System Settings, click the Data Source tab, and click the Directory Service link.
- 2 Select the directory service name and click Edit.
- 3 Change the password under Bind DN and click OK.

### ► To change the bind DN password for endpoints through a profile

- 1 Convert the new password to base64 encoding using any third-party tool.

- 2 In a profile, set the marimba.tuner.admin.ldap.password property to the converted, base64 password.
- 3 Update the profile on the endpoints.

As an alternative to changing the bind DN password through a profile, there are two other ways to change the bind DN password on endpoints:

- You can push the updated password out to endpoints from Transmitter Administration by changing the Authentication method to All users. After the change is saved, you can change the Authentication method back to the previous setting.
- You can also create a new policy in Policy Manager that contains the marimba.tuner.admin.ldap.password set to the converted, base64 password. Deploy the policy to all endpoints.

As a best practice, you should set the emergency password for Transmitter and Tuner Administration while setting permissions.

## Setting up multiple directory services for failover

If you want to set up multiple mirrored directory services for failover, you can enter a comma-separated list of host names and port numbers in the Host name and port number field for the directory service. CMS goes through the directory services in the order that you entered until it finds one that it can connect to successfully. The directory services that you specify must have the same settings (base DN, bind DN, password, and advanced settings). Make sure that the directory services have the same entries (containers, users, groups, and so on).

You cannot specify multiple host names if you use automatic discovery with Active Directory.

## Managing databases

This section describes how you can add, edit, or remove databases from the list available for use by the applications. The BMC Marimba Client Automation browser-based applications, such as Report Center, use the databases to store information. This section contains the following topics:

- “Adding or editing a database” on page 156
- “Removing a database” on page 157

## Adding or editing a database

You can add databases and make them available for use by applications. You can edit information for a database that is already in the list.

This procedure assumes that you have downloaded the database scripts that you must use with Report Center. For more information, see the installation chapter in the *BMC Marimba Client Automation Report Center User Guide*, available on the Marimba Channel Store.

**Database connections.** More database connections (threads) generally mean better performance; however, the database license might limit the number of connections. Because the connections persist, having constant connections can use up memory over time.

**Default settings.** Most of the time, you do not have to change the default settings. Schema Manager automatically creates reporting and inventory connections for the database. You usually use the same database for the reporting and inventory connections; however, you might want to use separate databases for performance and security. For example, you might want more granularity in setting minimum and maximum connections for the database.

### ► To add or edit a database

- 1 Choose Applications > Console > System Settings and then click the Data Source tab.
- 2 Click the Database link.
- 3 If you are adding a database, click Add a Database and then enter a name and description for the database.
- 4 If you are editing a database already in the list, select the database and click Edit.
- 5 In the Database type field, select a type.
- 6 Enter the host name and port number.

Commonly used port numbers are 1521 (Oracle) and 1433 (SQL Server).

- 7 In the SID field, enter one of the following:
  - For Oracle, the database system ID that was selected during the Oracle database installation.

- For SQL Server, the database name, which is usually `invdb`, unless you edited all the necessary database setup scripts to change this value change this value during the install, reinstall, or upgrade process.

The database administrator can provide you with the values.

- 8 Enter the minimum and maximum number of connections for the database.

The default settings (and recommended numbers) are a minimum of 5 connections and a maximum of 30 connections.

- 9 Enter the administrator-level user name and password.

The default is `user_view` for both, unless you edited the `install_inventory.sql` script to change the values.

- 10 Select the database action:

- **Do not designate default settings.**

- **Set as the default reporting connection.** The reporting connection is used for user actions. The default user name and password are both `user_view`.

For example, actions performed in Report Center such as executing, creating, and editing queries; actions performed in Patch Manager such as creating patch groups based on Report Center queries; and reporting policy compliance through Report Center.

- **Set as the default inventory connection.** The inventory connection is used by the internal actions of the applications. The default user name and password are both `inventory`.

For example, the actions can include inventory plug-in actions, LDAP-to-database synchronization, and access control configuration.

- 11 Click Check Connection to validate the database information that you provided.

- 12 Click OK.

You return to the Database page, and the database you added or edited appears in the list.

- 13 Click OK.

## Removing a database

When you remove a database from the list, the database is no longer available for use by BMC Marimba Client Automation applications.

## ► To remove a database

- 1 Choose Applications > Console > System Settings and then click the Data Source tab.
- 2 Click the Database link.
- 3 Select the database and click Remove.  
The database you removed no longer appears in the list.
- 4 Click OK.

## Synchronizing data from the directory service with the database

Synchronizing the directory service with the database works with the following data:

- User targets, machine targets, and their group membership information
- Access control list information
- Policy compliance information

To perform LDAP-to-database synchronization, you must be using LDAP or a directory service for user authentication. For more information, see “Selecting the user authentication type” on page 127. You must enable LDAP-to-database synchronization when you are using policy compliance or turning on access control for applications. For more information, see “Setting up access control lists” on page 163.

When scheduling LDAP-to-database synchronization, use the following guidelines:

- During deployment, when you are adding many users and machines, set the schedule so that synchronization takes place frequently.
- Set the synchronization schedule depending on your environment and how often you add machines and users.

For example, you set synchronization to occur once a week. You know that users and machines were added to the directory service and you want to set ACLs for them, so you synchronize data immediately.

- When you are troubleshooting a problem or when you are testing ACLs or policy compliance, you can synchronize data on demand.

- If you are using Active Directory with automatic discovery, synchronization for changes in Active Directory is affected by the following factors:
  - The LDAP-to-database synchronization schedule
  - The Active Directory and global catalog replication cycle
  - The Scanner Service schedule

As a result, changes in Active Directory (for example, the deletion of a machine) might not be reflected in areas affected by LDAP-to-database synchronization, such as policy compliance and ACLs, until Active Directory and global catalog replication is complete.

You can synchronize data on demand or through a recurring schedule.

#### ► To synchronize data on demand

- 1 Choose Applications > Console > System Settings and then click the Data Source tab.
- 2 Click the LDAP-to-Database Synchronization Service link.
- 3 In the Synchronization Status area, click Start Synchronization.  
A message appears when synchronization completes.
- 4 Click Save.

#### ► To synchronize data through a recurring schedule

- 1 Choose Applications > Console > System Settings and then click the Data Source tab.
- 2 Click the LDAP-to-Database Synchronization Service link.
- 3 In the Synchronization Schedule area, specify the frequency.
- 4 Click Save.

When you return to the LDAP-to-Database Synchronization Service page, the Synchronization Status area shows the date and time when the synchronization service last ran and when it is scheduled to run again.

# Configuring the CMS for integration with a NAP database

If you are using Network Access Protection (NAP) in your environment, you can configure a NAP database and CMS integration to get reports on machines that are currently quarantined by the Network Policy Server (NPS) that provide data to determine why the machines were quarantined.

## ► To configure the CMS for NAP integration

- 1 Choose Applications > Console > System Settings and then click the Data Source tab.
- 2 Click the NAP Database link.
- 3 On the NAP Database page, enter the following information:
  - **NAP database host name**—the name of the machine on which the NAP server logging database is running
  - **NAP database port**—the port number used to connect to the database remotely, often 1433 for Microsoft SQL Server
  - **NAP database service name**—the database name, usually NPSODBC
  - **NAP database user name**
  - **NAP database user password**
- 4 Click Check Connection to validate the database information that you provided.
- 5 Click OK.

# Chapter 10 Setting up access control lists

This chapter describes the access control lists (ACLs) that determine the permissions for each user who logs in to use the BMC Marimba Client Automation browser-based applications.

The following topics are provided:

- What are access control lists? (page 164)
- Target view and user/group view (page 165)
- Overview of targets (page 166)
- Assigning permissions for ACLs (page 170)
- Assigning permissions for applications (page 174)
- Deleting permissions for ACLs and applications (page 180)
- Deleting ACL users (page 182)
- Inheritance of permissions (page 183)

To change the system settings, you must be logged in as a primary administrator. To check, place the mouse pointer over the Status icon.

## What are access control lists?

Access control lists (ACLs) determine the permissions each user has for a particular object, in this case a target. A target can be a machine or a direct service object that contains machines (for example, a group of machines or a collection). On the console, each target can have an ACL that identifies the administrator or groups of administrators who have permission to view and change permissions for that target. For more information, see “Overview of targets” on page 164.

You set permissions for users in the console (Applications > Console > System Settings > Access Control tab), but the permissions are enforced at the application level.

For example, an ACL gives Joe, an administrator, permissions to assign policies to certain targets. Another ACL denies members of the Engineering group permissions to view the query results for certain targets.

**When you should use ACLs.** You might want to assign permissions for the following reasons:

- To enable certain administrators to view certain targets in Policy Manager, but prevent them from assigning policies to those targets.
- To enable certain administrators to assign policies to certain targets in Policy Manager.
- To limit certain administrators from assigning or viewing policies for certain targets in Policy Manager.
- To enable certain users and administrators to view certain targets in Report Center.
- To enable certain administrators to change permissions for certain targets in Policy Manager and Report Center.
- To enable certain standard administrators to view certain targets. (A primary administrator must assign at least one ACL to a standard administrator so the standard administrator can view targets.)

**Requirements for using ACLs.** Before using ACLs, make sure you meet the following requirements:

- Add a database and a directory service to the console. For information, see “Adding or editing a database” on page 158 and “Adding or editing a directory service” on page 145.

- Use a directory service for user authentication. For information, see “Selecting the user authentication type” on page 128.
- Assign roles to the groups of users who use the console. For information, see “Mapping roles to groups in a directory service” on page 137.
- Synchronize data from the directory service with the database. For more information, see “Synchronizing data from the directory service with the database” on page 160.

**ACLs for directory service groups.** You can set up access control lists for the groups (for example, countries, companies, divisions, or organizational units) established in a directory service.

If you plan the directory service implementation (or re-implementation) when you plan the BMC Marimba Client Automation implementation, you might want to organize the endpoints in the directory service into the groups you need for access control lists.

However, if you have an existing directory service with the following criteria:

- The endpoints in the directory service belong to groups that do not ideally match the partitioning for which you want to set up access control lists.
- Implementation or re-implementation of the directory service is not planned for the BMC Marimba Client Automation implementation.

You then have the following options:

- In the directory service, create groups (organizational units) that point to the endpoints so that they match the partitioning for which you want to set up access control lists. Set up access control lists based on the groups.
- In Report Center, create collections queries that result in machine groups that match the partitioning for which you want to set up access control lists. Set up access control lists based on the collections. For more information, see the *BMC Marimba Client Automation Report Center User Guide*, available on the Marimba Channel Store.

## Target view and user/group view

When assigning permissions, there are two views you can use. Data entered in one view can be seen in the other view.

To see the views, choose Applications > Console > System Settings. Click the Access Control tab and then click the Permissions for Access Control Lists link.

- Target view

You select a target and then specify users and groups who you want to have permissions for that target. When you specify users and groups, select names (or folders containing names) that have user and user group icons. For information, see the icons in “Overview of targets” on page 166.

- User/group view

You select a user or group and then specify targets for which you want that user or group to have permissions. When you specify targets, you can select names (or folders containing names) for machine, machine group, container, domain, or collections icons or for user or user group icons to indicate machines for users and groups.

## Overview of targets

A *target* encompasses one or more *endpoints*. An endpoint is a machine (computer or other device) on which a tuner is running.

**Types of targets.** A target can be one of the following:

-  A user (an endpoint identified by a login name)
-  A machine
-  A user group
-  A machine group
-  A container or organizational unit (OU)
-  A domain in Active Directory
-  A collection, which is a group of machines resulting from a database or LDAP query. Collections have ACLs like any other target.

In Report Center, collections query results contain only designated machines that the query finds; that is, query results contain only those machines for which you have Report Read permission. In Policy Manager, you must have Policy Write permission to save the collections query results in the directory service. For more information, see the sections about collections in the *Report Center Administrator’s Guide* and the *Policy Management Administrator’s Guide*, available on the Marimba Channel Store.

-  *All Endpoints*, a special virtual group composed of all endpoints, including all users and machines.

## Browsing targets

The left side of the page in the target view shows the list of targets to which you can assign permissions. You can view the targets by navigating through the list, which can include individual users and machines, groups of users and machines, and collections resulting from database and LDAP queries. When you select a target, you can view the permissions assigned to it on the right side of the page.

When you first view the target list, you see Home, which consists of the high-level containers in the directory service where target information is stored. For example, in Active Directory, you usually see the root domains in the forest environment; you can expand the root domains to display the objects that can be used as targets in that domain.

The target icons that you see in the target view indicate how the console obtains the list of targets:

- **Domains**—An expandable domain icon  indicates that targets are being obtained from an Active Directory forest environment. Root and subordinate domains are represented by this icon.
- **Containers**—An expandable folder icon  indicates that targets are obtained from the directory service. Organizational units and containers are represented by this icon.
- **Users (sourced from transmitter)**—An expandable transmitter icon  indicates that users and user groups are obtained from the transmitter where you have published the Policy Service plug-in (using the Plug-in Configuration page).

## Searching for targets

You can search for targets in the current expanded target group or container. This is useful when working with containers that contain large numbers of sub-containers or organizational units that contain large numbers of members.

When you search for targets, you can use the following options:

- **Basic search**

You can search for targets using the common name (CN) and can specify a type to narrow the search. For more information, see “Basic search for targets” on page 169.

## ■ Advanced search

If you are familiar with LDAP queries and search filters, you can search for targets with more flexibility. For more information, see “Advanced search for targets” on page 167.

**Active Directory.** Active Directory does not get the total number of entries until you have paged through all of the search results. The list displays “...” for the total number of entries until you reach the last page.

## Basic search for targets

### ► To perform a basic search for targets

- 1 Choose Applications > Console > System Settings, click the Access Control tab, and then click the Permissions for Access Control Lists link.
- 2 Click the Target View tab.
- 3 On the left side of the page, click the container in which you want to perform a search.
- 4 Click the Basic Search link.
- 5 In the Search for field, enter the common name (CN) or part of the CN for a target.

The search is not case-sensitive.

You can use an asterisk (\*) as a wildcard. If an asterisk is part of the name, however, you must escape it so that it is not considered a wildcard. For more information, see “Special characters in search strings” on page 168.

- 6 In the Limit to field, select the type of target for which you are searching, or choose All types.
- 7 To further limit the search, you can select the Do not search sub-containers check box.
- 8 Click Go.

Search results are displayed below the search area. When results are displayed in the list, the path changes to indicate that you are viewing search results.

To return to the top-level target view, click the Home link.

To return to the view where you originally started the search, click the Target View tab.

## Advanced search for targets

Use advanced search if you are familiar with LDAP queries and search filters for the directory service you are using. Because the console passes the query directly to the directory service, the search is faster than basic search.

However, you cannot use advanced search to look for targets using the complete distinguished name (DN).

You can enter simple queries, for example, searching for targets with `users` in the CN:

```
cn=users
```

You can enter complex queries that use conditions, for example, searching for targets with either `users` or `groups` in the CN by using the `or` notation (`|`):

```
( | (cn=users) (cn=groups))
```

For more information about LDAP search filters, see <http://www.ietf.org/rfc/rfc2254.txt>.

### ► To perform an advanced search for targets

- 1 Choose Applications > Console > System Settings, click the Access Control tab, and then click the Permissions for Access Control Lists link.
- 2 Click the Target View tab.
- 3 On the left side of the page in target view, click the container in which you want to perform a search.
- 4 Click the Advanced Search link.
- 5 In the LDAP Query field, enter an LDAP search filter.

The search is not case-sensitive.

You can enter simple or complex queries, which the console passes directly to the directory service. If the query includes special characters (such as `*` `(` `)` `\`), see “Special characters in search strings” on page 168.

- 6 Click Go.

Search results are displayed below the search area. When results are displayed in the list, the path changes to indicate that you are viewing search results.

To return to the top-level target view, click the Home link.

To return to the view where you originally started the search, click the Target View tab.

## Special characters in search strings

Some characters require special representation when you enter them in search strings, either from the browser-based interface or the command line. You must use the hexadecimal ASCII code for the character, preceded by a backslash. The special characters are summarized in Table 10-1.

Table 10-1: Special characters in search strings

Special characters	ASCII value (hexadecimal)	Search string representation
*	0x2a	\2a
(	0x28	\28
)	0x29	\29
\	0x5c	\5c

Some examples of using special characters in search strings are shown in Table 10-2.

Table 10-2: Examples of searching for special characters

To search for...	Enter the following...	Comment
A string beginning with “abc(“	abc\28*	Shows how to represent a parenthesis.
A string containing an asterisk (“*”).	*\2A*	Shows how to represent an asterisk, preventing it from being interpreted as a substring indicator.
The string “C:\MyTarg”	C:\5cMyTarg	Shows how to represent a backslash.

## Assigning permissions for ACLs

By default, only primary administrators can see permissions for applications. However, they can give administrators permissions for applications by assigning to administrators ACL permissions for targets. Primary administrators cannot give operators permissions for applications.

When accessing permissions for applications, an administrator cannot assign targets to any user if the targets are not assigned to that administrator. Administrators cannot remove targets to which they are assigned.

Primary administrators can give the following permissions to administrators:

- **Access Control Read:** Lets an administrator see users who have permissions for targets that are assigned to that administrator, but the administrator cannot assign or remove other users for those targets.

The permission lets an administrator see user permissions in applications (Policy Manager and Report Center) for targets assigned to that administrator. For more information, see “Assigning permissions for applications” on page 174.

- **Access Control Write:** Lets an administrator see users who have permissions for targets that are assigned to that administrator, and the administrator can assign or remove other users for those targets.

The permission lets an administrator see and change user permissions in applications (Policy Manager and Report Center) for targets assigned to that administrator. For more information, see “Assigning permissions for applications” on page 174.

For a user or group to display in the target list, the user or group must be in the directory service and must have a role. Primary administrators assign user and group roles on the User Roles page (Applications > Console > System Settings > User Authentication > User Roles).

## Setting target permissions for ACLs

You must be a primary administrator to set target permissions.

### ► To set target permissions for ACLs (Target View)

- 1 Choose Applications > Console > System Settings, click the Access Control tab, and then click the Permissions for Access Control Lists link.
- 2 Click the Target View tab.
- 3 Under Targets, click the link for a target. To see additional targets, click the plus expander button.

The Users/Groups permissions table for the target you select appears on the right side of the page.

- 4 If the user or group to which you want to give permissions does not appear in the Users/Groups permissions table, add the user or group.
  - a In the Users/Groups permissions table, click Add Users/Groups.

- b Under Targets, click the link for the user or group to which you want to give permissions. To see additional users or groups, click the plus expander button next to a group.

The user or group that you select appears in the Users/Groups permissions table.

- c If you want to delete a user or group, select the check box for the user or group in the Users/Groups permissions table and click Remove.
- d Click OK.

The user or group that you added appears in the Users/Groups permissions table with ACL Read permission.

- 5 In the Users/Groups permissions table, select the check box for the user or group to which you want to change permissions and click Edit Permissions.

To select all users and groups, select the Users/Groups check box. To select more than one user or group, select multiple check boxes.

- 6 Under Permissions, select the permissions that you want to give the selected user or group.

You cannot clear all permissions in the Permissions area. For information, see “Deleting permissions for ACLs and applications” on page 180.

- 7 Click Save.

The user and group permission selections appear in the Users/Groups permissions table.

Tip: If you want to view other targets for a user or group, select the check box for the user or group in the Users/Groups permissions table and click View All Targets. To return to the Target View page, select the check box for the target in the Target permissions table on the User/Group View page and click View All Users/Groups.

## Setting user and group permissions for ACLs

You must be a primary administrator to set user and group permissions.

### ► **To set user and group permissions for ACLs (User/Group View)**

- 1 Choose Applications > Console > System Settings, click the Access Control tab, and then click the Permissions for Access Control Lists link.
- 2 Click the User/Group View tab.

- 3 Under Users/Groups, click the link for the user or group to which you want to give permissions.

The Target permissions table for the user or group you select appears on the right side of the page.

- 4 If the user or group to which you want to give permissions does not appear in the Users/Groups list, add the user or group.

a Click Add Users/Groups.

b Under Users/Groups, click the link for the user or group to which you want to give permissions. To see additional users or groups, click the plus expander button next to a group.

The user or group that you select appears on the right side of the page.

c If you want to delete a user or group, select the check box for the user or group on the right side of the page and click Remove.

d Click OK.

The user or group that you added appears in the Users/Groups list. This user or group also appears in the Users/Groups list for application permissions.

- 5 If the target to which you want to give permissions does not appear in the Target permissions table, add the target.

a Click Add Targets.

b Under Targets, click the link for the target to which you want to give permissions. To see additional targets, click the plus expander button next to a target.

The target that you select appears in the Target permissions table.

c If you want to delete a user or group, select the check box for the user or group in the Target permissions table and click Remove.

d Click Save.

The target that you added appears in the Target permissions table with ACL Read permission.

- 6 In the Target permissions table, select the check box for the target to which you want to change permissions and click Edit Permissions.

To select all targets, select the Targets check box. To select more than one target, select multiple check boxes.

- 7 Under Permissions, select the permissions that you want to give the selected target.

You cannot clear all permissions in the Permissions area. For information, see “Deleting permissions for ACLs and applications” on page 178.

- 8 Click Save.

The permission selections appear in the Target permissions table.

Tip: If you want to view other users or groups for a target, select the check box for the target in the Target permissions table and click View All Users/Groups. To return to the User/Group View page, select the check box for the user or group on the right side of the Target View page and click View All Targets.

## Assigning permissions for applications

You can assign permissions for Policy Manager and Report Center. The products must be installed and running for the user permissions to be accessible.

### Working with Policy Manager permissions

Primary administrators can view and change user permissions for all Policy Manager targets.

For those Policy Manager targets, administrators who have

- Access control read permission for targets can view user permissions.
- Access control write permission for targets can view and change user permissions.

For more information, see “Assigning permissions for ACLs” on page 170.

### Policy Read and Policy Write permissions

Policy Manager has Policy Read and Policy Write permissions. The following table shows a comparison between the permissions.

An administrator can...	Policy Read	Policy Write
View a target	Yes	Yes
View policies for a target	Yes	Yes

An administrator can...	Policy Read	Policy Write
Assign policies to a target	No	Yes
Edit an existing policy for a target	No	Yes
Delete an existing policy for a target	No	Yes
View packages assigned to a target	Yes	Yes
Assign packages to a target	No	Yes
Edit assigned packages to a target	No	Yes
Delete assigned packages to a target	No	Yes
Edit settings, such as tuner and package properties, for a target	No	Yes

## Staging permissions

You can stage permissions for Policy Manager by setting the permissions while ACL functionality for Policy Manager is turned off. When you want the permissions to take effect, you can then turn on ACL functionality in Policy Manager. The top of the Permissions for Applications page shows if ACL functionality is enabled or disabled for Policy Manager.

For information about turning on ACL functionality for Policy Manager, see “Turning on and off the access control list feature” in the *BMC Marimba Client Automation Policy Management User Guide*.

If you turn on ACL functionality in Policy Manager before assigning permissions for the application, users see no targets and no policies for targets.

## Working with Report Center permissions

Primary administrators can view and change user permissions for all Report Center targets.

For those Report Center targets, administrators who have

- Access control read permission for targets can view user permissions.
- Access control write permission for targets can view and change user permissions.

For more information, see “Assigning permissions for ACLs” on page 168.

## Report Read (Allow) and Report Read (Deny) permissions

Report Center has the following user permissions:

- **Report Read (Allow)**

Lets administrators and operators view query results for the target.

- **Report Read (Deny)**

Does not let administrators and operators view query results for the target.

The deny permission overrides the allow permission: if the deny permission is assigned to an administrator or operator (directly or through inheritance), the administrator or operator cannot view query results for the target.

## Staging permissions

You can stage permissions for Report Center by setting the permissions while ACL functionality for Report Center is turned off. When you want the permissions to take effect, you can then turn on ACL functionality in Report Center. The top of the Permissions for Applications page shows if ACL functionality is enabled or disabled for Report Center.

For information about turning on ACL functionality for Report Center, see “Enabling access control functionality” in the *BMC Marimba Client Automation Report Center User Guide*.

If you turn on ACL functionality in Report Center before assigning permissions for the application, users see no data in Report Center query results.

## Setting target permissions for applications

You must be a primary administrator or an administrator with permissions for ACLs to set target permissions.

### ► To set target permissions for an application (Target View)

- 1 Choose Applications > Console > System Settings, click the Access Control tab, and then click the Permissions for Applications link.
- 2 Click the Target View tab.
- 3 Under Targets, click the link for a target. To see additional targets, click the plus expander button.

The Users/Groups permissions table for the target you select appears on the right side of the page.

- 4 If the user or group to which you want to give permissions does not appear in the Users/Groups permissions table, add the user or group.

a In the Users/Groups permissions table, click Add Users/Groups.

b Under Targets, click the link for the user or group to which you want to give permissions. To see additional users or groups, click the plus expander button next to a group.

The user or group that you select appears in the Users/Groups permissions table.

c If you want to delete a user or group, select the check box for the user or group in the Users/Groups permissions table and click Remove.

d Click OK.

The user or group that you added appears in the Users/Groups permissions table. If you are running Policy Manager, the user or group has Policy Read permission. If you are running Report Center, the user or group has Report Read permission.

- 5 In the Users/Groups permissions table, select the check box for the user or group to which you want to change permissions and click Edit Permissions.

To select all users and groups, select the Users/Groups check box. To select more than one user or group, select multiple check boxes.

- 6 Under Permissions, select the permissions that you want to give the selected user or group.

If an application is not installed and running, you do not have access to the permissions for the application.

You cannot clear all permissions in the Permissions area. For more information, see “Deleting permissions for ACLs and applications” on page 180.

- 7 Click Save.

The user and group permission selections appear in the Users/Groups permissions table.

Tip: If you want to view other targets for a user or group, select the check box for the user or group in the Users/Groups permissions table and click View All Targets. To return to the Target View page, select the check box for the target in the Target permissions table on the User/Group View page and click View All Users/Groups.

- 8 After you set target permissions for an application, you must access that application and turn on access control functionality.

For Policy Manager, see “Turning on and off the access control list feature” in the *BMC Marimba Client Automation Policy Management User Guide*.

For Report Center, see “Enabling access control functionality” in the *BMC Marimba Client Automation Report Center User Guide*.

## Setting user and group permissions for applications

You must be a primary administrator or an administrator with permissions for ACLs to set user and group permissions.

You can assign application permissions that a user or group has for targets. For a user or group to display in the list from which you can select, the user or group must be in the directory service and must have a role. Primary administrators assign user and group roles on the User Roles page (Applications > Console > System Settings > User Authentication > User Roles).

### ► **To set user and group permissions for an application (User/Group View)**

- 1 Choose Applications > Console > System Settings, click the Access Control tab, and then click the Permissions for Applications link.
- 2 Click the User/Group View tab.
- 3 Under Users/Groups, click the link for the user or group to which you want to give permissions.

The Target permissions table for the user or group you select appears on the right side of the page.

- 4 If the user or group to which you want to give permissions does not appear in the Users/Groups list, add the user or group.
  - a Click Add Users/Groups.

- b Under Users/Groups, click the link for the user or group to which you want to give permissions. To see additional users or groups, click the plus expander button next to a group.

The user or group that you select appears on the right side of the page.

- c If you want to delete a user or group, select the check box for the user or group on the right side of the page and click Remove.
- d Click OK.

The user or group that you added appears in the Users/Groups list. This user or group also appears in the Users/Groups list for ACL permissions.

- 5 If the target to which you want to give permissions does not appear in the Target permissions table, add the target.

- a Click Add Targets.
- b Under Targets, click the link for the target to which you want to give permissions. To see additional targets, click the plus expander button next to a target.

The target that you select appears in the Target permissions table.

- c If you want to delete a target, select the check box for the target in the Target permissions table and click Remove.
- d Click OK.

The target that you added appears in the Target permissions table. If you are running Policy Manager, the target has Policy Read permission. If you are running Report Center, the target has Report Read permission.

- 6 In the Target permissions table, select the check box for the target to which you want to change permissions and click Edit Permissions.

To select all targets, select the Targets check box. To select more than one target, select multiple check boxes.

- 7 Under Permissions, select the permissions that you want to give the selected target.

If an application is not installed and running, you do not have access to permissions for the application.

You cannot clear all permissions in the Permissions area. For more information, see “Deleting permissions for ACLs and applications” on page 180.

- 8 Click Save.

The permission selections appear in the Target permissions table.

Tip: If you want to view other users or groups for a target, select the check box for the target in the Target permissions table and click View All Users/Groups. To return to the User/Group View page, select the check box for the user or group on the right side of the Target View page and click View All Targets.

- 9 After you set user and group permissions for an application, you must access that application and turn on access control functionality.

For Policy Manager, see “Turning on and off the access control list feature” in the *BMC Marimba Client Automation Policy Management User Guide*.

For Report Center, see “Enabling access control functionality” in the *BMC Marimba Client Automation Report Center User Guide*.

## Deleting permissions for ACLs and applications

You must be a primary administrator to delete permissions for ACLs. You must be a primary administrator or an administrator with ACL permissions to delete permissions for applications.

If you no longer want a user or group to have permissions for a target, you can delete permissions for that particular user or group. You can delete only permissions that are explicitly assigned to a target, user, or group.

You can delete a user or group from the Users/Group list and consequently delete permissions for all targets for that user or group. For information, see “Deleting ACL users” on page 182.

You cannot delete inherited permissions. For information, see “Inheritance of permissions” on page 183.

## Deleting target permissions

You can delete target permissions for ACLs and applications.

### ► To delete target permissions for ACLs and applications (Target View)

- 1 Choose Applications > Console > System Settings and then click the Access Control tab.

- 2 Click the Permissions for Access Control Lists link or the Permissions for Applications link.
- 3 Click the Target View tab.
- 4 Under Targets, click the link for the target for which you want to delete permissions. To see additional targets, click the plus expander button next to a target.

The Users/Groups permissions table for the target you select appears on the right side of the page.

- 5 In the Users/Groups permissions table, select the check box for the user or group for which you want to delete permissions and click Delete Permissions.  
To select all users and groups, select the Users/Groups check box. To delete permissions for more than one user or group, select multiple check boxes.
- 6 In the confirmation page, click Delete.

The user or group no longer appears in the Users/Groups permissions table.

## Deleting user and group permissions

You can delete user and group permissions for ACLs and applications.

### ► **To delete user and group permissions for ACLs and applications (User/Group View)**

- 1 Choose Applications > Console > System Settings and then click the Access Control tab.
- 2 Click the Permissions for Access Control Lists link or the Permissions for Applications link.
- 3 Click the User/Group View tab.
- 4 Under Users/Groups, click the link for the user or group for which you want to delete permissions.

The Target permissions table for the user or group you select appears on the right side of the page.

- 5 In the Target permissions table, select the check box for the target for which you want to delete permissions and click Delete.

To select all targets, select the Targets check box. To delete permissions for more than one target, select multiple check boxes.

- 6 In the confirmation page that appears, make sure that this is the target for which you want to delete permissions and click Delete.

The target no longer appears in the Target permissions table. If the target for which you delete permissions does not have permissions for other users or groups, the user or group is removed from the Users/Groups list on the User/Group View page.

## Deleting ACL users

You can delete a user or group from the Users/Groups list and consequently delete permissions for all targets for that user or group. You can delete a user or group that has no assigned permissions.

You can delete a user or group that has inherited and explicitly assigned permissions. For information, see “Inheritance of permissions” on page 181.

To delete a user or group with permissions for ACLs, you must be a primary administrator. To delete a user or group with permissions for applications, you must be a primary administrator or an administrator with ACLs write permission for all of the explicitly assigned targets for that user or group.

### ► **To delete an ACL user**

- 1 Choose Applications > Console > System Settings and then click the Access Control tab.
- 2 Click the Permissions for Access Control Lists link or the Permissions for Applications link.
- 3 Click the User/Group View tab.
- 4 Under Users/Groups, click the link for the user or group that you want to delete.

The Target permissions table for the user or group you select appears on the right side of the page.

- 5 In the Target permissions table, click Delete User.

A confirmation page displays the assigned targets for that user.

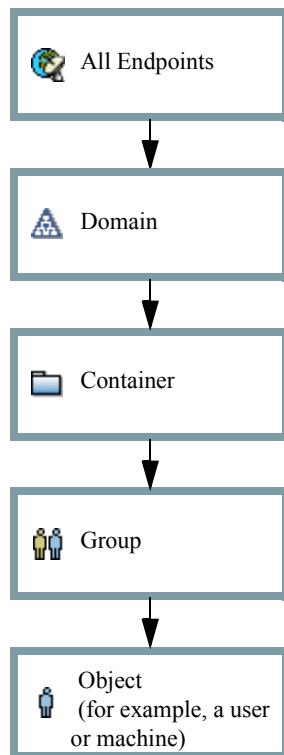
- 6 Click Delete.

The user or group no longer appears in the User/Groups list.

# Inheritance of permissions

Permissions and ACLs are inherited. An object inherits the permissions of the domains, containers, and groups to which it belongs. For example, if a domain is assigned access control read permissions on a target, a user in the domain inherits the access control read permissions and can view permissions for the target. Figure 10-1 shows how permissions are inherited:

Figure 10-1: Inheritance of permissions



User permissions are determined by a union of the permissions the user inherits from parents (groups, containers, domains, “All Endpoints”) and the permissions directly assigned to the user. The console lets you view both inherited and directly assigned permissions.

## ► To view inherited permissions for a target, user, or group

For targets, users, or groups that inherit permissions, a gray check mark appears for each permission that it inherits.

For example, in Figure 10-2, the gray check marks under the Policy Read and Report Read permissions columns indicate that the `en_admin_group` group of users has inherited permissions for the `british_24` target machine.

Figure 10-2: Gray check marks indicate inherited permissions

The screenshot shows a web-based interface titled "Users/Groups permissions for: `british_24`". At the top, there are buttons for "Edit Permissions", "Delete", "View All Targets", and "Add Users/Groups". Below these are several tabs: "Users/Groups" (selected), "Policy Read", "Policy Write", "Report Read", and "Report Deny". A table lists a single entry: "en\_admin\_group" with a user icon. Under the "Policy Read" column, there is a gray checkmark with a cursor hovering over it, and a tooltip box says "1 inherited permission(s)".

## ► To view how permissions are inherited

Click the arrow next to the gray check mark to view how the target, user, or group inherited the permissions.

For example, in Figure 10-3, clicking the gray check mark under the Policy Read column shows that the `british_24` target machine inherits permissions for the container `MarimbaComputers`. Because the `en_admin_group` group of users has policy read permissions for the container `MarimbaComputers`, `en_admin_group` also has policy read permissions for `british_24`.

Figure 10-3: Displaying how permissions are inherited

The screenshot shows a user interface for managing permissions. At the top, it says "Users/Groups permissions for: british\_24". Below that is a toolbar with "Edit Permissions", "Delete", "View All Targets", and "Add Users/Groups" buttons. To the right of the toolbar are buttons for "Policy Read", "Policy Write", "Report Read", and "Report Deny". A table titled "POLICY\_READ Inherited From" lists the inheritance source: "User/Group" (en\_admin\_group) and "Target" (MarimbaComputers).

User/Group	Target
en_admin_group	MarimbaComputers

If an administrator inherits permissions from more than one source, all sources are displayed.

For example, in Figure 10-4, clicking the gray check mark under the Policy Read column shows that the `british_24` target machine inherits permissions from two containers: `MarimbaComputers` and `Computers`. `british_24` is included in both containers, and both containers give the `en_admin_group` group of users policy read permissions to the `british_24` machine.

Figure 10-4: Example showing permissions inherited from two sources

This screenshot is similar to Figure 10-3, but it highlights the inheritance of multiple sources. A mouse cursor is hovering over the "Policy Read" column for the "en\_admin\_group" row. A tooltip box appears with the text "2 inherited permission(s)". The rest of the interface is identical to Figure 10-3.

User/Group	Target
en_admin_group	MarimbaComputers
en_admin_group	Computers

### ► To override inherited permissions

You can override the inherited permissions by setting permissions directly for the target, user, or group.

When you override permissions, the gray check mark becomes a green check mark. You can still click the arrow next to the check mark to view how and what permissions the target, user, or group inherited.

For example, in Figure 10-5, the green check marks under the Policy Read, Policy Write, and Report Read columns show that permissions have been directly assigned the `en_admin_group` group of users that override any other permissions it inherits for the `british_24` machine.

Figure 10-5: Green check marks indicate that directly assigned permissions override inherited permissions

The screenshot shows a web-based interface for managing user permissions. At the top, it says "Users/Groups permissions for: **british\_24**". Below this is a toolbar with "Edit Permissions", "Delete", "View All Targets", and "Add Users/Groups". The main area has a table with columns: "Users/Groups" (checkbox), "Policy Read", "Policy Write", "Report Read", and "Report Deny". A row shows the "en\_admin\_group" user with green checkmarks in all four columns. A tooltip "2 inherited permission(s)" appears over the "Policy Read" column. A cursor arrow points to the "Policy Read" checkbox for the "en\_admin\_group".

Chapter

# 11 Action Request System settings

The AR Settings tab lets you configure the console to communicate with the Action Request System mid tier, server, and database. You must set up the console before you can launch BMC Marimba Client Automation Policy Manager and Deployment Manager from within AR System.

---

Note: It is recommended that you configure the Definitive Software Library settings in Transmitter Administration. For information, see the *BMC Marimba Client Automation Transmitter and Proxy User Guide*.

---

The following topics are provided:

- Configuring the AR settings (page 188)
- Configuring for the AR database (page 189)

# Configuring the AR settings

The mid tier facilitates communication between a browser (in this case, BMC Marimba Client Automation) and the AR System server. The mid tier lets a web browser become a fully functional AR System client.

## ► To communicate with the AR System servers

- 1 Choose Applications > Console > System Settings.
- 2 Click the AR Settings tab and then click the AR Settings link.
- 3 In the Mid tier host field, enter the host name of the machine on which the mid tier web server is running. Make sure the mid tier is reachable.
- 4 In the Mid tier port field, enter the port number of the machine on which the mid tier web server is running. The default is 80.
- 5 In the AR Server field, enter name of the AR System server being used by the mid tier.
- 6 In the User name field, enter the user name for accessing AR System.

The user account must have the correct permissions to access the AR System Change Management application and the Definitive Software Library.

- 7 In the Password field, enter the password for accessing AR System.
- 8 In the HTTP timeout field, enter the timeout for the web services HTTP messages. The default is 50 seconds.
- 9 In the Company field, enter the company related to the task. The default is Global.
- 10 To activate SSL on the server for communication with AR System, select the Use SSL check box.
- 11 Click OK.

# Configuring for the AR database

Every AR System server is configured to a database, which stores the definitions and data. This page lets you specify a database location and name so Report Center can leverage the AR System DSL to generate inventory reports with normalized names, reports based on CMDB queries, and so on.

There are several possible database platform combinations when establishing a communication link between the BMC Marimba Client Automation and Action Request systems. The BMC Marimba Client Automation Action Request systems are supported on the Oracle and SQL Server database platforms.

## ► To communicate with the AR System database

- 1 Choose Applications > Console > System Settings.
- 2 Click the AR Settings tab and then click the AR Database link.
- 3 In the AR database type field, select a database type from the list.
- 4 In the AR database host name field, enter the name of the machine on which the AR System database is running.
- 5 In the AR database port field, enter the port number used to remotely connect to the database. Port numbers are usually 1521 for Oracle and 1433 for SQL Server.
- 6 In the AR database service name field, enter the AR System database name. The default is ARSYSTEM.

For SQL Server, enter the AR System Database Name.

For Oracle, enter the AR System SID.

- 7 Click OK.



Chapter

# 12 Working with web services

The BMC Marimba Client Automation Web Services tab in the CMS console displays a list of the available web services that help you work more efficiently.

The CMS SecurityTicketService web service provides seamless authentication with the Action Request System. For example, you logged in and are working in AR System when you have to perform a task that is in the BMC Marimba Client Automation CMS console. Instead of logging in manually to the CMS console, the SecurityTicketService web service authenticates your user name and lets you use the CMS console without having to log in.

The following topics are provided:

- Viewing the web services (page 192)
- Changing the service status (page 192)
- Publishing web services to the Atrium Web Service Registry (page 193)

## Viewing the web services

With BMC Marimba Client Automation web services, you can see a list of the web services that are provided, along with the provider, a description of the service, and the service status. You can also view the WSDL for a specific web service to get the protocols and formats for that service. Each service is automatically added to the list by its provider channel.

Two important services are

- **SecurityTicketService**

Lets you move between AR System and CMS. This service must be running for seamless authentication to work.

- **PolicyMgrTaskService**

Lets you verify compliance for policy-based tasks based on a target, package, or both.

### ► To work with the web services

- 1 Choose Applications > Console > System Settings.
- 2 Click the Web Services tab.
- 3 Click the Web Services link.

For each web service, the provider, a description of the service, the status, and a link to the WSDL view are provided.

- 4 If you want to return to the main page, click OK.
- 5 If you want to view the WSDL for a web service, click View for that service. When done, click OK to return to the list.

In the WSDL view, the URL is automatically filled in with the CMS host name and port.

## Changing the service status

Because the services in the list are automatically added by the appropriate channels, you cannot add, delete, or stop services.

If the status shows that a service is stopped, you can, however, change the status to running by working with the channel.

- If the channel is stopped, start the channel using Tuner Administration. After the channel starts, the service also starts.
- If the channel is running, check the channel configuration. The configuration set-up might be preventing the service from running.  
For example, if PolicyMgrTaskService is not running, the LDAP service was not set up correctly. Go to Policy Manager to fix configuration issues — check the server logs for information.

## Publishing web services to the Atrium Web Service Registry

Using the Publish Web Service page, you can publish a web service to the Atrium Web Service Registry.

### ► **To publish a web service to the Atrium Web Service Registry**

- 1 Access the Publish Web Service page by clicking the Publish Web Services link on the Web Services tab in System Settings.
- 2 Enter the BMC Atrium Web Service Registry server name and port number in the fields provided.
- 3 Enter the user name and password.
- 4 Find the web service in the table that you want to publish to the BMC Atrium Web Service Registry and click the corresponding Publish button.
- 5 Click OK.



Chapter

# 13 Troubleshooting system settings

This section provides suggestions for troubleshooting common problems with the system settings.

**Problem:**

I cannot log in to Report Center or Policy Manager. For example, I get an error message that says, “Unable to log in. Please contact your primary administrator, or check the following....”

**Possible solutions:**

The most common problem when logging in is incorrectly typing the user name, the password, or both. Try entering them again. If you have made sure that you are entering the correct user name and password but still cannot log in, check the items described in this section.

---

Note: Some solutions might require access to pages that are reserved for primary administrators. If you do not have access to these pages, contact the primary administrator.

---

You might have to log in with the emergency user name, which is `admin`, and its password. By default, no password is set, but it is recommended that you do set an emergency password.

If you have problems logging in, first verify that the user name is either in the local user database or in the directory service, whichever you are using to authenticate users:

- 1 Find out which data source you are using by going to the User Authentication Type page (choose Applications > Console > System Settings > User Authentication tab > User Authentication Type link).

Either the Directory Service option or the Local User Database option is selected.

- 2 Do one of the following:

- If the Local User Database option is selected: Verify that the user is in the local user database by going to the Local User Database page (choose Applications > Console > System Settings > User Authentication tab > Local User Database link).
- If the Directory Service option is selected: Verify that the user is in the directory service by using the directory service's administration tool. Users must belong to a group, and the group must be mapped to a user role in the User Roles page (choose Applications > Console > System Settings > User Authentication tab > User Roles link).

If a directory service is being used for user authentication, you can check the following possible causes:

- No directory service has been specified or directory service settings are incorrect.

Check the directory service settings by going to Edit Directory Service page (choose Applications > Console > System Settings > Data Source tab > Directory Services link). Make sure that the field information is correct.

If you change the directory service settings, any users who are currently logged in are asked to log in again. You might want to warn users who are currently using the console or any applications before you change the directory service settings.

- The directory service is offline or not available.

Check that the directory service is running and that CMS is able to connect to it.

- Groups in the directory service have not been mapped to user roles.

Check that groups have been mapped to user roles by going to the User Roles page (choose Applications > Console > System Settings > User Authentication tab > User Roles link). Make sure that groups you want to have access are specified for one of the user roles. To specify multiple groups, enter a comma-separated list of groups for each role.

- If you are using Active Directory for user authentication, and you have multiple groups and users with the same name in different domains within your enterprise, use fully qualified distinguished names when you specify the groups on the User Roles page and when you log in with a user name and password. Otherwise, CMS cannot properly authenticate users.

**Note:** If you want to use the built-in administrator account created by Active Directory using the user principal name (UPN) format (for example, administrator@company.com), you must set up the UPN attribute for the administrator account using the Microsoft Management Console (MMC). By default, no UPN attribute is assigned to the administrator account. If the UPN attribute cannot be found for an account, the user cannot log in; this scenario is true even when an account with the same user name has been set up with a UPN attribute in one domain but not another (for example, administrator@root1.com has been given a UPN attribute, while administrator@east.root1.com has not).

#### Problem:

When I try to enter the URL for accessing Report Center or Policy Manager (`http://<machine_name>:8888`), another browser-based application appears. If another application is already using the default port 8888, how do I change the port number for Report Center or Policy Manager?

#### Possible solution:

The Common Management Services channel (which in turn runs Report Center and Policy Manager) first attempts to use port 8888 by default, but if it finds that port is already in use, it attempts to use port 8889. If that port is in use, it attempts to use port 8890, and so on. Keeping this behavior in mind, you can use the following solutions:

- If you are attempting to access Report Center or Policy Manager remotely, you can try using port 8889.
- If you are on the machine that hosts Report Center or Policy Manager, you can use the CMS command-line `-getPort` option to find out which port number is being used (for example, `runchannel http://trans.acme.com/cms -getPort`), and then you can enter the URL with that port number.
- If you are on the machine that hosts Report Center or Policy Manager, you can use the Common Management Services command-line option called `-setPort` to change the port number (for example, `runchannel http://trans.acme.com/cms -setPort 8880`), and then you can enter the URL with that port number.

**Problem:**

I stopped working in Report Center or Policy Manager to do something else. When I returned and clicked something, the login page appeared.

**Possible solution:**

You were logged out automatically. Users who have been idle or inactive for a specified number of minutes are automatically logged out to help to prevent unauthorized access to the applications. You can change this setting on the User Timeout page (choose Applications > Console > System Settings > General tab > User Timeout link). The default user timeout is 60 minutes. You can disable the user timeout by setting it to 0 minutes.

**Problem:**

I changed the number of minutes specified on the User Timeout page, but the new user timeout I specified does not seem to be taking effect.

**Possible solution:**

If you change the User Timeout setting, the new timeout does not apply to users who are already logged in. The new timeout takes effect the next time users log in. You must log out and log in again for the new setting to take effect.

**Problem:**

I cannot find the log files.

**Possible solution:**

Log files for applications are stored in the tuner workspace directory. You can find the exact location of the log files by looking in the Log Files page (choose Applications > Console > System Settings > General tab > Log Files link).

**Problem:**

When clicking a link in the system settings, I get redirected to the login page.

**Possible solution:**

Being redirected to the login page might be a result of having cookies disabled for the browser. You must configure the browser to accept cookies before using BMC Marimba Client Automation browser-based applications.

**Problem:**

I created some new users to Active Directory and made sure the new users belong to groups that have been assigned user roles in the console system settings. However, logging in as any of the new users results in the error message “You do not have privileges to access this server.”

**Possible solution:**

CMS is using cached information to authenticate users and does not recognize the newly added users until the cache expires and it contacts the directory service (Active Directory in this case). This situation occurs because CMS has caching turned on by default when you configure a directory service to work with CMS. Cache is turned on by default for improved performance. CMS refreshes the directory service cache at time intervals specified on the Directory Service page. For more information, see the caching options described in “Advanced settings for the directory service” on page 153.

You can force CMS to refresh its cache immediately and recognize the newly added users by restarting CMS. For more information, see “Restarting CMS and the console” on page 87.



# Chapter 14 Infrastructure Status Monitor

The Infrastructure Status Monitor provides health-related metrics about your BMC Marimba Client Automation infrastructure. It provides an overall, health-at-a-glance view of your infrastructure components and provides detailed monitoring views of Master transmitters, Repeaters, Mirrors, Proxies and clients.

Using the Infrastructure Status Monitor, you can monitor your environment to ensure that your BMC Marimba Client Automation infrastructure is running properly and to diagnose any issues that arise.

This section contains the following topics:

- “Configuring the Infrastructure Status Monitor” on page 203
- “Viewing the Infrastructure Status Monitor” on page 207
- “Viewing component tabs” on page 211
- “Viewing audit log entries” on page 220
- “Configuring settings (Setting tab)” on page 221
- “Using a custom channel to collect and display customized stats attributes in ISM” on page 227
- “Viewing the status of deployed jobs in ISM dashboard and using Report Center query” on page 245

---

Note: The Infrastructure Status Monitor does not maintain historical data.

---

# Configuring the Infrastructure Status Monitor

This section provides the following procedures required to configure the Infrastructure Status Monitor:

- “Configure the Infrastructure Status Monitor”
- “Configure settings for the Infrastructure Status Monitor”
- “Configure the master transmitter for the Infrastructure Status Monitor”

## ► Before you begin

- For fresh installations of the BMC Marimba Client Automation infrastructure, ensure that all post installation steps have been completed through “Setting up the Infrastructure Status Monitor” as listed in the *BMC Marimba Client Automation Installation Guide*.
- For upgraded installations of the BMC Marimba Client Automation infrastructure, complete the upgrade for the following components as described in “Part 4 Upgrade” of the *BMC Marimba Client Automation Installation Guide* before configuring the Infrastructure Status Monitor:
  - transmitters and proxies
  - CMS console
  - Report Center
- Ensure that the SNMP dashboard port number is open, available, and not blocked.
- The Inventory schema must be installed before the Infrastructure Status Monitor schema.

## ► Configure the Infrastructure Status Monitor

- 1 Create Infrastructure Status Monitor Write and Read database connection pools:
  - a From the CMS console, navigate to the Data Source Database page, go to Applications -> Console -> System Settings.
  - b Click the Data Source tab.
  - c Click the Database link.
  - d From the Database page, click Add a Database.

- e Enter the database information.
- f Type `hmadmin` in the **User name** field.
- g Enter the password. The default password is `hmadmin`.
- h Select **Set as default Infrastructure Status Monitor write Connection**.
- i Click **Check Connection** to determine if this database connection pool is successful. If successful, click **OK**. Otherwise, check the database information that you have provided.
- j Repeat steps “d” through “i” using `hmuser` as the user name with the default password of `hmuser` by selecting **Set as default Infrastructure Status Monitor Read Connection**.

The ISM Write Connection for `hmadmin` has full control over the Infrastructure Status Monitor objects. This user is used for the Logging Service plug-in.

The ISM Read Connection for `hmuser` has read access to the database views. This user is used for the Infrastructure Status Monitor view.

- 2 Configure the Logging plug-in from Report Center to enable the Infrastructure Status Monitor:
  - a From the CMS console, choose **Applications -> Report Center**. If any errors occur, restart Report Center.
  - b Click the **Configuration** tab.
  - c Click the **Logging Configuration** link.
  - d Type the Logging Service URL on the master transmitter (or on the load balancer if mirrors are configured to replicate contents from the master and are configured behind a load balancer).
  - e Click **OK**.
  - f Go to the Database section, and change the user name and password for the Infrastructure Status Monitor `hmadmin` user. The default user name and password are both `hmadmin`.
  - g Click **Preview** and then click the **Save and Publish** button.

If you have not installed the Infrastructure Status Monitor schema module, the following error message appears in the Logging Plug-in log file: Could not connect to ISM tables. Check the plugin configuration if it is configured with the valid ISM database user.

---

Note: The Logging plug-in and the database must be on the same time zone.

---

- 3 Subscribe to the Infrastructure Status Monitor channel from the tuner machine that hosts the CMS as described in “Subscribing to new applications” on page 75.

After logging in to the CMS and opening the Infrastructure Status Monitor, if any errors are displayed in the Infrastructure Status Monitor Dashboard, restart the Infrastructure Status Monitor channel.

## ► **Configure settings for the Infrastructure Status Monitor**

- 1 Access the Infrastructure Status Monitor from the CMS console:  
**Applications > Infrastructure Status Monitor.**
- 2 Configure the logging plug-in as described in “Configuring the logging plug-in” on page 220.
- 3 Define component health as described in “Defining component health” on page 220.
- 4 Set display preferences as described in “Setting display preferences” on page 223.

## ► **Configure the master transmitter for the Infrastructure Status Monitor**

- 1 From Tuner Administration or from a profile for the tuner hosting the master transmitter, click the **Advanced** and **ISM** tabs.
- 2 In **Server**, type the host name where the logging plug-in resides.
- 3 In **Port**, type the SNMP manager port number to enable SNMP traps/alerts in the transmitter.

The default is 162. The values you enter here for Server and Port set the following tuner property: `marimba.tuner.hm.dashboard=<plugin hostname>:<snmp manager port>`.

- 4 In **URL**, type the channel URL of the Logging Service.

For example: `http://mpl-esx:5282/ism/LoggingService`

Setting the URL enables statistics gathering. This URL and the Infrastructure Service must point to the same master transmitter. The URL value entered here sets the `marimba.tuner.hm.statsURL` tuner property.

- 5 Under **Component Reporting Schedule**, set the schedule for sending status information to the Infrastructure Status Monitor Dashboard.

The default schedule is every 15 minutes, daily. Setting the schedule here sets the `marimba.tuner.hm.schedule` tuner property. For example:  
`marimba.tuner.hm.schedule=every 1 days update at 4:15pm`

- 6 Click **Preview** and then **Apply**.

You must configure these settings in order to receive and view statistics and SNMP trap data from the Infrastructure Status Monitor Dashboard page.

## ► **Configure Infrastructure Status Monitor profile settings for server and client components**

You can update existing server profiles (Mirror/Repeater/Proxy/Reverse Proxy/Secure Reverse Proxy/CMS) and client (tuner) profiles to enable the Infrastructure Status Monitor features with the following settings on the Edit Profile page, Advanced tab > ISM tab:

- 1 In **Server**, type the host name or IP address of the master transmitter, mirror transmitter, or load balancer where the SNMP Alerts information is sent and where the Logging Service is running. Leave this field blank for proxy and client profiles.
- 2 In **Port**, type the dashboard port number. This can be configured to any valid port value. Default value is 162. Leave this field blank for proxy and client profiles. The port value you enter here sets the following tuner property:  
`snmp.manager.port`.
- 3 In **URL**, type the URL of the Logging Service on the master transmitter, mirror transmitter, or load balancer. For example:

`http://<transmitter-or-loadbalancerhost>/ISM/LoggingService`

- 4 Under **Component Reporting Schedule**, set the schedule for the components to send their status to the plug-in.

Updated profiles are applied to the server components in the next scheduled update of the Infrastructure Service channel on the server and client components.

For more information about profiles, see the Creating profiles, installers, and running deployments chapter in the *BMC Marimba Client Automation Installation Guide*.

# Viewing the Infrastructure Status Monitor

To access the Infrastructure Status Monitor, choose **Applications > Infrastructure Status Monitor** from the CMS console. The **Dashboard** tab is the default view.

## Dashboard tab

The Dashboard tab displays the overall health of your BMC Marimba Client Automation infrastructure. The page has four sections as shown in Figure 14-1:

- Server Component Status and Client Component Status
- Replication Status (Not In Sync)
- SNMP Alerts

## ■ Critical Server Component Status

**Dashboard**   **Master**   **Mirror**   **Repeater**   **Proxy**   **Client**   **Settings**   **bmcsoftware**

[Audit Log](#)

**Server Component Status**

Component	Status
Master[1]	Good
Mirror[2]	Good
Repeater[4]	Critical
Proxy[3]	Critical

Legend: ■ Critical ■ Warning ■ Good

**SNMP Alerts**

Host Name	Component	Alert Type	Alert Time	Details
blknode-pun-01	Master	Plugin error: Logger Plugin	08/19/2009 18:38:56	<a href="#">View</a>
blknode-pun-01	Master	Plugin error: Logger Plugin	08/19/2009 18:38:53	<a href="#">View</a>
blknode-pun-01	Master	Plugin error: Logger Plugin	08/19/2009 18:37:53	<a href="#">View</a>
blknode-pun-01	Master	Plugin error: Logger Plugin	08/19/2009 18:36:51	<a href="#">View</a>
blknode-pun-01	Master	Plugin error: Logger Plugin	08/19/2009 18:36:50	<a href="#">View</a>
blknode-pun-01	Master	Plugin error: Logger Plugin	08/19/2009 18:35:50	<a href="#">View</a>

**Client Component Status**

Total: 19

Status	Count
Critical	11
Warning	2
Good	6

Legend: ● Critical = 11 ● Warning = 2 ● Good = 6

**Replication Status**

Host Name	In Sync	Last Replication Time	Details
PUN-ETHANGAV-45	✓	08/20/2009 04:33:18	<a href="#">View</a>
ethangav-pun-01	✓	08/19/2009 17:54:16	<a href="#">View</a>
VM-W23-MAR33	✓	07/30/2009 08:38:13	<a href="#">View</a>

**Critical Server Component Status**

Host Name	Component	Status Updated Time	Details
PUN-ETHANGAV-45	Proxy	08/19/2009 23:38:09	<a href="#">View</a>
ethangav-pun-01	Repeater	08/19/2009 17:54:16	<a href="#">View</a>
VM-W28-MAR15	Proxy	08/19/2009 16:31:12	<a href="#">View</a>

Figure 14-1: Infrastructure Status Monitor

**Dashboard** **Master** **Mirror** **Repeater** **Proxy** **Client** **Settings** **bmcsoftware**

[Audit Log](#)

**Server Component Status**

Component	Status	Count
Master[1]	Good	1
Mirror[2]	Good	2
Repeater[4]	Critical	1
Repeater[4]	Good	3
Proxy[3]	Critical	2
Proxy[3]	Good	1

**Client Component Status**  
Total: 19

Status	Count
Critical	11
Warning	2
Good	6

**SNMP Alerts**

Host Name	Component	Alert Type	Alert Time	Details
blkhodke-pun-01	Master	Plugin error: Logger Plugin	08/19/2009 18:38:56	
blkhodke-pun-01	Master	Plugin error: Logger Plugin	08/19/2009 18:38:53	
blkhodke-pun-01	Master	Plugin error: Logger Plugin	08/19/2009 18:37:53	
blkhodke-pun-01	Master	Plugin error: Logger Plugin	08/19/2009 18:36:51	
blkhodke-pun-01	Master	Plugin error: Logger Plugin	08/19/2009 18:36:50	
blkhodke-pun-01	Master	Plugin error: Logger Plugin	08/19/2009 18:35:50	

**Replication Status**

Host Name	In Sy	Last Replication Time	Detail
PUN-ETHANGAV-45		08/20/2009 04:33:18	
ethangav-pun-01		08/19/2009 17:54:16	
VM-W23-MAR33		07/30/2009 08:38:13	

**Critical Server Component Status**

Host Name	Component	Status Updated Time	Details
PUN-ETHANGAV-45	Proxy	08/19/2009 23:38:09	
ethangav-pun-01	Repeater	08/19/2009 17:54:16	
VM-W28-MAR15	Proxy	08/19/2009 16:31:12	

## Server Component Status and Client Component Status

The Server Component Status section shows a bar chart of the health of each infrastructure server component along with the number of each component type. The Client Component Status section shows a pie chart of the health of all tuners in your environment.

The colors in the charts indicate the health of the component as defined from the **Settings** tab:

- Green indicates good health
- Yellow indicates a warning condition
- Red indicates a critical condition

Bars and pie slices with multiple colors indicate that multiple components of the same type are being monitored and currently have different health conditions.

You can click a bar in the chart or a slice in the pie chart to display the information page for the component type that you clicked.

## Replication Status (Not In Sync)

The Replication Status section shows the replication status for mirrors and repeaters that are not in sync. You can limit the view to one or the other by using the **Component** drop-down menu.

To display replication sync details for a specific host, click the **Details** icon in the same row. The Replication Sync Details page displays a log of replication activity.

## SNMP Alerts

The SNMP Alerts section shows SNMP alerts from masters, mirrors, repeaters, proxies, clients (tuners) and the CMS. You can display alerts from all of these components or only from specific component types using the **Component** drop-down menu. If you place your mouse cursor over the **Details** icon, hover text is displayed showing the alert description.

## Critical Server Component Status

The Critical Server Component Status section displays all infrastructure components whose status is critical. This status corresponds to how component health is defined on the Define Component Health page under the **Settings** tab.

You can display all critical components or only those of a specific component type using the **Component** drop-down menu. From the **Rationale** drop-down menu, you can select to display

- component hosts that are **Not Healthy** and are able to send data to the Infrastructure Status Monitor
- component hosts that have **Not Checked In** or have not sent data to the Infrastructure Status Monitor within the configured time period
- all server component hosts whose status is critical

You can define the “Not Checked in” time from the Set Display Preferences page on the **Settings** tab as described in “Setting display preferences” on page 223.

You can click the **Details** icon for a host name to display the Health Status page that contains detailed status, attributes, and metrics, including the group attributes that define the health of the component. For more information, see “Health Status page” on page 216.

## Viewing component tabs

The Infrastructure Status Monitor has a tab for each infrastructure component type.

### Master tab

The Master tab page displays the following sections:

- **Overview**—Contains a color-coded pie chart for the master transmitters in your environment that indicates the status for each host.
- **Component Details**—Contains a table that displays a row for each machine hosting a master transmitter along with its **Health** status, the **Load** on the host, **Requests Per Minute**, and **Status Updated Time**. From this table you can

- filter the table to show only the components with a particular status using the **Status** drop-down menu
- filter the table using the **Rationale** drop-down menu to show only the components that have one of the following conditions:
  - Not Healthy**—Displays components whose status is not healthy as defined on the Define Component Health page under the **Settings** tab.
  - Not Checked In**—Displays components that have not “checked in” with Infrastructure Status Monitor within the specified time as defined on the Set Display Preferences page on the **Settings** tab.
  - All**—Displays all tuners of any status or rationale.
- click the **Details** icon to display detailed status, attributes, and metrics, including the group attributes that define the health of the component as specified on the Define Component Health page.
- **SNMP Alerts**—Contains a table of SNMP alerts for the host. You can click the **Details** icon for a host name to display the Health Status page that contains detailed status, attributes, and metrics, including the group attributes that define the health of the component. For more information, see “Health Status page” on page 216.

## Mirror tab

The **Mirror** tab page displays the following sections:

- **Overview**—Contains a color-coded pie chart for the mirrors in your environment that indicates the status for each host.  
The **Mirror Statistics** link below the pie chart displays the following statistics for mirrors:
  - Load Distribution
  - Average Processing Time
  - Bytes Sent (KB)
  - Bytes Received (KB)
- **Component Details**—Contains a table that displays a row for each machine hosting a mirror along with its **Health** status, the **Load** on the host, **Requests Per Minute**, and **Status Updated Time**. From this table you can

- filter the table to show only the components with a particular status using the **Status** drop-down menu
- filter the table using the **Rationale** drop-down menu to show only the components that have one of the following conditions:
  - Not Healthy**—Displays components whose status is not healthy as defined on the Define Component Health page under the **Settings** tab.
  - Not Checked In**—Displays components that have not “checked in” with Infrastructure Status Monitor within the specified time as defined on the Set Display Preferences page on the **Settings** tab.
  - All**—Displays all tuners of any status or rationale.
- click the **Details** icon to display detailed status, attributes, and metrics, including the group attributes that define the health of the component as specified on the Define Component Health page.
- **SNMP Alerts**—Contains a table of SNMP alerts for the host. You can click the **Details** icon for a host name to display the Health Status page that contains detailed status, attributes, and metrics, including the group attributes that define the health of the component. For more information, see “Health Status page” on page 216.

## Repeater tab

The Repeater tab page displays the following sections:

- **Overview**—Contains a color-coded pie chart for the repeaters in your environment that indicates the status for each host.

The Repeater Group Statistics link below the pie chart displays a table of repeater statistics, organized by user-defined groups. See “Creating repeater groups and viewing group statistics” on page 217 for more information.
- **Component Details**—Contains a table that displays a row for each machine hosting a repeater along with its **Health** status, the **Load** on the host, **Requests Per Minute**, and **Status Updated Time**. From this table you can
  - filter the table to show only the components with a particular status using the **Status** drop-down menu
  - filter the table using the **Rationale** drop-down menu to show only the components that have one of the following conditions:

**Not Healthy**—Displays components whose status is not healthy as defined on the Define Component Health page under the **Settings** tab.

**Not Checked In**—Displays components that have not “checked in” with Infrastructure Status Monitor within the specified time as defined on the Set Display Preferences page on the **Settings** tab.

**All**—Displays all components of any status or rationale.

- click the **Details** icon to display detailed status, attributes, and metrics, including the group attributes that define the health of the component as specified on the Define Component Health page.
- **SNMP Alerts**—Contains a table of SNMP alerts for the host. You can click the **Details** icon for a host name to display the Health Status page that contains detailed status, attributes, and metrics, including the group attributes that define the health of the component. For more information, see “Health Status page” on page 216.

## Proxy tab

The Proxy tab page displays the following sections:

- **Overview**—Contains a color-coded pie chart for the proxies in your environment that indicates the status for each host.
- **Component Details**—Contains a table that displays a row for each machine hosting a proxy along with its **Health** status and **Status Updated Time**. From this table you can
  - filter the table to show only a particular proxy type (All, Proxy, Reverse Proxy, or Secure Reverse Proxy) using the **Component** drop-down menu
  - filter the table to show only the components with a particular status using the **Status** drop-down menu
  - filter the table using the **Rationale** drop-down menu to show only the components that have one of the following conditions:

**Not Healthy**—Displays components whose status is not healthy as defined on the Define Component Health page under the **Settings** tab.

**Not Checked In**—Displays components that have not “checked in” with Infrastructure Status Monitor within the specified time as defined on the Set Display Preferences page on the **Settings** tab.

All—Displays all tuners of any status or rationale.

- click the Details icon to display the Health Status page that contains detailed status, attributes, and metrics, including the group attributes that define the health of the component. For more information, see “Health Status page” on page 216.

## Client tab

The Client tab page displays information about the health of the client and the tuner running on the client. The page contains the following sections:

- **Client Overview**—Contains a color-coded pie chart for client that indicates the overall status of the tuners in your environment.
- **Not Checked-In Status**—Contains a color-coded pie chart that displays the “Not Checked-In” status of the client tuners as defined on the Set Display Preferences page on the **Settings** tab.
- **Component Details**—Contains a table that displays a row for each machine hosting a tuner along with its **Health** status, the **Machine Status**, **Tuner Status**, and **Status Updated Time**. By default, this table shows client tuners that are not healthy. From this table you can
  - search for one or more tuners using the **Search** field and clicking **Go**. You can type the first few letters of a host name to search for tuner hosts that begin with those letters. For example, searching for “v” will display all hosts that begin with the letter “v.” You can also use an asterisk as a wildcard to replace one or more characters. For example, searching for “\*v\*” will display all tuner hosts that have the letter “v” in the host name.
  - check the connectivity of a machine hosting the tuner and the tuner itself by selecting its row in the table and clicking **Check Connectivity**. You can check the connectivity of multiple machines and tuners by holding down the **Ctrl** key and selecting more rows.
  - filter the table to show only the clients with a particular status using the **Status** drop-down menu.
  - filter the table to show only the clients from a particular site using the **Site Name** drop-down menu. This feature only displays if you have configured a subnet-base repeater policy. Clients without a site name are listed under the N/A category.

- filter the table using the **Rationale** drop-down menu to show only the components that have one of the following conditions:

**Not Healthy**—Displays tuners whose status is not healthy as defined on the Define Component Health page under the **Settings** tab. This is the default setting.

**Not Checked In**—Displays tuners that have not “checked in” with the Infrastructure Status Monitor within the specified time as defined on the Set Display Preferences page on the **Settings** tab.

**All**—Displays all tuners of any status or rationale.

- export the table to a .csv file by clicking the **Export to File** button.
- click the **Details** icon to display the Health Status page that contains detailed status, attributes, and metrics, including the group attributes that define the health of the component. For more information, see “[Health Status page](#).”

The ISM dashboard retrieves some of the tuner specific information from the prefs.txt file of each tuner and displays the data in the Client Details section of each tuner. A few tuner property attributes are as follows:

- `marimba.tuner.p2p.peer%`

This tuner property gets set in the prefs.txt file of the MESH-enabled tuner which is configured to send health and monitoring stats report. The value of this property is calculated based on the p2p.peerpc channel property and is captured from the last channel or package subscribe or update operation through MESH. This property value represents the total percentage of file downloaded through peer tuners.

- `marimba.tuner.p2p.tx%`

This tuner property gets set in the prefs.txt file of the MESH-enabled tuner which is configured to send health and monitoring stats report. The value of this property is calculated based on the p2p.peerpc channel property and is captured from the last channel or package subscribe or update operation through MESH. The value for this property represents the percentage of total file downloaded from the transmitter and is calculated as the difference between the percentage of total files and the percentage downloaded through peer tuners.

- **marimba.tuner.memusage%**

This tuner property gets set in the prefs.txt file of the tuner and represents the percentage of maximum allocated JVM memory to a tuner in a machine.

## CMS tab

The CMS tab page displays the following sections:

- **Overview**—Contains a color-coded pie chart for the CMS hosts in your environment that indicates the status for each host.
- **Component Details**—Contains a table that displays a row for each machine hosting a CMS along with its Health status and Status Updated Time. From this table you can
  - filter the table to show only the components with a particular status using the Status drop-down menu
  - filter the table using the Rationale drop-down menu to show only the components that have one of the following conditions:
    - Not Healthy**—Displays components whose status is not healthy as defined on the Define Component Health page under the **Settings** tab.
    - Not Checked In**—Displays components that have not “checked in” with the Infrastructure Status Monitor within the specified time as defined on the Set Display Preferences page on the **Settings** tab.
    - All**—Displays all CMS machines of any status or rationale.
- click the Details icon to display the Health Status page that contains detailed status, attributes, and metrics, including the group attributes that define the health of the component. For more information, see “Health Status page.”
- **SNMP Alerts**—Contains a table of PET (Platform Event Trap) alerts for the CMS host. This information only appears for vPro-enabled CMS hosts. You can click the Details icon for a host name to display the Health Status page that contains detailed status, attributes, and metrics, including the group attributes that define the health of the component. For more information, see “Health Status page.”

## Health Status page

When you click the Details icon for a host (of any component type) from the Component Details page, the Health Status page is displayed. This page contains the following sections:

- **Health Status**—Displays the connectivity status of the component (checked in or not checked in).
- **Group Summary**—Displays a table that contains the status of the group attributes that define the health of the component as specified on the Define Component Health page under the **Settings** tab. The table displays the warning and critical thresholds that you have set along with the actual (current) value. When you click a group name, the content of the **Attributes Summary** table changes to include only attributes that are related to the group name that you clicked.
- **Attributes Summary**—Displays a table that contains attributes for the host that vary depending on the component type. If you click a group name in the **Group Summary** table, the content of the **Attributes Summary** table changes to include only attributes that are related to the group name that you clicked. You can return to the full list of attributes by clicking the **Show All** link that displays at the top right of the table.
- You can change the content of the **Attributes Summary** table by clicking a group name in the **Group Summary** table.
- **Machine Details** link—Click to display the Machine Details page for the host. Machine detail information is only available if the scan report is in the inventory schema.
- **Administer Transmitter**, **Administer Proxy**, or **Administer Tuner** link—Click to launch Transmitter Administration, Proxy Administration, or Tuner Administration, depending on the host’s component type.
- **Audit Log** link—Click to display the Audit Log page. The **Target** field contains the name of the host that you were examining.
- **Launch vPro Console** link—Click to launch the vPro Console. This feature is only available for vPro-enabled machines that have been configured as described in “Configuring vPro settings” on page 222.

## Creating repeater groups and viewing group statistics

On the Repeater tab underneath the pie chart, click the **Repeater Group Statistics** link to display a table of repeater statistics. The Repeater Group Statistics page displays a group of repeater hosts in a table that contains:

- the Load on the repeater
- the Average Processing Time for the repeater
- the number of Bytes Sent by the repeater
- the number of Bytes Received by the repeater

The table displays only the repeaters that are in the selected group.

### ► To create a repeater group and view statistics for the group

- 1 From the Repeater Group Statistics page, click the **Manage Groups** link on the far right side above the table, to display the Manage Groups page.
- 2 Click the **New Group** button.
- 3 Type a name for the group in the field provided.
- 4 (optional) Enter a description for the group.

This description is displayed on under the Repeater Group Statistics page for the selected group.

- 5 From the All Repeaters list, highlight one or more repeater hosts for the group you want to create and click the > button to move them to the Selected Repeaters list.

You can select all repeaters on the left by clicking the >> button. You can select multiple repeaters by using the shift or control key while clicking.

If the **All Repeaters** list is long, you can search for a repeater using the **Search** field and clicking **Go**. You can use an asterisk as a wildcard to replace one or more characters. For example, searching for “t\*” will display all repeaters that begin with the letter “t.”

- 6 Click **Save** to create the group.
- 7 Click **Return to Group Statistics** at the top of the page to return to the Group Statistics page.
- 8 Using the **View Group** drop-down menu, select the group you created.

The table contains statistics for the repeater hosts in the group you selected.

## Viewing audit log entries

You can display the Audit Log page by clicking the **Audit Log** link on the right side of the Dashboard page or the right side of the Health Status page for any component.

The Audit Log page displays audit log entries from the host of each component. The audit log basically displays the user name that performed an action, the action that was preformed, and the time the action was performed. For more information, see “Tuner audit logs” on page 392. For more information, see “Tuner audit logs” on page 392. The tuner workspace directory also contains an audit log that is populated with messages that contain the “AUDIT” severity level from the tuner and channels. Audit logs are named by the order in which they are created. For example, the first audit log file is named `audit-1.log`, the second one `audit-2.log`, and so on.

## Filtering log entries

By default, the Audit Log tab displays 25 of the most recent entries, but you can filter/search to narrow the results by using one or more of the following search criteria fields and clicking **Search**:

- **User**—Enter one or more, comma separated, user names to filter the results to only the specified users.
- **Log Id**—Type a log id to filter the results to only the specified log id.
- **Source**—Select the source component that initiated the change from the drop-down menu to filter the results to only the specified component.
- **Date From and To**—Click to select a date range to display entries that occurred during the specified time period.
- **Target**—Type a target machine name on which the change occurred filter the results to only the specified target machine.
- **Description**—Type a partial description using wildcards to filter the results. For example, type `*invdb*` to display entries relate to the Marimba database. For SQL Server, the default database name is `invdb`, unless you edited the necessary database setup batch scripts to change this value during the install, reinstall, or upgrade process.

Leaving a search field blank searches for all or any entries. You can use many or all of the search fields in the same search. For example, if you want to check to see if user smith made changes that affect the Marimba database (For SQL Server, the default database name is invdb, unless you edited the necessary database setup batch scripts to change this value during the install, reinstall, or upgrade process.), you could search with the following field entries:

- **User:** `smith`
- **Source:** `Schema Manager`
- **Description:** `*Marimba database name*`

## Using the audit log table controls

After your search displays data in the audit log table, you can use the following controls to sort of page through the data:

- number of rows to display—Click the Display drop-down menu to display 25, 50, 75, or 100 rows.
- column sorting—Click the heading of any column to perform an ascending or descending sort.
- paging—Click the following controls to page through the data:
  - <<—Jump to the first entry.
  - >>—Jump to the last entry.
  - <—Jump to the previous page.
  - >—Jump to the next page.
  - number—Jump to a specific page.

## Configuring settings (Setting tab)

The Setting page displays links to the following configuration options:

- “Configuring the logging plug-in” on page 222
- “Defining component health” on page 222
- “Configuring email notifications” on page 223
- “Setting display preferences” on page 225

## Configuring the logging plug-in

### ► To configure the logging plug-in

- 1 From the Settings tab, click the **Plugin** tab.
- 2 Enter the logging plug-in URL.
- 3 Enter the Subscribe User Name and Password if subscribe permissions are set on the master transmitter.
- 4 Click Save.

If you receive the following error, restart the CMS channel:

Plugin Access has been Failed, check whether the subscribe user name and password are correct or not.

## Defining component health

You can configure the attributes and metrics used by the Infrastructure Status Monitor to determine the health of a server or client machine.

### ► To define component health

- 1 From the **Settings** tab, click the **Health** tab.
- 2 From the **Select Component** drop-down menu, choose a component type.
- 3 In the table, set the attributes for each group name to define the warning and critical states.

The available attributes differ depending on the selected component type (Master, Mirror, Repeater, and Proxy, Reverse Proxy, Secure Reverse Proxy, CMS, or Client).

- 4 Click the Remove button (trash can) to remove a group attribute from the component's health definition.

If you remove a group attribute, the **Add Group** drop-down menu is displayed. You can use this drop-down menu to add back deleted group attributes.

- 5 Click Save.
- 6 Click Publish to publish the new settings which restarts the plug-in.

When you change how the health of an infrastructure component is defined and publish it to the plug-in, the changes are reflected in the Infrastructure Status Monitor only when the plug-in sends the new health data at the specified schedule. Until the new data is sent, the group status and component status are out of sync.

## Configuring email notifications

You can set up email reports that contain information about alerts displayed in the Infrastructure Status Monitor.

### ► To configure email notifications

- 1 Configure CMS email notifications from **Applications > Console > System Settings > General tab > E-mail Notifications** link. For more information, see “Configuring email notifications” on page 85. Applications that run on top of CMS, such as Report Center, can send email notifications with attachments after certain actions or events.
- 2 To enable email notifications, you must configure these settings in the CMS console. You can also set the user name and password needed if your SMTP server requires authentication.
- 3 For more information, see “Configuring email notifications” on page 85.
- 4 From the **Settings** tab, click the **Preferences** tab.
- 5 In the Email Notification Settings section, enter data in the following fields:
  - **Sender Name**—Type the name that you want to display as the sender’s name in the email.
  - **Sender Address**—Type the email address of the person sending the report.
  - **SMTP Host**—Displays the SMTP mail host that you specified in step 1 under **System Settings > General tab > E-mail Notifications**. If this field is blank, go to step 1.
- 6 Click **Save**.
- 7 Click the **Email Notification** tab.
- 8 Click the **Manage Email Notification** link on the right side of the page.
- 9 Click **New Notification**.
- 10 Enter a **Notification Name**.

- 11 Select the **Alert Types** that you want to include in the email report.
- 12 Select the **Report Type**, either HTML or CSV.
- 13 Enter the email address of the report recipient in the **Send To** field.
- 14 Select a scheduled time to send the email report.
- 15 Click **Save**.

The configured email report is sent to the specified email address according to the configured schedule.

- 16 Click **Return to Email Notifications**. to view the list of configured email notifications.

## Configuring vPro settings

By specifying Intel AMT vPro settings in the Infrastructure Status Monitor, you can view vPro Platform Event Trap (PET) information from all vPro-enabled endpoints in the SNMP Alerts table of the Infrastructure Status Monitor Dashboard.

### Before you begin

You must configure the following on every endpoint that you want to monitor:

- Infrastructure Status Monitor settings—Configure the **Advanced > ISM** tab in a profile or in Tuner Administration.
- vPro settings—Configure the **Advanced >vPro** tab in a profile or in Tuner Administration.

### ► To configure vPro settings for the Infrastructure Status Monitor

- 1 From the Infrastructure Status Monitor, click the **Settings** and **vPro** tabs to display the vPro Configuration page.
- 2 Towards the bottom of the page under **Platform Even Alert Subscription Settings** in **SNMP Manager Host**, type the host name for the transmitter that is running the logging service. This must match the server name specified in ISM tab for the profile or in Tuner Administration, and the port number must be 162.
- 3 Click **Save**.

The configuration settings are saved in the database. These settings are used by the Infrastructure Status Monitor according to the AMT Watchdog Creation schedule, usually once a day.

To start receiving vPro PET trap information quickly, you can restart the Infrastructure Status Monitor.

## Configuring vPro agent watchdog settings for Infrastructure Status Monitor

You can control the creation of vPro agent watchdog in the **vPro Configuration** tab of the **Infrastructure Status Monitor (ISM)** settings page. To allow ISM perform the task of creating vPro agent watchdogs, select the **Create vProAgent Watchdog/Platform Event Alert (PET) Subscription** check box.

---

Note: By default, ISM does not perform the task of vPro watchdog creation for vPro-enabled computers.

---

## Configuring the maximum number of concurrent threads to handle vPro agent watchdog settings in ISM

If you have selected the **Create vProAgent Watchdog/Platform Event Alert (PET) Subscription** check box to perform the task of vPro agent watchdog creation, then you can control the maximum number of active threads used to create vPro Watchdog and Platform Event Alert (PET). To configure the number of active threads, modify the value of **Max Concurrent Threads** in the **Preferences** tab of the **Settings** page of ISM. For example, if you specify 10 in the **Max Concurrent Threads** box, then ISM uses a maximum of 10 threads simultaneously to create vPro Watchdog and Platform Event Alert (PET). The default value of Max Concurrent Threads parameter is 20.

## Setting display preferences

### ► To set display preferences

- 1 From the **Settings** tab, click the **Preferences** tab.
- 2 Review the following options and set your preferences:

- **Server Status refresh interval**—sets the refresh rate for server component information in minutes. The default is one minute.
- **Client Status refresh interval**—sets the refresh rate for client information in minutes. The default is 15 minutes.
- **SNMP Alert page refresh interval**—sets the refresh rate of the SNMP Alert page in minutes. The default is one minute.
- **Multi page display**—sets the numbers of items that can appear on a page. The default is 10 items per page.
- **Show component status in bar chart**—determines which components are displayed in the Server Component Status bar chart.
- **Not Checked In duration for server components**—sets the length of time during which component hosts should have “checked in” or sent data to the Infrastructure Status Monitor. Component hosts that have not communicated with the Infrastructure Status Monitor within the specified Warning or Critical time frames are marked as “Not Checked In.”

For servers that have exceeded the warning range, the Health column in the Component Details table is marked with a warning icon.

For servers that have exceeded the critical range, the Health column in the Component Details table is marked with a critical icon.

- **Not Checked In duration for client components**—sets the length of time during which a client’s tuner should have “checked in” or sent data to the Infrastructure Status Monitor. Tuners that have not communicated with the Infrastructure Status Monitor within the specified Warning or Critical time frames are marked as “Not Checked In.”

For clients that have exceeded the warning range, the Health column in the Component Details table is marked with a warning icon.

For clients that have exceeded the critical range, the Health column in the Component Details table is marked with a critical icon.

# Using a custom channel to collect and display customized stats attributes in ISM

The ISM dashboard displays stats attributes, however you can also collect customized stats attributes. If you want to collect customized stats attributes from the endpoints and display the stats in the ISM dashboard, you must build a custom channel and use it. You can build a custom channel for SMCA using Java IDE. You can use the custom channel to collect the required attributes from every endpoint and display them in the ISM dashboard.

---

Note: For more information on how to create or build a custom channel for SMCA, see Marimba Advanced Programming Guide.

---

## Overview of implementing the custom channel

To implement a custom channel to collect and display stats attributes, you must perform the following steps:

- 1 Write the code for a Java class file to implement the functionality required in the custom channel
- 2 Build a custom channel using the Java class file
- 3 Publish the custom channel
- 4 Configure the database
- 5 Configure the tuner to send the custom stats attributes

## Prerequisites

Prior to creating a custom channel, you must create a java class file. To create or modify a custom channel, you can use a Java IDE to modify or write the Java code.

To implement the custom channel, ensure that the following tools are installed:

- An text editor to write the Java code
- A fully interactive tuner with the following channels:
  - Publisher

- Channel Copier
- Transmitter
- Tool or script to send SNMP alerts

## Creating the custom channel

You use the custom channel to collect the required stats attributes from the endpoints and send them to the database. The custom channel should use the following classes to send the stats to the database.

- ICustomStatsProvider.java
- IStatsAttribute.java
- IStatsService.java

### The ICustomStatsProvider.java class

This class provides the following API:

API: int getCustomComponentType()

Usage: Use to indicate the ISM component with which the custom stats provider is associated.

Return value: has to be one of the following:

- CUSTOM\_TX
- CUSTOM\_PROXY
- CUSTOM\_CLIENT
- CUSTOM\_CMS

### The IStatsAttribute.java class

This class provides the following APIs:

■ String statsAttribute();

Usage: Returns the status attribute mapping. For example, 1.3.2.3.1.

Return value: : A string which represents the status attribute mapping.

■ Object statsValue();

Usage: returns the value of the attribute. It should be one of the following supported data types:

- Integer
- Long
- Float
- Double
- String

Return value: The value of the status attribute represented by one of the supported data types.

## The IStatsService.java class

This class contains the following APIs:

- void registerCustomStatsProvider(ICustomStatsProvider provider);

A custom stats channel uses this API to register itself with the service.

Return value: null

- void unRegisterCustomStatsProvider(ICustomStatsProvider provider);

A custom stats channel uses this API to un-register itself from the service.

Return value: null

## Sample code for using the APIs

The following sample code shows how to use the preceding APIs:

```
import com.marimba.intf.application.*;
import com.marimba.intf.stats.*;
import com.marimba.intf.util.*;

public class StatsChannelTuner implements IApplication {
    IApplicationContext context;
    MyStatsProvider provider;
    IStatsService service;
    IConfig config;
    IConfig tunerPropertiesConfig;

    public void notify(Object sender, int msg, Object arg) {
        switch(msg) {
            case APP_INIT:
                context = (IApplicationContext)arg;
                service = (IStatsService)context.getFeature("ism");
                config = (IConfig)context.getFeature("config");
                service.registerCustomStatsProvider(provider);
                String prot =
                    config.getProperty("marimba.tuner.service.protect");
```

```
        String mig =
config.getProperty("marimba.tuner.session.affintiy");
        provider = new
MyStatsProvider(prot,mig,context.getChannelURL().toString());

        if(provider != null) {
service.registerCustomStatsProvider(provider);
}
        break;
case APP_NOTIFY:
        break;
case APP_STOP:
        service.unregisterCustomStatsProvider(provider);
        System.out.println("Successfully unregistered the Stats
Provider");
        provider = null;
        break;
}
}
class MyStatsAttribute implements IStatsAttribute {
    public String id;
    public Object val;
    public MyStatsAttribute() {
    }
    public String statsAttribute() {
        return id;
    }
    public Object statsValue() {
        return val;
    }
}

class MyStatsProvider implements ICustomStatsProvider {
    String channelURL;
    String protection;
    String migration;
    public MyStatsProvider(String protection, String migration, String
channelURL) {
        this.channelURL = channelURL;
        System.out.println("Channel URL: " +channelURL);
        this.migration = migration;
        System.out.println("Property value: " +migration);
        this.protection = protection;
        System.out.println("Protection value: " +protection);
    }

    public int getCustomComponentType() {
        return CUSTOM_CLIENT;
    }

    public IStatsAttribute[] getStats() {
        MyStatsAttribute t1,t2;
        t1 = new MyStatsAttribute(); t2 = new MyStatsAttribute();
```

```

t1.id = "11.6.1";
if ( migration != null && migration.equalsIgnoreCase("true"))
t1.val = "1";
else
t1.val = "0";
t2.id = "11.6.2";
//The t1.id variable contains the stats id. Every stats attribute is
associated with an id and a value. The custom channel sends the
values of both id and val for each stat attribute.
// Important note: When you specify the values for t1.id, use only
values starting from 11.0.0.
if (protection != null && protection.equalsIgnoreCase("true"))
t2.val = "1";
else
t2.val = "0";

IStatsAttribute[] arr = new IStatsAttribute[4];
arr[0] = t1;
arr[1] = t2;
// The array stores the stat attribute values.
System.out.println("The stats array values:"+arr[0] +arr[1]);
return arr;
}

public String getChannelURL() {
    return this.channelURL;
}
}
}

```

### A note about the logic implemented in the code

- The sample code checks whether session migration and tuner protection is enabled on the endpoint tuner. If the session migration and tuner protection properties are enabled, the code sends the number “1” as the stats value (not a Boolean). If the properties are not enabled, the code sends the number “0”. The explanation of code is as follows:
- The import com.marimba.intf.stats.\* jar file consists of all the APIs that enable the channel to send stats.
- The first two lines of the following code capture the property values of session affinity and tuner protection in two strings.

```

String prot = config.getProperty("marimba.tuner.service.protect");
String mig = config.getProperty("marimba.tuner.session.affinity");
provider = new
MyStatsProvider(prot,mig,context.getChannelURL().toString());

```

The MyStatsProvider class is created and used to send the stats reports. The provider object is created for this class and the values of prot, mig and the channel URL are passed to this object.

```
if(provider != null) {  
    service.registerCustomStatsProvider(provider);  
}  
break;
```

Once the object is created, the code registers this object as CustomStatsProvider and indicates to the tuner that this object is used to send the stats attributes.

- The service.unRegisterCustomStatsProvider(provider); command unregisters the customs stats provider API.
- Every stats attribute is associated with an id and a value. The custom channel sends the values of both id and val for each stat attribute. The t1.id variable contains the stats id and the t1.val variable contains the value of the stats id.

```
public IStatsAttribute[] getStats() {  
    MyStatsAttribute t1,t2;  
    t1 = new MyStatsAttribute();  
    t1.id = "11.6.1";  
    if ( migration != null && migration.equalsIgnoreCase("true"))  
        t1.val = "1";  
    else  
        t1.val = "0";
```

---

Note: When you specify the value of the stats id, use only values starting from 11.0.0. For example, t1.id = 11.6.1. Values up to 10.x.x are reserved for SMCA.

---

## Publishing the custom channel

### ► To publish the custom channel:

- 1 Start the Publisher channel.
- 2 In the left side pane, click Tasks.
- 3 In the Create a New Channel section, click New Channel.

The Publisher channel displays the Choose Directory dialog box.

- 4 Navigate to the directory where the .java file of the custom channel is stored.
  - 5 Click OK.
  - 6 In the **Create a New Destination** section, click **New Destination**.
  - 7 In the **Choose Channel** box, specify the folder where the .java file of the custom channel is located.
  - 8 In the Target URL Information section, select the URL of the target transmitter.
  - 9 In the **Channel URL** box, type the URL of the channel.
  - 10 Click OK.
  - 11 In the Publisher, click **Perform Operation**.
  - 12 In the home page of the Publisher, right click on the custom ISM channel and click **Edit Channel**.
  - 13 Specify the following details:
    - Title: The title of the channel.
    - Type: Application
    - MIME-Type: application/x-castanet-channel
    - File Extension: channel
    - Classpath: ':'
  - 14 Click **Application Tab**.
  - 15 In the **Main Class** box, type the name of the main class of the custom channel.
  - 16 Click **Apply**.
  - 17 Click OK.
- Publish the channel.
- The custom channel is published on the destination transmitter.

## Configuring the database

Before you can configure the database, ensure that you install the latest ISM schema.

Configuring the database comprises of running several scripts to:

- Create a custom table

- Grant permission to hmadmin and hmuser
- Add entries in the mapping table
- Recreate view with custom attributes
- Grant permission to hmuser

► **To configure the database, run the following scripts:**

When you run scripts for various components like tuner and transmitter, it is recommended to use table names as specified in the following:

Table 14-1: Recommended table names

Component	Recommended table name
Tuner	hm_custom_tuner_stats
Transmitter	hm_custom_tx_stats
Proxy	hm_custom_proxy_stats
CMS	hm_custom_cms_stats

- 1 To create a table to store custom tuner stats attributes, run the following script:

```
create table hm_custom_tuner_stats(  
    machine_id varchar(128) not null,  
    tuner_id numeric(20, 0) not null,  
    type_id smallint not null,  
    last_modified_time datetime,  
    id int not null identity,  
    custom_col1 varchar(100),  
    custom_col2 varchar(100))
```

The custom\_col1 and custom\_col2 data columns are used to store the collected stats attributes data. You can specify any name for the custom\_col1 and custom\_col2 data columns. You can specify any number of columns or as required to send the custom stats attributes.

Note: The hm\_custom\_tuner\_stats table has two entries: one entry inserts stats for '11.6.1' while the other for '11.6.2'. You must define each column for each stats entry. While defining the columns for each stats, you can specify any value such as an int.

- 2 To grant permission to the hmadmin and hmuser users, run the following script:

```
GRANT SELECT, INSERT, UPDATE, DELETE ON hm_custom_tuner_stats TO
hmadmin
```

```
GRANT SELECT, INSERT, UPDATE, DELETE ON hm_custom_tuner_stats TO
hmuser
```

- 3 To add an entry in the mapping table, run the following script:

```
INSERT INTO hm_lookup
(node_id,node_number,node_desc,type_name,tablename,columnname,datatype,can_be_formula,compulsory,unit,post_processing)VALUES(1101,
'11.6.1','Mig','tuner','hm_custom_tuner_stats','custom_col1','varchar',1,NULL,NULL,NULL);

INSERT INTO hm_lookup
(node_id,node_number,node_desc,type_name,tablename,columnname,datatype,can_be_formula,compulsory,unit,post_processing)VALUES(1102,
'11.6.2','Prot','tuner','hm_custom_tuner_stats','custom_col2','varchar',1,NULL,NULL,NULL);
```

Note: You can use the following guidelines while mapping entries:

Table 14-2: Map entries

<b>Map entry</b>	<b>Description</b>
node_id	Any number starting from 1000. Marimba uses values in the 0 to 1000 range.
node_number	Any value starting from 11.x.x. Marimba uses the 1.x.x to 10.x.x. Ensure that the value of this entry is the same as the value of the stats which we defined in the custom channel. For example, in this scenario, it is 11.6.1 .
node_desc	Any string. This string is displayed in the Formulae Builder description of the Summary Details page of the ISM dashboard.
type_name	Specifies for which component the stats is being defined. For example, you can define it for any of the following: <ul style="list-style-type: none"> <li>■ ‘tuner’</li> <li>■ ‘transmitter’</li> <li>■ ‘proxy’</li> <li>■ ‘cms’</li> </ul>

Map entry	Description
Tablename	Specifies the name of the table in which the custom stats are inserted. For example, hm_custom_tuner_stats. You can specify any name, but it is recommended to start the name of the table with hm _custom_.
columnname	Specifies the name of the column in which the value of stats id are inserted. For example, custom_col1.
datatype	Specifies the data type for the column. For example, int or boolean. <b>Note:</b> You should specify the same datatype which you have used while declaring t1.value variable in the custom channel code.
can_be_formula	This map entry specifies whether the attribute you send should be included for defining any formula in the ISM Dashboard. If you specify 1, you can define a formula. If you specify 0, you cannot define a formula. For example, can_be_formula 0.
compulsory	Specifies whether the endpoint should mandatorily send the information.
unit	Displays the unit of the custom stats in the ISM dashboard. For example, %.
post-processing	Specifies the value of the custom stats after processing.

#### 4 Recreate the view with custom attributes

To display the stats attributes in ISM Dashboard, you have to add views for the new tables which you have added.

Add the following new columns:

```
dbo.hm_custom_tuner_stats.custom_col1,
dbo.hm_custom_tuner_stats.custom_col2
```

To recreate the views, run the following SQL script:

```
drop view hmv_client_tuner_summary
create view hmv_client_tuner_summary(
SELECT dbo.hm_machine.machine_id, dbo.hm_machine.tuner_id,
dbo.hm_machine.mac_host, dbo.hm_machine.mac_ipaddress,
dbo.hm_machine.network_ip, dbo.hm_machine.tuner_port,
dbo.hm_machine.tuner_version, dbo.hm_machine.tuner_release_date,
dbo.hm_machine.vm_vendor, dbo.hm_machine.vm_heap_total,
dbo.hm_machine.vm_version, dbo.hm_machine.vm_arguments,
```

```

dbo.hm_machine.vm_thread_count, dbo.hm_machine.vm_heap_available,
dbo.hm_machine.total_diskspace,
dbo.hm_machine.available_diskspace,
dbo.hm_machine.os_name, dbo.hm_machine.os_version,
dbo.hm_machine.os_architecture, dbo.hm_tuner_stats.type_id,
dbo.hm_tuner_stats.health_id, dbo.hm_tuner_stats.up_since,
dbo.hm_tuner_stats.stats_last_changed,
dbo.hm_tuner_stats.is_ssl_enabled,
dbo.hm_tuner.p2p_peerpercent, dbo.hm_tuner.p2p_txpercent,
dbo.hm_tuner.memory_usage, dbo.hm_tuner.p2p_enabled,
dbo.hm_tuner_stats.available_volume_size,
dbo.hm_tuner.total_volume_size,
dbo.hm_custom_tuner_stats.custom_col1,
dbo.hm_custom_tuner_stats.custom_col2
FROM dbo.hm_machine INNER JOIN
dbo.hm_custom_tuner_stats ON dbo.hm_machine.tuner_id =
dbo.hm_custom_tuner_stats.tuner_id INNER JOIN
dbo.hm_tuner_stats ON dbo.hm_machine.tuner_id =
dbo.hm_tuner_stats.tuner_id AND dbo.hm_tuner_stats.isclient = 1
INNER JOIN
dbo.hm_tuner ON dbo.hm_machine.tuner_id = dbo.hm_tuner.tuner_id
)

```

If you are using the Oracle database, use the following script:

```

create or replace view hmv_client_tuner_summary
AS (
SELECT hm_machine.machine_id, hm_machine.tuner_id,
hm_machine.mac_host, hm_machine.mac_ipaddress,
hm_machine.network_ip, hm_machine.tuner_port,
hm_machine.tuner_version, hm_machine.tuner_release_date,
hm_machine.vm_vendor, hm_machine.vm_heap_total,
hm_machine.vm_version, hm_machine.vm_arguments,
hm_machine.vm_thread_count, hm_machine.vm_heap_available,
hm_machine.total_diskspace, hm_machine.available_diskspace,
hm_machine.os_name, hm_machine.os_version,
hm_machine.os_architecture, hm_tuner_stats.type_id,
hm_tuner_stats.health_id, hm_tuner_stats.up_since,
hm_tuner_stats.stats_last_changed, hm_tuner_stats.is_ssl_enabled,

```

```
hm_tuner.p2p_peerpercent, hm_tuner.p2p_txpercent,  
hm_tuner.memory_usage, hm_tuner.p2p_enabled,  
hm_tuner_stats.available_volume_size, hm_tuner.total_volume_size,  
hm_custom_tuner_stats.custom_col1,  
hm_custom_tuner_stats.custom_col2  
FROM hm_machine INNER JOIN  
hm_custom_tuner_stats ON hm_machine.tuner_id =  
hm_custom_tuner_stats.tuner_id INNER JOIN  
hm_tuner_stats ON hm_machine.tuner_id = hm_tuner_stats.tuner_id  
AND hm_tuner_stats.isclient = 1 INNER JOIN  
hm_tuner ON hm_machine.tuner_id = hm_tuner.tuner_id  
)
```

**Note:**

- If you are adding a new attributes in tuner, then update hmv\_client\_tuner\_summary.
- If you are adding new attributes in Transmitter, then update hmv\_tx\_summary.
- If you are adding new attributes in Proxy, then update hmv\_proxy\_summary.
- If you are adding new attributes in CMS, then update hmv\_cms\_summary.

- 5 To grant permission to the hmuser user, run the following script:

```
GRANT SELECT, INSERT, UPDATE, DELETE ON  
hmv_client_tuner_summary TO hmuser
```

## Configuring the tuner to send custom stats data

To configure the tuner to send the custom stats data:

- 1 After you have configured the settings for the tuner to report the stats to the ISM console, add the following properties for each of the following components in their related properties:

For a client, add the marimba.tuner.hm.customclient.url=<custom channel URL> property.

For a transmitter add the marimba.tuner.hm.customtx.url=<custom channel URL> property.

For a proxy, add the marimba.tuner.hm.customproxy.url=<custom channel URL> property.

For a tuner, add the marimba.tuner.hm.customcms.url=<custom channel URL> property.

You can add these properties using the profile, policy or through manual configuration in the Tuner Administrator.

---

Note: Once the database and the tuner are configured, the tuner automatically sends the custom stats data according to schedule. The stats report contains the custom stats data. You can view the custom stats in the Attributes Summary table component of the ISM dashboard.

---

---

Note: If you want the custom stats to be part of the health calculations in the Health tab, then proceed with step 2.

---

- 2 In the **Health** tab of the ISM Dashboard, use the Formula Builder to specify the formula required for the custom channel.

### Specifying the custom formula

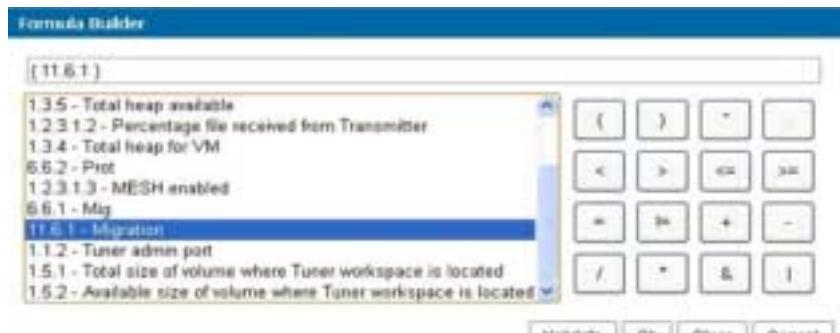
#### ► To specify the custom formula:

- 1 In the ISM home page, navigate to **Settings => Define Component Health => Manage Groups**.
- 2 Select **New Group**.
- 3 Select **Component Type**.
- 4 In the **Group Name** text box, type the name of the group.
- 5 In the **Description** text box, type the description.
- 6 In the **Data Type** list, select the required data type.
- 7 Click **Formula Builder** to select a stats attribute.

The Formula Builder window appears.



In the Formula Builder window, you can create formulas using the built-in attributes like 1.3.5 and you can also use custom values.



For example, you can type  $(1.3.5)-(1.3.4)$ .

- 8 Click Validate to check if the formula is a valid formula.

You can view the result of the validation in the lower left corner of the **Formula Builder** dialog box.

- 9 Click OK to save the formula.

**OR**

Click Cancel if you do not want to save the formula.

- 10 In the **Condition** list, select the condition which is required to calculate the health.
- 11 In the **Warning** text box, type the value for which the condition is evaluated as a warning status.

- 
- 12 In the **Critical** text box, type the value for which the condition is evaluated as critical.

- 13 Click **Save**.

ISM creates the new group.

- 14 In the **Part of formula** list, select **Yes** if you want this formula to be part of the formula group. Select **No** if you do not want the formula to be a part of the formula group.

- 15 Click **Return to Define Component Health**.

- 16 In **Select Component** list, select the required component.

In the **Part of formula** list, if you have selected **Yes**, then you can view the group name in the Group Name column of the Define Component Health page.

If you have selected **No**, then you cannot view the group in the Group Name column of the Define Component Health page. However, you can add the group in the Define Component Health page. To add the group, in the Define Component Health page, select the group from the **Add group** list and click **Save**.

In the **Add Group** list you can view the name of the group you have created.

- 17 Click on **Save**.

ISM saves the new formula.

---

Note: Once you save the groups, you have to publish them. Only after the groups are published, the new formula is used in the health calculations.

---

## Exporting and importing groups

If you need to make many changes in groups data, you can use the Export Groups or Import Groups feature to export groups data into a CSV file and then modify the data. After you have performed the required modifications, you can import the CSV file. It is always recommended to export the data to a CSV file, make modifications to the data, and import the CSV file.

### ► **To export and import the groups data into a CSV file:**

- 1 In the ISM page, click **Settings** tab.

2 Click Health tab.

You can view the Manage Formula Groups page.

3 Click Export Groups, and save the CSV file in a local directory.

4 Make the required modifications on the data in the CSV file.

5 To import the modified CSV file, click Import Groups and select the required CSV file.

---

Note: Only users belonging to the admin or primary user group can export or import the groups data.

---

For predefined groups, you cannot modify the following fields:

- Groupname
- Description
- Datatype
- Formula

---

Note: Even if you make changes to the preceding fields related to the predefined groups in the .csv file, after you upload the CSV file, ISM does not capture the modifications performed on the specified fields for the predefined groups.

---

## SNMP alerts

The tuner has an inbuilt SNMP Agent which sends the required SNMP alerts to the SNMP Manager which is the transmitter.

---

Note: You can also use any third party tool to send an SNMP alert.

---

The following table describes the parameters used in the alert format:

Table 14-3: Parameters used in the alerts

<b>Attribute name</b>	<b>Value</b>	<b>Description</b>
Trap time	String	A string representation of the timestamp when the trap is sent.
IP address	String	The IP address of the computer from which the trap is sent.
Tuner ID	String	The ID of the tuner.
Trap type	String	A generic string which represents the type of error or event. For example, storage error.
Trap details	String	A string which describes details on the error or event. For example, failure due to storage exception.
Trap mapping	String	A string which has the following format: <stats attribute>=<value>. The <stats attribute> is mapped in the ISM database so that the ISM Console reads this value from the trap and correlates it to the mapped parameter in the database. Note: You must specify the <value> parameter as an integer.
Machine ID	String	A string which represents the machine ID. You can also reuse the tuner ID to represent the machine ID.
Type ID	String	A string which represents the type of transmitter. When a transmitter sends a trap, this parameter indicates the type of transmitter like mirror, repeater, or proxy.

The format of the alert is:

```
<Trap_id_for_time><Time> <Trap_id_for_ipAddress><IP Address>
<Trap_id_for_tunerID><Tuner ID> <Trap_id_for_Type><Trap Type>
<Trap_id_for_Trap_details ><Trap Details>
<Trap_id_for_stats_mapping><Stats_mapping>
<Trap_id_for_machine_id><Machine ID> <Trap_id_for_type_id><Type ID>
```

The following example shows the SNMP alert with the trap id:

```
<1.3.6.1.4.1.1031.101.1.100 ><Time> <1.3.6.1.4.1.1031.101.1.130 ><IP
Address> <1.3.6.1.4.1.1031.101.1.131 ><Tuner ID>
<1.3.6.1.4.1.1031.101.1.132 ><Trap Type> <1.3.6.1.4.1.1031.101.1.110
><Trap Details> <1.3.6.1.4.1.1031.101.1.111 ><traps_mapping>
<1.3.6.1.4.1.1031.101.1.134 ><Machine ID> <1.3.6.1.4.1.1031.101.1.135
><Type ID>
trapgen -d 10.128.136.213:6162 -v 1.3.6.1.4.1.1031.101.1.100 STRING
"Oct 17, 2011 07:05:10 AM" -v 1.3.6.1.4.1.1031.101.1.130 STRING
"10.128.3.187" -v 1.3.6.1.4.1.1031.101.1.131 STRING
"1948317712414235923" -v 1.3.6.1.4.1.1031.101.1.132 STRING "Trap
Type: Storage Error" -v 1.3.6.1.4.1.1031.101.1.110 STRING "Storage
error Occurred on xp-mar183" -v 1.3.6.1.4.1.1031.101.1.111 STRING
"6.6.1 = 1" -v 1.3.6.1.4.1.1031.101.1.134 STRING
"1948317712414235923" -v 1.3.6.1.4.1.1031.101.1.135 STRING "7"
```

**Note:**

You can use:

- <1.3.6.1.4.1.1031.101.1.100 ><format: of time: Oct 17, 2011
07:05:10 AM" to specify the time.
- 1.3.6.1.4.1.1031.101.1.130 to specify the IP address.
- 1.3.6.1.4.1.1031.101.1.131 to specify the Tuner ID from which the alert is
sent.
- 1.3.6.1.4.1.1031.101.1.132 to specify the type of trap. For example,
storage trap.
- 1.3.6.1.4.1.1031.101.1.110 to specify the details of the trap.
- 1.3.6.1.4.1.1031.101.1.111 to specify the trap mapping.
- 1.3.6.1.4.1.1031.101.1.134 to specify the machine ID.
- 1.3.6.1.4.1.1031.101.1.135 to specify the Type ID.

---

Note: The format of the preceding example is specific to the tool used to send SNMP alerts. In this example, the Trapgen tool is used to generate the SNMP alert.

---

## Using scripts to define and send custom SNMP alerts through e-mail notifications

You can run database scripts to define and send custom SNMP alerts through e-mail notifications.

The following script shows an example of the database script:

```
Insert into hm_snmp_lookup values('id','Trap_id','Trap Description',
'Is_Custom')
```

Where:

- The Id parameter must be a number greater than 10.
- The Trap id parameter specifies the OID of the SNMP agent.
- The Trap\_description parameter specifies the name of the trap.
- The Is\_custom parameter specifies whether the SNMP alert is a custom alert. If you specify the value as 1, ISM displays the SNMP alert in the ISM dashboard. The value 1 signifies a custom alert.

Valid values: 0 or 1. The default value is 0.

For example:

```
insert into hm_snmp_lookup values(11,'1.10.02.1.22','Error occurred
in Tuner',1)
```

## Viewing the status of deployed jobs in ISM dashboard and using Report Center query

Once the deployment is completed on the target computer, you can view the following status attributes in ISM dashboard:

- Deployment Name
- Deployment Status
- Last Deployed Date

You can also use the following query in Report Center to view the deployment status:

```
select * from dm_deployment_status_detail
```

If you configure 1.8.3-Deployment Status parameter in Formulae Builder of ISM, then ISM calculates the health of the component based on the Deployment Status parameter. Ensure that you create a new group for using the 1.8.3 Deployment Status parameter in the Formulae Builder.



Section

# III Tuner Administration

Section 3 discusses the following topics:

- “Tuner basics” on page 249
- “Getting started with Tuner Administration” on page 263
- “Package and channel management for a tuner” on page 302
- “General tuner settings” on page 320
- “Tuner security” on page 338
- “Tuner properties” on page 332
- “Tuner security” on page 338
- “Advanced tuner settings” on page 352
- “Tuner background information” on page 361



## Chapter

# 15 Tuner basics

This chapter provides an overview of tuners and describes how you can use Tuner Administrator to manage and configure tuners.

The following topics are provided:

- What is a tuner? (page 250)
- What are channels and packages? (page 250)
- Tuner installation directory (page 251)
- Tuner workspace directory (page 252)
- What is Tuner Administrator? (page 255)
- Administering a tuner (page 256)
- 64-bit Tuner (page 257)
- Marimba over Internet (page 261)

## What is a tuner?

The tuner is the client component that is installed on the endpoints in a Symphony Marimba Client Automation architecture. The tuner lets you manage endpoints through the following features:

- Subscribe to packaged applications so that they are downloaded and installed on endpoints.
- Manage the schedule and manner in which packaged applications and updates are downloaded and installed.
- Provide a platform on which other Symphony Marimba Client Automation products can run.

You can configure tuners depending on how you want to use them in your enterprise. For example, you can configure tuners to have a user interface visible to users, or you can configure tuners to be completely invisible to users.

### Tuner icon behavior

When you right-click the tuner icon, the tuner icon displays the **View Software Updates** command even when User Controlled Software (UCS) package deployments are not available. If UCS updates are available, the **View Software Updates** command displays the UCS dialog with the list of available packages. If UCS updates are not available, and then if you select the **View Software Updates** command, then it displays a dialog with the **No Updates Available** message.

## What are channels and packages?

One of the main features of tuners is managing channels and packages. Channels and packages are applications or files downloaded by a tuner and installed on the endpoint where the tuner is running.

A channel is a generic term used for an application or file downloaded and installed by a tuner.

Packages and Symphony Marimba Client Automation channels are terms that refer to particular types of channels.

- Packages refer to applications, files, and other information that someone has packaged into the channel format using the Application Packager product.
- Symphony Marimba Client Automation channels refer to Symphony Marimba Client Automation components that are distributed using the channel format.

Packages and channels are stored on a transmitter in a fashion similar to pages stored on a website. That is, the transmitter stores the channels, and the tuner (like a web browser) downloads the channels so they can run on a local computer. However, unlike a web browser and a website, both the tuner and the channels are designed to be consistently up-to-date; if they need updating, they can get their updates automatically from a transmitter. You can use the tuner and channels even if you are not connected to the network.

Updates occur quickly because the tuner updates channels incrementally — if only part of the channel changes, only the changed information is updated.

## Tuner installation directory

The default directory into which the tuner is installed is:

- On Windows, C:\Program Files\BMC\_Software\BBCA\Tuner
- On UNIX, /opt/BMC\_Software/BBCA/Tuner

For the console server (the tuner that you install during the initial setup and deployment), the default installation directory on UNIX is /opt/BMC\_Software/BBCA/Tuner.

The installation directory contains the following items:

- The lib directory, which contains the libraries, Java Runtime Environment (JRE), and images that the tuner must have to run.
- The tuner program, which lets you start the tuner from the command line.

You can specify arguments that you want the tuner to use when starting. For more information, see the command-line chapter of the *Symphony Marimba Client Automation Reference Guide*, available on the Marimba Channel Store.

- The `runchannel` program, which lets you start a channel on the tuner from the command line.

If the tuner is not running, `runchannel` starts it first. If you repeatedly interact with a channel or run a channel from a batch file or a script, `runchannel` is better suited for holding a command-line session. For more information, see the command-line chapter of the *Symphony Marimba Client Automation Reference Guide*.

- The tuner workspace directory, usually in a directory named `.marimba`.

For more information, see “Tuner workspace directory” on page 250.

- The `System` directory, which contains additional libraries that you want the tuner to use.

The tuner searches this directory (if it exists) before searching the `lib` directory for native libraries. This feature of the `System` directory applies to all platforms. On UNIX, the directory name case-sensitive. This directory can contain libraries that are used for uninstallation of the tuner.

## Tuner workspace directory

The tuner workspace directory is the directory on the machine where the tuner stores channel files (in subdirectories called channel directories). It is usually located inside the installation directory.

On Windows, the workspace directory is determined using the `tuner` keyword that you specify when you create the tuner installer. By default, the `tuner` keyword is based on the profile name. If you install the tuner so that it runs as a service on Windows machines, the `tuner` keyword is also used as the name of the service.

The tuner workspace directory usually has the following paths:

- On Windows, `C:\Program`

`Files\BMC_Software\BBCA\Tuner\.marimba\<keyword>`

For the console server (the tuner that you install during the initial setup and deployment), the default installation directory is `C:\Program`  
`Files\BMC_Software\BBCA\Tuner\.marimba\Marimba`.

- On UNIX, `/opt/BMC_Software/BBCA/Tuner/.marimba/<keyword>`.

For the console server, the default installation directory is `/opt/BMC_Software/BBCA/Tuner/.marimba/ws3`.

You can change the location of tuner workspace directory when you are creating the installer during setup and deployment. When installing the tuner interactively (that is, not with a silent or semi-interactive installation), users can change the location of the workspace directory. For more information, see the [Setup & Deployment help](#).

The workspace directory contains the following items:

- The `prefs.txt` file, which includes the settings for the tuner (tuner properties). If you set tuner properties using Tuner Administrator, they are saved in this file; you can edit the file to modify the tuner settings. For more information, see “[Tuner properties](#)” on page 329.

Closely related to this file is the `properties.txt` file (usually found in the tuner installation directory under `\lib\tuner\`). If you set tuner properties using profiles, the settings are saved in the `properties.txt` file. Tuner properties set using Tuner Administrator (in `prefs.txt`) override those set using profiles (in `properties.txt`). You should change tuner property values in the `prefs.txt` file and treat `properties.txt` as read only.

- The history log files, which record tuner events, such as when a tuner subscribes to or starts a channel. For more information, see “[Tuner logging](#)” on page 396.

In addition, the tuner workspace directory might contain additional log files on Windows:

- `stdout.log`, which contains standard output that is stored to this file if it is not directed to a console.
- `launch.log`, which contains information about the tuner when it goes into minimal mode.

There is no default value to this property. By default, the `launch.log` file is always created in the tuner workspace only on the Windows platform.

When you set the value of the `marimba.launch.logFile` property to “no”, no launch file is created in the tuner workspace. Setting any value other than “no” to the `marimba.launch.logFile` property does not affect the default behavior of creating the launch file.

You can specify the amount of detail in this log file by setting the tuner `marimba.launch.logLevel` property. For more information, see the tuner properties chapter of the *Symphony Marimba Client Automation Reference Guide*, available on the Marimba Channel Store.

- The map.txt file, which shows a mapping between the channels (channel URLs) and the channel directories.

For example:

```
http://localhost:5282/ChannelManager=ch.1  
http://localhost:5282/InfrastructureAdministration=ch.4  
http://localhost:5282/Transmitter=ch.2  
http://localhost:5282/cms=ch.3
```

This mapping is useful when you are troubleshooting a particular channel.

- The channel directories, which contain the data for the channels installed on the tuner. Each channel is stored in a numbered subdirectory, named ch.1, ch.2, and so on.
- The certDB and certDBinf.txt files, which contain information about the tuner certificates.
- The properties.txt file, which keeps track of the number of channels in the tuner workspace. Do not confuse this file with the properties.txt file in the tuner installation directory, which contains tuner properties.

## Checking for tuner workspace corruption

Starting in version 6.0.3SP1, you can set the following channel properties for Infrastructure Service to check and repair the tuner workspace directory:

`tuner.checkrepair`

controls whether Infrastructure Service checks for the tuner workspace directory for corruption when it runs. The default value is true.

Valid value: true or false

`tuner.repairfilter`

sets the repair filter for repairing the tuner workspace directory if Infrastructure Service finds any corruption.

Valid value: an integer

# What is Tuner Administrator?

Tuner Administrator lets you administer the tuners in your enterprise. It lets you manage and view tuners remotely; that is, you can configure a user's tuner from another computer. A help-desk operator can also connect to a user's tuner and then view and fix problems.

You can use Tuner Administrator to do the following items:

- **Manage channels.** You can add, delete, start, stop, or update channels on a remote tuner.
- **Configure tuner settings.** You can control options set in a remote tuner: security and proxy settings, modem control, update schedules, and so on.
- **Change tuner properties.** You can remotely add, edit, and delete tuner properties for a remote tuner. Tuner properties configure many characteristics and settings of a tuner, especially those that you cannot control using the browser-based interface of Tuner Administrator.
- **Restart a tuner.** You can restart a remote tuner after you change the properties or options.
- **Update a tuner.** You can update a user's tuner. For example, if a user is running an older version of the tuner, you can connect to the tuner and update it remotely.
- **Perform operations on multiple tuners.** You can restart and update tuners, scan machines, update policies, update transmitters, update proxies, and update Patch Service on multiple tuners.
- **View information about the tuner.** On the Edit Settings and Manage Channels pages, a box at the top of the page displays how long the tuner has been running (uptime), the tuner version, and the JRE version.

The tuners you administer are usually on remote machines within the network, but you can also administer a tuner on the same machine as Tuner Administrator.

# Administering a tuner

You can administer a tuner using one of the following methods:

- “Browser-based interface (console)” on page 256
- “Profiles” on page 256
- “Command-line interfaces” on page 257

This document discusses using the Tuner Administrator browser-based application to administer tuners in your environment. Most actions involving managing channels can be performed from either the console or the command-line interface.

## Browser-based interface (console)

The Tuner Administrator browser-based interface that you see through the console offers you a centralized way to manage tuners that are distributed throughout your environment. You can administer one tuner or multiple tuners simultaneously. Because Tuner Administrator is a browser-based application, you can use it remotely from any web browser. Built-in user authentication ensures that only users with appropriate permissions have access and can use Tuner Administrator.

The Tuner Administrator browser-based interface is a part of the Infrastructure Administration channel. This channel is installed as part of setup and installation. For information, see the *Symphony Marimba Client Automation Installation Guide*, available on the Marimba Channel Store.

## Profiles

Profiles let you apply the same configuration settings to multiple tuners simultaneously. Most of the time, you use profiles to change the configuration of tuners. You use Tuner Administrator (browser-based application or command-line interface) only when you must make minor changes to a particular machine or when you must configure features that you cannot use using profiles. For more information, see “Profiles and administration tools” on page 33.

## Command-line interfaces

You can administer a tuner using the Tuner Administrator command-line interface, or the command-line interface of the tuner itself.

- The Tuner Administrator command-line interface enables you to administer a tuner—one tuner at a time. The tuner can be local or remote. To use the Tuner Administrator command-line interface, subscribe to the channel called Tuner Administrator. For information, see the *Symphony Marimba Client Automation Reference Guide*, available on the Marimba Channel Store.
- The tuner command-line interface enables you to administer the local tuner. You can pass arguments to the tuner channel as it starts, and can use the `runchannel` program to manage the channels on the local tuner. For more information, see the command-line reference in the *Symphony Marimba Client Automation Reference Guide*.

The procedures provided in this document assume that you are using the console.

## 64-bit Tuner

### Introduction

Deploying the 64-bit tuner on the 64-bit Windows operating system provides you all the benefits of the 64-bit environment. The 64-bit tuner utilizes the 64-bit JRE. The 64-bit tuner uses 64-bit memory space, address space, and more number of threads that provide improved performance benefits.

---

Note: You can deploy the 64-bit tuner only on the Windows operating systems.

---

64 bit tuner is supported for following server profiles:

- Master
- Mirror
- Repeater

---

Note: The tuner can run in 64-bit mode only for transmitters. The 64-bit tuner does not support CMS.

---

The 64-bit segments are available for the following channels:

- Application Packager
- Inventory Service
- Policy Service
- Content Rep
- Deployment Service
- Patch Service
- Infrastructure Service

---

Note: SMCASMCA uses the 32-bit launcher and the 64-bit JRE.

---

The Registry Hive for Wow6432Node cannot be disabled as the tuner refers to the registry in Wow6432Node. The tuner runs in a hybrid mode and not completely in the 64-bit mode.

## Upgrade path

- 1 To run the Tuners in the 64-bit mode, first upgrade your infrastructure components from the following versions:
  - 8.1.01.009d
  - 8.2.00.005a
  - 8.2.01.002
- 2 Set the property marimba.tuner.depricate64bitsegment to false on the Tuners that you want to upgrade to 64 bit. You can set the property through Policy or Profile Update.
- 3 Update the infrastructure service and start it.

The tuner starts in the 64-bit mode.

---

Note: SMCA channels prior to 8.2.02 version will not work on the 64-bit tuner until you upgrade them to 64-bit versions. This applies only to the channels that contain OS-specific segments. Channels with “any/any” segment will not be affected.

---

There are three methods to verify whether the tuner started in the 64-bit mode.

To verify:

- 1 Go to Infrastructure Administration, and click Tuner Administration, and connect to your tuner. The tuner architecture information appears on the screen.
  - If Tuner Architecture is shown as “64 bit”, the tuner is running in 64 bit mode.
  - If Tuner Architecture is shown as “32 bit”, the tuner is running in 32 bit mode.
- 2 Go to the ISM dashboard. In the Attribute Summary table, the “Tuner Architecture” attribute has been added to determine whether the tuner is running in the 32-bit mode or 64-bit mode.
- 3 Verify the value of the “marimba.tuner.jre.arch” property. This property holds the architecture of the tuner jre. Possible values are 32 and 64.

## Fallback Mechanism

While implementing the 64-bit tuner, you can also toggle from a 64-bit tuner to a 32-bit tuner using the following property:

**marimba.tuner.depricate64bitsegment**

- If the property value is true, the tuner brings x86(32-bit) segments from the transmitter.
- If the property value is false, the tuner brings x64(64-bit) segments from the transmitter.

---

Note: After the tuner property **marimba.tuner.depricate64bitsegment** is applied, you must restart the tuners.

---

## Java Heap and PermGen settings for 64-bit Tuners

After you upgrade the tuner to 64-bit or install a new tuner in 64-bit mode, it is recommended to change the default Java Heap and PermGen settings to:

**-Xms128m -Xmx8192m -XX:PermSize=32m -XX:MaxPermSize=2560m**

---

Note: After you change this setting, restart the tuner.

---

## Marimba over Internet

The tuner has the ability to support SMCA operations over the internet. If you want to configure endpoints to resolve host names based on which network the endpoint is located in, you can use this feature to control how endpoints download updates or send reports to the SMCA server infrastructure. For example, you can use this feature in a use case scenario where you use a non-SSL load balancer inside the company network, and it is required for the endpoints to connect to an SSL-enabled reverse proxy located outside the company network. In this scenario, if you have a mechanism to resolve host names of policy and package URLs, the tuner is capable of switching between the load balancer and the reverse proxy.

To enable this feature set the **marimba.tuner.internetdeploy.enabled** tuner property to true. If this property is not set, or set to false, this feature is disabled. By default, this feature is disabled



Chapter

# 16 Getting started with Tuner Administration

This chapter provides the necessary information when you first start administering the tuner.

The following topics are provided:

- Prerequisites before using Tuner Administration (page 264)
- General process for administering a tuner (page 265)
- Starting and stopping tuners (page 268)
- Logging in to and out of Tuner Administrator (page 269)
- Operations for one tuner versus multiple tuners (page 272)
- Connecting to one or more tuners (page 273)
- Triggering a deployment job from Tuner Administration (page 282)
- Monitoring a job (multiple tuners only) (page 282)
- Viewing information about a tuner (page 286)
- Restarting a tuner (page 288)
- Updating a tuner (page 289)
- Scanning the machine on which the tuner is running (page 291)
- Updating the policy on the endpoint where the tuner is running (page 293)
- Updating transmitters and proxies (page 294)
- Updating Patch Service on the endpoint where the tuner is running (page 295)
- Starting the console window (page 296)

# Prerequisites before using Tuner Administration

Before you can use Tuner Administrator, you must meet the following prerequisites:

- **Install and configure the required channels.** Because Tuner Administrator is a part of the Infrastructure Administration channel and relies on the CMS channel to run, the CMS and Infrastructure Administration channels must be installed and configured. You must know the host name of the machine on which the channels were installed and you must provide the host name when you log in to the browser-based console to use Tuner Administrator.
- **Have a user account with the proper access.** You must already be assigned a user name, a password, and a user role that has access to Tuner Administrator. User roles determine the capabilities of users when they log in to the console. When users log in, their roles are assigned based on the user name and password they provide. The following roles are available: primary administrator, standard administrator, and operator. The roles determine the features of Tuner Administrator to which you have access. For more information, see “Using roles to limit access to Tuner Administrator features” on page 269.
- **Make sure the tuners are running.** The tuners must be running before you can administer them. For more information, see “Starting and stopping tuners” on page 269.
- **Know machine information.** You must know the host name or IP address of the machine where the tuner is running. If the tuner is not using the default administration port (7717), you must know what port it is using.
- **Know administration credentials.** If administration is restricted for a tuner, you must know the user name and password for the tuner you want to administer.
- **Tuner starts up upon machine startup.** It is recommended that the tuner on which you download Tuner Administrator is configured to start upon machine startup. This is more efficient for logging in to and using Tuner Administrator remotely. After the tuner starts, the console and Tuner Administrator start as well. If that tuner is not configured to start upon machine startup, you have to start the tuner and Tuner Administrator manually.

However, if you plan to package applications (using Application Packager) on the machine and save the package to a network share, do not configure the tuner to run as a service. Instead, configure it to run upon machine start up by adding the tuner to the Windows Startup Folder.

- **DNS or WINS resolution.** Make sure you have DNS or WINS resolution set up and working properly in your environment. This is important especially when you are specifying the tuners you want to administer by entering the host name of machines or selecting from a list of host names.
- **Required versions.** Tuner Administrator and the tuner should be the same version (for example, if you are using tuner 7.1, it is recommended that you use the Tuner Administrator that is a part of the Infrastructure Administration 7.1 channel).

## General process for administering a tuner

This section explains the general process for administering the tuner using the Tuner Administrator. For more information, see “Performing actions on channels” on page 307.

### ► To configure tuners using Tuner Administrator

1 Make sure the tuner you want to configure is running—if the tuner is not running, you cannot configure it. For more information, see “Starting and stopping tuners” on page 268.

2 Log in to Tuner Administrator, as described in “Logging in to Tuner Administrator” on page 271.

The role assigned to you determines what features of Tuner Administrator you can use, as described in “Using roles to limit access to Tuner Administrator features” on page 267.

3 Connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 279.

4 Edit settings or perform actions on the tuner.

5 If you have changed any settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 264.

After applying the changes, Tuner Administrator usually returns to the Edit Settings page. However, if the changes include the following settings, Tuner Administrator warns you that it will disconnect from the tuner:

- Administration port
- Remote administration access settings
- Administration port SSL settings

For more information, see “Specifying remote administration access to the tuner” on page 338 and “Working with SSL settings” on page 345.

## Previewing and applying configuration settings

Before you can apply configuration changes to the tuner, you must preview the changes. The following figure shows the Preview page for Tuner Administrator:

Figure 15-1: Preview page for Tuner Administrator

	New Value	Original Value
User Interaction Mode		
User Interaction Mode	Fully interactive	Semi-interactive
URL for the tuner user interface:	http://marimba:5282/ChannelManager	(none entered)

The Preview page parallels the Edit Settings page. The Preview page contains the following tabs, each corresponding to a tab on the Edit Settings page:

- The **General** tab shows the settings for the tuner user interaction mode and channel update restrictions.
- The **Security** tab shows the administration access settings and trusted transmitters for the tuner.
- The **Custom Properties** tab shows the tuner properties that you want to apply to the tuner.
- The **Advanced** tab shows advanced settings for the tuner, such as licensing, proxy, and bandwidth management information.

Each tab has two subtabs:

- The **My Changes** tab shows the settings you have changed during the session.
- The **All Settings** tab shows all the settings for the tuner, including settings that you have and have not changed during the session.

When you apply configuration settings, you apply changes that you have set in all the tabs. Make sure you review the changes in all the tabs before you apply them.

► **To preview the changes and then save them, discard them, or further modify them**

- 1 Click Preview after you have edited settings for the tuner.

Make sure you click each tab to preview the changes made to those sections.

- 2 If you do not want to save the changes, and want to continue editing the tuner settings, click Back to Edit.

This returns you to the tab from which you entered the Preview page. For example, if you entered the Preview page from the Advanced > Bandwidth tab, clicking Back to Edit brings you back to the Advanced > Bandwidth tab.

- 3 If you want to save the settings, click Apply to confirm the edits and apply them to the tuner.

When you apply configuration settings, you apply changes that you have set in all the tabs.

- 4 At any point, if you want to discard the changes and disconnect from the tuner, click Disconnect.

# Starting and stopping tuners

There are several ways to start and stop a tuner. You must have access to the machine on which the tuner is running to perform the following actions.

If there is no network connection when a tuner starts, there is a 10-minute delay after the network becomes available for the tuner to detect the network connection. The delay affects any scheduled channel operations (such as updates).

## ► To start the tuner on Windows

Do one of the following options:

- Click the Start button in the task bar and then choose All Programs > BMC > Launch Marimba Tuner.
- Double-click the tuner icon  on the desktop.
- Using a command prompt, go to the directory where you installed the tuner and then type `tuner`. For a list of options, see the command-line reference chapter in the *Symphony Marimba Client Automation Reference Guide*.
- If you have configured the tuner to run as an NT service on Windows, use the Services utility in the Control Panel to start, stop, and configure automatic startup of the tuner.

When the tuner is running, the tuner icon usually appears in the task bar.

## ► To stop the tuner on Windows

Do one of the following options:

- Right-click the tuner icon  in the task bar and then select Exit.
- When the tuner is configured to run as a service on Windows, you can stop it using the Services utility in the Control Panel.

## ► To start the tuner on UNIX

- At the command line, type  
`<install_directory>/marimba/tuner/bin/tuner`  
where `<install_directory>` is the path where you installed the tuner.

For a list of options to use when starting the tuner, see the command-line reference.

## ► To stop the tuner on UNIX

- The tuner quits after you stop all channels.

While you can close the tuner window by choosing Close from the tuner window manager menu, the tuner kernel and any running channels keep running. The tuner kernel stops when the last channel is stopped.

# Logging in to and out of Tuner Administrator

The following sections provide information for logging in to and logging out of Tuner Administrator:

- “Using roles to limit access to Tuner Administrator features” on page 269
- “Logging in to Tuner Administrator” on page 270
- “Logging out of Tuner Administrator” on page 271

## Using roles to limit access to Tuner Administrator features

Part of the initial installation and configuration is to specify which users are primary administrators, standard administrators, or operators.

- Primary administrators have access to all Tuner Administrator features.
- Standard administrators have access to all Tuner Administrator features.
- Operators can perform a limited set of actions.

Operators can perform most operations for a single tuner, but cannot manage Symphony Marimba Client Automation channels. They cannot edit configuration settings for tuners and cannot connect to and perform actions for multiple tuners.

You can find out whether you logged in as a primary administrator, standard administrator, or operator by displaying the Status pop-up window. Place the mouse pointer over the console Status icon  .

The following table summarizes roles and available features.

Features	Primary administrator	Standard administrator	Operator
<b>For a single tuner</b>			
Manage packages	Yes	Yes	Yes
Manage BMC channels	Yes	Yes	No
Restart a tuner	Yes	Yes	Yes
Scan a machine	Yes	Yes	Yes
Update a policy	Yes	Yes	Yes
Update Patch Service	Yes	Yes	Yes
Launch a console window	Yes	Yes	Yes
Edit configuration settings	Yes	Yes	No
<b>For multiple tuners</b>			
Restart tuners	Yes	Yes	No
Update tuners	Yes	Yes	No
Scan machines	Yes	Yes	No
Update policies	Yes	Yes	No
Update Patch Service	Yes	Yes	No
Update transmitters	Yes	Yes	No
Update proxies	Yes	Yes	No

For information about assigning the roles to users or groups, see the section on user authentication (a system setting).

## Logging in to Tuner Administrator

After the prerequisites described in “Prerequisites before using Tuner Administration” on page 262 have been met, you can open a browser window to log in to Tuner Administrator.

---

Note: Multiple users can log in to Tuner Administrator at one time, and can administer the same tuners in the infrastructure. Be aware of this behavior when administering tuners.

---

## ► To log in to Tuner Administrator

- 1 Open a browser window and enter `http://<machine_name>:<port>` where `<machine_name>` is the host name of the machine on which the CMS console and Tuner Administrator (from the CMS and Infrastructure Administration channels) are running and `<port>` is the browser access port number for the console. The default port number is 8888.
- 2 In the login window, enter your user name and password and then click Login. Make sure you specify a user name that is defined as either a primary administrator or administrator. For more information, see “Using roles to limit access to Tuner Administrator features” on page 267.

If the defaults have not yet been changed, in the User name field, enter `admin` and leave the Password field empty. When you log in as the user `admin`, you are logged in as a primary administrator.

Note: The user name `admin` is the *emergency* user name. By default, the emergency administrator password is blank. It is recommended that you create your own emergency administrator password to prevent unauthorized users from logging in using the default emergency user name. For more information, see the System Settings online help.

- 3 Click Applications > Infrastructure > Tuner Administration.

You can now connect to and start administering one or more tuners.

Note: If you cannot log in to Tuner Administrator because it is not yet running, use the Applications Manager page (part of System Settings) to start it. You must start the Infrastructure Administration channel that includes Tuner Administrator. For information, see the System Settings online help.

## Logging out of Tuner Administrator

If you do not use Tuner Administrator for 60 minutes (the default timeout), you are automatically logged out: the next time you click a button, the login box prompts you to log in again. You can configure the timeout by using a system setting. For more information, see the System Settings online help.

When you are finished using Tuner Administrator, it is a good practice to *completely log out* of Tuner Administrator by clicking Log Out and then closing the browser window. When you do this, you are really logging out of the console. The session does *not* automatically end when you close the browser window, or when you leave Tuner Administrator and start using another application (like Report Center) running on the console.

## Operations for one tuner versus multiple tuners

Using Tuner Administrator, you can administer one or more tuners. When administering one tuner, you can change configuration settings, as well as perform actions, such as scanning the machine and restarting the tuner. When administering multiple tuners, you can only perform actions, but not change configuration settings.

When administering *multiple* tuners, you can perform the following actions:

- Scan the machine
- Update the policy on the endpoint
- Restart the tuner
- Update the tuner
- Update the transmitter running on the tuner
- Update the proxy running on the tuner
- Update Patch Service on the tuner

When administering *one* tuner, in addition to performing all the previously described actions, you can edit configuration settings, such as the user interaction mode and security settings.

When performing actions for either multiple tuners or a single tuner, Tuner Administrator connects to the tuner and starts the action, but it does not monitor whether the action completed successfully.

A user who is logged in to Tuner Administrator can perform only one action on multiple tuners at any one time. For example, you cannot first update policies for a group of tuners, and then scan inventory information on a group of tuners. However, you can use Tuner Administrator to perform actions on a single tuner while Tuner Administrator is performing an action on multiple tuners.

# Connecting to one or more tuners

Before you can perform any actions or configure any settings, you must connect to one or more tuners. You usually connect to tuners by specifying their host names and port numbers.

This section describes the different ways in which you can connect to tuners. It includes the following topics:

- “Manually entering a list of tuners” on page 273
- “Selecting from a list of recently used tuners” on page 274
- “Querying for a list of tuners” on page 278

## Manually entering a list of tuners

You can manually enter the list of tuners you want to administer. Use this feature when you know the exact host name of the tuners you want to administer. If you want to administer a large number of tuners, you might want to select from a list of recently used tuners or query for a list of tuners.

### ► To specify tuners by manually entering a list

- 1 On the Connect to a Tuner page, from the Specify tuners using list, choose Manual entry.
- 2 In the Host Name and Port text area, enter the host name and port number of one or more tuners.

If specifying more than one tuner, include a line break after each host name and port number. For example:

```
http://ca_client:7000  
http://ny_client:7000  
http://hi_client:7000
```

Tip: You can specify just the host name of the tuners. Tuner Administrator automatically attaches `http://` and 7717 (the default administration port). If the tuner is using a secure connection (`https://`) or is running on another port, you must use the following format: `https://<host_name>:<port_number>` (for example, `https://ca_client:7000`).

- 3 If administration access is restricted to the tuners, enter the administration user name and password in the Tuner user name and Tuner password fields.

Note: If you are administering multiple tuners, the same user name and password are used to connect to all the tuners you have specified. Depending on the browser that you are using, you can save the user name and password so that you do not have to type them again later when you reconnect to the tuner. For more information, see the browser online help.

- 4 If you are administering multiple tuners, specify values used while connecting to and performing actions on the tuners:
  - From the Simultaneous connections list, select the maximum number of tuners that Tuner Administrator tries to connect to simultaneously.
  - In the Action timeout field, specify the number of seconds that Tuner Administrator allows for an action to be started on a tuner. If the action has not been started on a tuner after this amount of time, Tuner Administrator no longer tries to start the action on that tuner. This happens only on a per-tuner basis. A value of 0 (zero) means that the action never times out.
  - In the Job timeout field, specify the number of minutes that Tuner Administrator allows for an action to be started on all the specified tuners. If the action has not been started on the entire group of tuners after this amount of time, Tuner Administrator does not start the action on the remaining tuners. A value of 0 (zero) means that the job never times out.

Note: For more information, see “What is a job?” on page 281.

- 5 Specify the administration action you want to perform on the tuners:
  - Click Manage Channels. This option lets you perform actions on packages and channels for one tuner.
  - Click Edit Settings. This option lets you change the configuration settings for one tuner.
  - Select an action from the drop-down list, and click Go. This option is the only one available if you are administering multiple tuners. You can use the list to perform an action for a single tuner.

## Selecting from a list of recently used tuners

Tuner Administrator keeps a list of the tuners that it has attempted to connect to recently. From this list, you can select the tuners that you want to administer. This feature is useful when you know the host name of the tuners you want to administer, and it lets you avoid manually entering the names.

By default, the 10 most recently used tuners appear in this list. To change the number, see “Advanced: configuring the number of tuners displayed in the list” on page 274. By default, you are presented with the list of recently used tuners on the Connect to a Tuner page. The only exceptions are if you have not previously entered a list of tuners to administer, or if you have set the default option to be manual entry. To change the default entry mode to be manual, see “Advanced: changing the default entry mode” on page 275.

### ► To select from a list of recently used tuners

- 1 From the Specify tuners using list, select List of recently used tuners.
- 2 In the list of tuners that appears, select the check boxes next to the tuners you want to administer.

**Tip:** Be careful when selecting the tuners. All tuners that Tuner Administrator attempted to connect to appear in this list, not just the ones that Tuner Administrator connected to successfully. This means that miss-typed host names appear in the list. The tuners do not appear in the order in which they were added to the recently used list.

- 3 If administration access is restricted to the tuners, specify the administration user name and password in the Tuner user name and Tuner password fields.

**Note:** If you are administering multiple tuners, the same user name and password are used to connect to all the tuners you have specified. Depending on the browser that you are using, you can save the user name and password so that you do not have to type them again later when you reconnect to the tuner. For more information, see the browser online help.

- 4 If you are administering multiple tuners, specify values used while connecting to and performing actions on the tuners:
  - From the Simultaneous connections list, select the maximum number of tuners that Tuner Administrator tries to connect to simultaneously.
  - In the Action timeout field, specify the number of seconds that Tuner Administrator allows for an action to be started on a tuner. If the action has not been started on a tuner after this amount of time, Tuner Administrator no longer tries to start the action on that tuner. This happens only on a per-tuner basis. A value of 0 (zero) means that the action never times out.

- In the Job timeout field, specify the number of minutes that Tuner Administrator allows for an action to be started on all the specified tuners. If the action has not been started on the entire group of tuners after this amount of time, Tuner Administrator does not start the action on the remaining tuners. A value of 0 (zero) means that the job never times out.

Note: For more information, see “What is a job?” on page 281.

- 5 Specify the administration operation you want to perform on the tuners:
  - Click Manage Channels. This option lets you perform actions on packages and channels for one tuner.
  - Click Edit Settings. This option lets you change the configuration settings for one tuner.
  - Select an action from the drop-down list, and click Go. This option is the only one available if you are administering multiple tuners. You can use the list to perform an action for a single tuner.

## Advanced: configuring the number of tuners displayed in the list

You can configure the number of tuners that are displayed in the list of recently used tuners by editing a property in the Infrastructure Administration channel. By default, the 10 most recently used tuners are retained and appear in the list.

---

Note: This property applies to all the administration tools. It affects how many tuners, transmitters, and proxies are displayed in Tuner Administration, Transmitter Administration, and Proxy Administration.

---

### ► To configure the number of tuners displayed in the list

- 1 Locate the channel directory for the Infrastructure Administration channel.

You can use the `map.txt` file in the tuner workspace directory. For more information, see “Tuner workspace directory” on page 250. The `map.txt` file shows a mapping between the channels (channel URLs) and the channel directories (for example, `http://localhost:5282/InfrastructureAdministration=ch.4`).

- 2 In the Infrastructure Administration channel directory, locate the properties.txt file in the data/persist directory (for example, ch.4/data/persist/properties.txt).
- 3 In the properties.txt file, add the property infraAdmin.remoteadmin.recentlist.size property and set its value to an integer greater than zero (0); the default is 10. Save the file.
- 4 Restart the Infrastructure Administration channel.

The next time you use Tuner Administration (or any of the administration tools), the specified number of tuners are retained and displayed in the list of recently used tuners.

## Advanced: changing the default entry mode

By default, you are presented with the list of recently used tuners on the Connect to a Tuner page. The only exceptions are if you have not previously entered a list of tuners to administer, or if you have set the default option to be manual entry. You can change the default entry mode to be manual (instead of selecting from a list of recently used tuners) by editing a property in the Infrastructure Administration channel.

---

Note: This property applies to all the administration tools and determines the default entry mode for the Tuner Administration, Transmitter Administration, and Proxy Administration.

---

### ► To set manual entry as the default

- 1 Locate the channel directory for the Infrastructure Administration channel. You can use the map.txt file in the tuner workspace directory. For more information, see “Tuner workspace directory” on page 250. The map.txt file shows a mapping between the channels (channel URLs) and the channel directories (for example, http://localhost:5282/InfrastructureAdministration=ch.4).
- 2 In the Infrastructure Administration channel directory, locate the properties.txt file in the data/persist directory (for example, ch.4/data/persist/properties.txt).

- 3 In the properties.txt file, add the property infraAdmin.remoteadmin.target.input.type property and set its value to manual. The default is recent, indicating that the default option is the list of recently used tuners. Save the file.
- 4 Restart the Infrastructure Administration channel.

The next time you use Tuner Administrator (or any of the administration tools), manual entry appears as the default mode for specifying tuners on the Connect to a Tuner page.

## Querying for a list of tuners

You can select the tuners you want to administer from the results of a Report Center query. You define the query in Report Center, and then select the query in Tuner Administrator to see the list of tuners. This feature is useful when you want to administer tuners that meet certain criteria. It is also useful when you know the kind of tuners you want to administer (for example, tuners running on a particular port) but not the host names.

In general, it is recommended that you configure the CMS (on which Tuner Administrator is running) to use a directory service. This enables the fully qualified name of the machine to be displayed in the query results, so that you can select the exact machine that you want to administer. This feature is useful especially if your environment includes machines with the same host name, but belonging to different domains.

This section contains the following topics:

- “Prerequisites for using queries with Tuner Administrator” on page 276
- “Defining a query in Report Center” on page 277
- “Using the query in Tuner Administrator” on page 279

### Prerequisites for using queries with Tuner Administrator

To query for a list of tuners using Tuner Administrator, you must meet the following prerequisites:

- Report Center must be running on the same machine as Tuner Administrator.
- You must have configured the database settings in the Data Source section of the system settings. For information, see “Managing databases” on page 155.

- Report Center must be configured to query this database. Scanner Service on the machines you are planning to administer must be configured to send reports to this database.

## Defining a query in Report Center

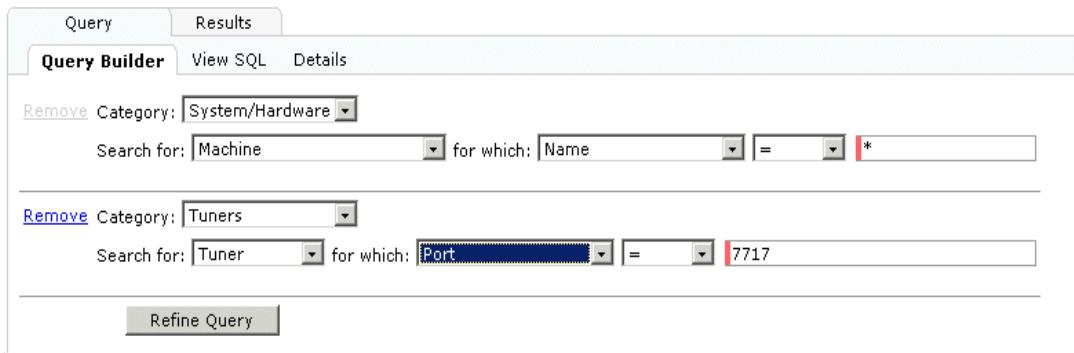
In Report Center, you must define queries that search for machines on which a tuner is running. You can specify search criteria that query for machines in a particular region or subnet. After you save this query to a particular folder in Report Center, you can run this query using Tuner Administrator.

### ► To define a query for machines with tuners in Report Center

- 1 Log in to Report Center.
- 2 Make sure you have already imported the query library. For information, see the *Symphony Marimba Client Automation Report Center User Guide*, available on the Marimba Channel Store.
- 3 Under the Queries > BCAC Administrative Groups > Tuner Administrator folder, create a query that searches for a list of machines that have a tuner installed on them.
- 4 If you want to use Query Builder to construct this query, you must first search according to machine name, and then (if desired) according to other attributes of the machine, and lastly, you must search for tuners that have a particular attribute. Do the following:
  - a From the Category list, select System/Hardware.
  - b For the search criteria, specify Machine, and specify the types of machines for which you want to search. For example, machines in a particular domain.
  - c Click Refine Query.
  - d From the Category list, select Tuners.
  - e For the search criteria, select Tuner and specify the kinds of tuners for which you want to search. For example, you can search for a particular version of a tuner or the administration port the tuner is using.
  - f At this point, you can choose to refine the query even more and search by any category.
  - g Save the query.

**Example:** The following figure shows a Query Builder example of a tuner query:

Figure 15-2: Query builder example of a tuner query



- 5 If you are building a raw SQL query, make sure you include the following columns in the query:

- machine\_name
- machine\_domain
- id
- rpcport
- rpcsslport
- rpcipaddr

For example, the following raw SQL query finds all tuners that use the administration port 7880:

```
select inv_machine.name machine_name,inv_machine.machine_domain,
id, rpcport, rpcsslport, rpcipaddr from inv_tuner, inv_machine
where inv_machine.id = inv_tuner.machine_id and inv_tuner.rpcport
= 7880
```

Make sure you save the query in the **Queries > BCAC Administrative Groups > Tuner Administrator** folder. Queries that you save in any other folder or subfolder do not appear in Tuner Administrator.

## Using the query in Tuner Administrator

After you have defined queries in Report Center and saved them in the appropriate folder, you can use the results of the queries in Tuner Administrator to select the tuners you want to administer.

For queries to appear in the Tuner Administrator list, you must create them using Report Center, and save them to a particular folder. For more information, see “Defining a query in Report Center” on page 277.

### ► To select from a list of tuners in a query result

- 1 In Tuner Administrator, from the Specify tuners using list, select the name of the query that you defined in Report Center.

The list of tuners in the query result appears in the table.

- 2 In the list of tuners that appears, select the check boxes that correspond to the tuners you want to administer.
- 3 If administration access is restricted to the tuners, specify the administration user name and password in the Tuner user name and Tuner password fields.

Note: If you are administering multiple tuners, the same user name and password are used to connect to all the tuners you have specified. Depending on the browser that you are using, you can save the user name and password so that you do not have to type them again later when you reconnect to the tuner. For more information, see the browser online help.

- 4 If you are administering multiple tuners, specify values used while connecting to and performing actions on the tuners:
  - From the Simultaneous connections list, select the maximum number of tuners that Tuner Administrator tries to connect to simultaneously.
  - In the Action timeout field, specify the number of seconds that Tuner Administrator allows for an action to be started on a tuner. If the action has not been started on a tuner after this amount of time, Tuner Administrator no longer tries to start the action on that tuner. This happens only on a per-tuner basis. A value of 0 (zero) means that the action never times out.
  - In the Job timeout field, specify the number of minutes that Tuner Administrator allows for an action to be started on all the specified tuners. If the action has not been started on the entire group of tuners after this amount of time, Tuner Administrator does not start the action on the remaining tuners. A value of 0 (zero) means that the job never times out.

Note: For more information, see “What is a job?” on page 281.

- 5 Specify the administration task you want to perform on the tuners:
  - Click Manage Channels. This option lets you perform actions on packages and channels for one tuner.
  - Click Edit Settings. This option lets you change the configuration settings for one tuner.
  - Select an action from the drop-down list, and click Go. This option is the only one available if you are administering multiple tuners. You can also use the list to perform an action for a single tuner.

## Triggering a deployment job from Tuner Administration

You can start a deployment job directly from the Tuner Administration.

### ► To start a deployment job from the Tuner Administration:

- 1 Navigate to Tuner Administrator.
- 2 In the Connect to a Tuner page, select the required targets on which you want to perform a deployment task.
- 3 In the Select an Action drop down list, select Deploy DM Job action.
- 4 Click Go.

The Deployment Manager automatically starts and displays the Edit Task page where you can define the commands which you want to execute on the selected targets. Deployment Manager automatically creates the Folder, Target Group, and Deployment job for the new deployment task. In the Edit Task Group, by default the Trigger Scan & Stats report check box is selected to trigger scan and stat report after the deployment task is completed. You can clear the Trigger Scan & Stats report check box if you do not want the scan and stat report.

- 5 Once you define the commands, run the deployment job.

## Monitoring a job (multiple tuners only)

The following sections introduce you to the concept of a job, and explain how you can monitor and control the progress of a job:

- “What is a job?” on page 283

- “Viewing job status details” on page 283
- “Stopping, resuming, and retrying a job” on page 285

You do not have to remain logged in to Tuner Administrator (with the browser window open) when performing an action on multiple tuners. If you log out and close the browser window, you can come back later, open a new browser window, and log in to Tuner Administrator again to monitor the progress of the action that you started.

## What is a job?

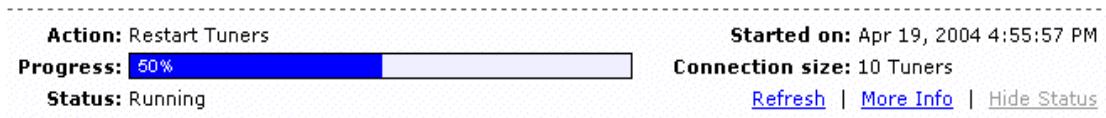
An action being performed on a group of tuners is called a *job*. An action (such as restarting the tuner) is performed and is completed on *each individual tuner*. A job refers to the action being performed on an *entire group of tuners*. A job is completed only after the action has been performed (successfully or not) on all the specified tuners.

## Viewing job status details

You can view the status of a job. A job refers to an action (such as restarting a tuner) being performed on an entire group of tuners. For more information, see “What is a job?” on page 283.

### ► To view detailed information about a job

- 1 On the Connect to a Tuner page, in the progress section near the top of the page, click More Info.



- 2 When you want to exit the Detailed Job Information page, click Done. You return to the Connect to a Tuner page.

On the Detailed Job Information page, you can view information about the job, including the following items:

- **Action.** The action you have chosen to perform on the tuners.

- **Started on.** The date and time when Tuner Administrator started connecting to the group of tuners and performing the action that you specified.
- **Total connections.** The total number of tuners to which Tuner Administrator tries to connect and perform the action that you specified.
- **Progress.** The progress of the job. This is the percentage of tuners that Tuner Administrator has connected to and started the action that you specified.

**Note:** The progress for the job reflects whether Tuner Administrator was able to connect to the tuners and start the action. It does not reflect whether the specified action was completed successfully on the tuners.

- **Status.** The status of the job, which can be one of the following: not started, running, paused, done, cancelled, or timed out.
- **Time remaining.** The estimated time remaining for Tuner Administrator to complete the job. In other words, this is the estimated time remaining for Tuner Administrator to connect to the tuners and start the specified action on all the tuners.

You can view the current status of the individual tuners on which you are performing the action. The status for a tuner can be one of the following:

- **Pending.** Indicates that Tuner Administrator is still trying or will soon try to connect to and start the action on the tuner.
- **Successful.** Indicates that Tuner Administrator connected to and started the action on the tuner. A status of successful does not indicate that the action was completed successfully on the tuner.
- **Failed.** Indicates that Tuner Administrator could connect to the tuner, but failed to start the action on the tuner.
- **Could not connect.** Indicates that Tuner Administrator could not connect to the tuner successfully, for example, because of network issues or because the incorrect administration credentials were provided.
- **Timed out.** Indicates that the action has been timed out on that tuner (according to the action timeout value).

By default, the tuners are displayed 20 at a time. If the list includes more than 20 tuners, you can use the **next** link or the drop-down list to see the next group of tuners. If you want to change the number of tuners displayed, follow the procedure listed in the section “Advanced: configuring the number of tuners that appear per page” on page 285.

## Advanced: configuring the number of tuners that appear per page

You can configure the number of tuners that you want to appear at one time on the Detailed Action Information page by editing a property in the Infrastructure Administration channel. This property applies to all the administration tools.

### ► To configure the number of tuners per page

- 1 Locate the channel directory for the Infrastructure Administration channel.

You can use the `map.txt` file in the tuner workspace directory. For more information, see “Tuner workspace directory” on page 250. The `map.txt` file shows a mapping between the channels (channel URLs) and the channel directories (for example,

`http://localhost:5282/InfrastructureAdministration=ch.4`).

- 2 In the Infrastructure Administration channel directory, locate the `properties.txt` file in the `data/persist` directory (for example, `ch.4/data/persist/properties.txt`).
- 3 In the `properties.txt` file, add the property `infraAdmin.page.size` and set its value to an integer greater than zero (0); the default is 20. Save the file.
- 4 Restart the Infrastructure Administration channel.

The next time you use Tuner Administrator (or any of the administration tools), tuners appear on the Detailed Action Information page according to the number that you specified.

## Stopping, resuming, and retrying a job

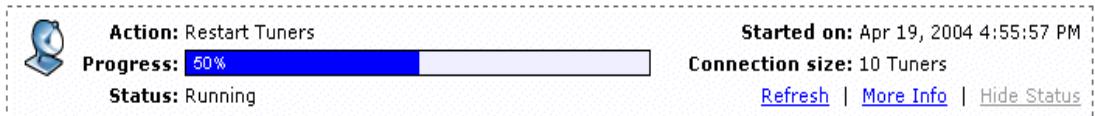
In addition to viewing status information about a job, you can control the job in the following ways:

- Pause the job.
- Stop the job.
- Retry the job.

For more information, see “What is a job?” on page 283.

## ► To stop, resume, or retry a job

- 1 On the Connect to a Tuner page, in the progress section near the top of the page, click More Info.



- 2 Do one of the following:
  - Click Pause Job to temporarily stop the job at any time. After this, you can click Resume Job to start the job again at the point at which it was paused.
  - Click Stop Job to stop the job completely.
  - Click Retry Failed to retry the job. This retries performing the action on tuners on which the action is pending, failed, timed out, or to which Tuner Administrator could not connect.
- 3 When you want to exit the Detailed Job Information page, click Done. You return to the Connect to a Tuner page.

## Advanced: configuring the refresh rate for status pages

You can configure the refresh rate for the areas that reflect job status. By default, the pages refresh automatically every 30 seconds. You can configure the refresh rate for the following areas:

- The status bar in the Connect to a Tuner page (which appears automatically after you start an action on multiple tuners).
- The Detailed Job Information page.

You configure the refresh rate by editing a property in the Infrastructure Administration channel. This property applies to all the administration tools.

## ► To configure the refresh rate for the status pages

- 1 Locate the channel directory for the Infrastructure Administration channel.

You can use the `map.txt` file in the tuner workspace directory. For more information, see “Tuner workspace directory” on page 250. The `map.txt` file shows a mapping between the channels (channel URLs) and the channel directories (for example, `http://localhost:5282/InfrastructureAdministration=ch.4`).

- 2 In the Infrastructure Administration channel directory, locate the `properties.txt` file in the `data/persist` directory (for example, `ch.4/data/persist/properties.txt`).
- 3 To configure the refresh rate of the status bar in the Connect to a Tuner page, in the `properties.txt` file, add the property  
`infraAdmin.remoteadmin.1-n.progress.basic.refresh.interval` and set its value to an integer greater than zero (0), representing the number of milliseconds after which the page refreshes. The default is 30000 milliseconds (30 seconds).
- 4 To configure the refresh rate of the Detailed Job Information page, in the `properties.txt` file, add the property  
`infraAdmin.remoteadmin.1-n.progress.detailed.refresh.interval` and set its value to an integer greater than zero (0), representing the number of milliseconds after which the page refreshes. The default is 30000 milliseconds (30 seconds).
- 5 To configure the refresh rate of the Tuner Administration > Manage Channels page, in the `properties.txt` file, add the property  
`infraAdmin.remoteadmin.tuneradmin.ajaxRequest.update.interval` and set its value to an integer greater than zero (0), representing the number of milliseconds after which the page refreshes. The default is 30000 milliseconds (30 seconds). For slower networks, this value can be increased, by multiples of 1000, to optimize network bandwidth utilization.
- 6 Save the `properties.txt` file.
- 7 Restart the Infrastructure Administration channel.

The next time you use Tuner Administrator (or any of the administration tools), the specified refresh rates apply to the status pages.

## Viewing information about a tuner

When you are connected to a tuner, a box near the top of the Edit Settings and Manage Channels pages lets you view the following information:

- **Up since.** Displays the date and time when the tuner started running. For tuners version 6.0 and higher, the Up since date and time includes periods when the tuner went into minimal mode.

For older tuners, you see the JRE up since date and time instead of the Up since date and time because only new tuners have a statistic that stores the date and time when the tuner started running (regardless of how many times it has gone in and out of minimal mode). The date and time for older tuners is not as accurate for determining how long a tuner has been running because it only measures how long the current instance of the Java Virtual Machine (JVM) has been up and running. When the tuner goes in and out of minimal mode, the statistic is reset.

- **JRE up since.** Displays the date and time when the tuner started running. This date and time is based on how long the current instance of the Java Virtual Machine (JVM) has been up and running. The date and time are reset when the tuner goes in and out of minimal mode, so if the tuner goes into minimal mode, the date and time reflect how long it has been running since coming out of minimal mode.
- **Tuner version.** Displays the version number of the tuner to which you are connected.
- **JRE version.** Displays the version number for the JRE used by the tuner to which you are connected.

## Restarting a tuner

You can restart a remote tuner using Tuner Administrator. This is useful when you update a remote tuner or change its properties, and you must restart the tuner for the update or changes to take effect.

### ► To restart a tuner

Use Tuner Administrator to connect to the tuners you want to restart as described in “Connecting to one or more tuners” on page 273.

- 1 If you specified a single tuner to which you want to connect:

- a At the bottom of the Connect to a Tuner page, click either Edit Settings or Manage Channels.
  - b Near the top of the Edit Settings or Manage Channels page, click the Restart Tuner link.
  - c Confirm that you want to restart the tuner.
- 2 If you specified multiple tuners to which you want to connect:
    - a At the bottom of the Connect to a Tuner page, select Restart tuner from the drop-down list, and click Go.
    - b Monitor the job as described in “Monitoring a job (multiple tuners only)” on page 280.

---

Note: The status message reflects whether Tuner Administrator was able to connect to the tuners and start the action successfully. The status message does not reflect whether the specified action was completed successfully on the tuners.

---

Unlike older versions, Tuner Administrator versions 6.0 and higher do not attempt to reconnect to a tuner after restarting it.

If the SSL certificate password for the tuner is not saved, the restarted tuner cannot start the administration port in SSL-enabled mode.

## Updating a tuner

When you update a tuner using Tuner Administrator, Tuner Administrator updates and starts the Infrastructure Service channel on the remote tuners. The Infrastructure Service channel downloads updates to the tuners (both binaries and profile updates) and installs them.

Usually, the Infrastructure Service channel restarts the tuner after it downloads and applies any updates, unless the tuner has been configured not to restart after updates.

For more information, see “Updates to profiles and tuner binaries” on page 290.

## ► To update a remote tuner

- 1 Use Tuner Administrator to connect to the tuners you want to update as described in “Connecting to one or more tuners” on page 271.
- 2 At the bottom of the page, select Update tuner from the drop-down list, and click Go.

This action updates and starts the Infrastructure Service channel on the remote tuners. The Infrastructure Service channel downloads updates to the tuners (both binaries and profile updates) and installs them. After it downloads and applies any updates, the Infrastructure Service channel restarts the tuner, unless the tuner has been configured not to restart after updates.

**Note:** The status message reflects whether Tuner Administrator was able to connect to the tuners and start the action successfully. The status message does not reflect whether the specified action was completed successfully on the tuners.

## Updates to profiles and tuner binaries

The Infrastructure Service that runs on all the tuners in your enterprise is the software that performs updates to both the tuner executable (binaries) and the configuration settings (profile) for that tuner.

**Updates to binaries.** Updates to the tuner binaries can occur when Symphony releases a new version of the Infrastructure Service channel. This channel contains three types of segments: segments for default profiles, segments for installer templates, and platform-specific segments for tuner binaries. Following is a list of the tuner binary segments:

- Linux,i386/any
- Windows,x86/any
- any/any

For the tuners in your enterprise to get updates to the tuner binaries when a new version is released, you must use Transmitter Administration to copy the segments from the transmitter to the Infrastructure Service channel on the master transmitter. At the scheduled time (which was set by creating or editing the tuner profile), updates to the binaries are automatically applied and the tuner is restarted. You can also update tuners manually using Tuner Administrator; see “Updating a tuner” on page 287. (Or, if the tuners are part of a Server Management infrastructure and so do not have a schedule, you can run a deployment job to update the Infrastructure Service on the endpoints and then restart the tuner.)

**Updates to profiles.** Updates to profiles most often occur when you edit a profile and save the changes. In this case, the new configuration settings get “published” to a profile segment of the Infrastructure Service channel. The name of the segment corresponds to the profile name. For example, if you create a profile and name it `Win_HR_Endpoints`, then the segment are named:

`.profile_Win_HR_Endpoints`

Updates to a profile are applied to a tuner according to the same schedule as for updates to binaries, since both are part of the Infrastructure Service channel. The tuner is restarted after applying updates to its profile, so that the new configuration settings can take effect.

## Scanning the machine on which the tuner is running

You can use Tuner Administrator to scan the machine on which the tuner is running and send the information it gathers to a database. Then, you can use Report Center, to view the gathered information.

This section describes how you use Tuner Administrator to scan machines. It contains the following topics:

- “What is Scanner Service?” on page 291
- “Scanning the machine” on page 292

### What is Scanner Service?

Scanner Service is a client agent that runs on the tuner on each endpoint. It enables endpoints to perform inventory scans (you can define the kind of information you want to gather) and then sends this information back to the Inventory plug-in that resides on a transmitter.

Usually, the Scanner Service scans machines according to a start schedule that you set using Report Center. You can use Tuner Administrator to scan machines independently from the schedule.

## Scanning the machine

When you perform this action, the Scanner Service channel scans the machine and sends the information it gathered to the Inventory plug-in, which in turn inserts the information into the database. You can use Report Center to view the gathered information. For more information, see the *Symphony Marimba Client Automation Report Center User Guide*, available on the Marimba Channel Store.

### ► To scan the machine on which the tuner is running

Use Tuner Administrator to connect to the tuners as described in “Connecting to one or more tuners” on page 273.

- 1 If you specified a single tuner to which you want to connect:
  - a At the bottom of the Connect to a Tuner page, click either Edit Settings or Manage Channels.
  - b Near the top of the Edit Settings or Manage Channels page, click the Scan Machine link.
  - c Confirm that you want to scan the machine.
- 2 If you specified multiple tuners to which you want to connect:
  - a At the bottom of the Connect to a Tuner page, select Scan machine from the drop-down list, and click Go.
  - b Monitor the job as described in “Monitoring a job (multiple tuners only)” on page 282.

Note: The status message reflects whether Tuner Administrator was able to connect to the tuners and start the action successfully. The status message does not reflect whether the specified action was completed successfully on the tuners.

# Updating the policy on the endpoint where the tuner is running

You can use Tuner Administrator to update the policy on the endpoint on which the tuner is running. Then, the tuner downloads and applies the policy that you have assigned the endpoint using Policy Manager.

This section describes how you use Tuner Administrator to update policies. It contains the following topics:

- “What is Policy Service?” on page 293
- “Updating the policy” on page 293

## What is Policy Service?

Policy Service is a client agent that runs on the tuner on each endpoint. It applies the policies assigned to the endpoints using Policy Manager. It downloads the policies from the Policy Service plug-in that resides on a transmitter. The policies determine, among other things, which packages to install on endpoints.

Usually, Policy Service updates and applies policies according to a schedule that you set using Policy Manager. You can use Tuner Administrator to update policies independently from the schedule.

## Updating the policy

When you perform this action, the Policy Service channel updates and downloads the policy from the Policy Service plug-in, which in turn gets the policy information from the directory service. Then, Policy Service applies the policy to the endpoint, which might include downloading and installing packages. For more information, see the *Symphony Marimba Client Automation Policy Manager User Guide*, available on the Marimba Channel Store.

### ► To update the policy on the endpoint where the tuner is running

Use Tuner Administrator to connect to the tuners as described in “Connecting to one or more tuners” on page 273.

- 1 If you specified a single tuner to which you want to connect:

- a At the bottom of the Connect to a Tuner page, click either Edit Settings or Manage Channels.
  - b Near the top of the Edit Settings or Manage Channels page, click the Update Policy link.
  - c Confirm that you want to update the policy.
- 2 If you specified multiple tuners to which you want to connect:
    - a At the bottom of the Connect to a Tuner page, select Update policy from the drop-down list, and click Go.
    - b Monitor the job as described in “Monitoring a job (multiple tuners only)” on page 280.

Note: The status message reflects whether Tuner Administrator was able to connect to the tuners and start the action successfully. The status message does not reflect whether the specified action was completed successfully on the tuners.

## Updating transmitters and proxies

As part of upgrading the transmitters and proxies in your enterprise, you can use Tuner Administrator to update the transmitter and proxy channels to a new version. Tuner Administrator downloads updates for the transmitter and proxy channels on the remote tuners.

Before you update the transmitter and proxy channels, make sure you read the chapter on upgrading transmitters and proxies in the upgrade section of the *Symphony Marimba Client Automation Installation Guide*, available on the Marimba Channel Store. This guide tells you what you must do to prepare for upgrading proxies and the different types of transmitters.

### ► To update proxies or transmitters

- 1 Use Tuner Administrator to connect to the tuners on which proxies or transmitters are running as described in “Connecting to one or more tuners” on page 271.
- 2 At the bottom of the page, select Update proxy or Update transmitter from the drop-down list, and click Go.

This action updates the proxy or transmitter channels on the remote tuners.

**Note:** The status message reflects whether Tuner Administrator was able to connect to the tuners and start the action successfully. The status message does not reflect whether the specified action was completed successfully on the tuners.

## Updating Patch Service on the endpoint where the tuner is running

You can use Tuner Administrator to update and start Patch Service on the endpoint on which the tuner is running. Then, the tuner updates and starts Patch Service, installing any patches required by the endpoint as determined by Patch Service.

This section describes how you use Tuner Administrator to update Patch Service. It contains the following topics:

- “What is Patch Service?” on page 293
- “Updating Patch Service” on page 294

### What is Patch Service?

Patch Service is a client agent that runs on the tuner on each endpoint. It controls patch installation and serves two functions:

- It builds a list of patches to install, determines which are relevant and the dependencies between them, and installs them. To decide on the order of installation, Patch Service considers all dependency constraints. If a patch depends on another patch that has not been installed and is unavailable, or if the operating system is not compatible with the patch, then it is not installed.
- It enhances the inventory scan of an endpoint by extending the amount of patch information that can be reported.

Usually, Patch Service updates and starts according to a schedule that you set using Patch Manager. You can use Tuner Administrator to update and start Patch Service independently from the schedule.

## Updating Patch Service

When you perform this action, the Patch Service channel updates, determines which patches are relevant to the endpoint, and installs them. For more information, see the *Symphony Marimba Client Automation Patch Management User Guide*, available on the Marimba Channel Store.

► **To update and start Patch Service on the endpoint where the tuner is running**

- 1 Use Tuner Administrator to connect to the tuners as described in “Connecting to one or more tuners” on page 271.
- 2 At the bottom of the Connect to a Tuner page, select **Update Patch Service** from the drop-down list, and click **Go**.
- 3 If you are performing this action on more than one tuner, monitor the job as described in “Monitoring a job (multiple tuners only)” on page 280.

**Note:** The status message reflects whether Tuner Administrator was able to connect to the tuners and start the action successfully. The status message does not reflect whether the specified action was completed successfully on the tuners.

## Starting the console window

You can display a console window to troubleshoot problems with the tuner that you are administering. The console window displays information about tuner and channel actions. For example, you can use the console window if you are having problems with a particular channel, and you want to capture its output so that you can send it to technical support.

**Prerequisite:** You must have a tuner running on the machine where you are using the Tuner Administrator browser-based interface. The Console Window channel runs on the tuner on this machine, not the one where the remote tuner is running.

► **To start a console window for the tuner**

- 1 Use Tuner Administrator to connect to the tuners as described in “Connecting to one or more tuners” on page 271.
- 2 At the bottom of the Connect to a Tuner page, click either **Edit Settings** or **Manage Channels**.

- 3 Near the top of the Edit Settings or Manage Channels page, click the Launch Console link.

If you do not already have the Console Window channel, the tuner on the local machine subscribes you to it.

- 4 If the tuner that you connect to requires a user name and password, enter them in the dialog box that appears.

The console window appears. Notice that it displays the host name and port of the tuner you are connected to, as well as the date and time when the console was started. For example:

```
Console Started(client:7717/tuner): October 30, 2003 3:49:24 PM
```

## Advanced: configuring the URL for the console window

By default, the administration tools use the host name and port number from the deploy wizard (if the host name and port number are not null) to get the console window from the following URL:

```
http://<host_name>:<port_number>/Marimba/Current/ConsoleWindow
```

If the host name and port number are null, then the administration tools use the following URL:

```
http://products.marimba.com/Current/ConsoleWindow
```

You can configure the URL for the console window by editing a property in the Infrastructure Administration channel. This property applies to all the administration tools.

### ► To configure the URL for the console window

- 1 Locate the channel directory for the Infrastructure Administration channel.

You can use the `map.txt` file in the tuner workspace directory. For more information, see “Tuner workspace directory” on page 250. The `map.txt` file shows a mapping between the channels (channel URLs) and the channel directories (for example, `http://localhost:5282/InfrastructureAdministration=ch.4`).

- 2 In the Infrastructure Administration channel directory, locate the `properties.txt` file in the `data/persist` directory (for example, `ch.4/data/persist/properties.txt`).

- 3 In the properties.txt file, add the property infraAdmin.console.url and set its value to a URL where the Console Window channel is located (for example, <http://localhost:5282/Marimba/Current/ConsoleWindow>). Save the file.
- 4 Restart the Infrastructure Administration channel.

The next time you use Tuner Administrator (or any of the administration tools) and launch the console window, it uses the URL that you specified.

## Waking up an endpoint using the WoW feature

You can use the Wake-on-Wan (WoW) feature to wake up machines that are in a power off state. The WoW feature runs in CMS as a service and for each WoW task in CMS, the WoW feature creates a unique Task ID. For more information about the WoW feature, see the *Policy Management User Guide*.

You can use the Tuner Administrator to wake up a target machine which is in a power off state. Once you trigger the WoW wake up task for a machine, Tuner Administrator displays the status of the WoW task based on the magic packet which is sent to the target machine. Magic packets are UDP packets that are broadcasted to the machines that need to be woken up in a subnet.

### Waking up a single target

In the Tuner Administrator, to wake up a single target machine, you can use the WoW feature from the Connect to a Tuner page. You can wake up a single machine by manually typing the hostname or by selecting the hostname from the recently used list of hostnames. Once the hostname is typed or selected, select Wakeup from the list which you can see beside the Go button, and click Go.

### Waking up multiple targets

In the Tuner Administrator, you can wake up multiple targets by creating a collection and then run the wake up process on the computers specified in the collection.

#### ► To wake up multiple computers in a collection:

- 1 In Report Center, create a collection under the Tuner Administrative groups of the Queries tab.

- 2 In the Tuner Administrator login page, select the collection which you have created in the preceding step.

The tuner administrator runs the collection and displays the list of the computers in the collection.

If you do not want to use a collection, you can also manually enter the list of target machines in the text box. If you manually specify the target name, instead of using the collection name, and if the same hostname exists in multiple domains, then you need to specify a fully qualified name.

- 3 Select the required computers from the displayed list.
- 4 Select the Wake Up option from the dropdown list which you can see beside the Go button.
- 5 Click Go.

The WoW features displays the status of overall WoW task completion.

- 6 To view the WoW task status of individual machines, click the More info link.

The WoW feature displays the status of each individual target machine based on the status of the magic packet which it sends to the target machines.

## WOW Properties

Below is the list of WOW Properties:

- "marimba.wow.wakeup.strategy"
- "marimba.wow.filter.subnets"
- "marimba.wow.ping.timeout"
- "marimba.wow.ping.useapi"
- "marimba.wow.ping.retrycount"

**Permission:** Primary and tenant Primary

**Location:** [System Settings](#) - > [Features Management](#) -> “Wake-on-WAN” link

**Screen Shot:**



## Distribute WOW Properties:

Below is the list :

- "marimba.taskdistribution.port"
- "marimba.taskdistribution.enabled"
- "marimba.taskdistribution.password"
- "marimba.taskdistribution.groupname"
- "marimba.taskdistribution.port.autoincrement"
- "marimba.taskdistribution.multicast.port"
- "marimba.taskdistribution.multicast.address"
- marimba.taskdistribution.tcpip.enabled"
- "marimba.taskdistribution.tcpip.members"

**Permission:** primary, tenant super admin

**Location:** [System settings -> Features Management -> “Distribute Wake-on-WAN” link](#)

**Screen Shot:**

Distribute Wake-on-WAN Settings Page

i From this page, you can configure the Distribute Wake-on-WAN related settings.

---

<input checked="" type="checkbox"/> Allow to use distribute WOW using task executor service.
Group Name : <input type="text"/>
Port : <input type="text"/>
Password : <input type="password"/>
<input type="checkbox"/> Allow to use auto increment of the port number for running multiple workers in a single computer.
Multicast Port : <input type="text"/>
Multicast Address : <input type="text"/>
<input type="checkbox"/> Allow to use only TCP/IP for environments where multicast is not available or preferred.
TCP/IP Members : <input type="text"/>

# Chapter 17 Package and channel management for a tuner

Tuner Administrator lets you manage the packages and channels on the remote tuner. You can start, stop, subscribe, unsubscribe, and update packages and channels. You can view and edit the package or channel properties, including changing the update schedule. For more information, see “What are channels and packages?” on page 248.

In this chapter, topics and procedures uses the term channels to refer to both packages and channels when discussing actions that can be performed on both. For actions that can be performed on either packages only or BMC Marimba Client Automation channels only, that restriction is mentioned in those topics and procedures.

The following topics are provided:

- Viewing channels on the tuner (page 300)
- Performing actions on channels (page 304)
- Viewing and changing channel-specific information (page 310)

## Viewing channels on the tuner

When you connect to a tuner using Tuner Administrator, you can view the channels to which the tuner is subscribed. To distinguish between applications you packaged and applications provided by BMC Marimba Client Automation, there are two tabs: the Packages tab and the BMC Marimba Client Automation Channels tab.

Both tabs show the following information for channels:

- The channel names.
- The host name and port number of the transmitter that hosts the channel.
- The current status of the channel. (For more information, see “Channel states” on page 301.)
- The date when the channel was last updated. If the channel was updated today, the time of the last update is shown.
- The size of the channel.

### ► **To view the channels on the tuner**

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 271.
- 2 After specifying the tuner you want to connect to, click Manage Channels.
- 3 Click the Packages tab or BMC Marimba Client Automation Channels tab depending on what you want to view.

## Filtering the list of channels using groups

Depending on how channels were created and published, they might belong to a group. These groups let you view certain channels together in Tuner Administrator. These groups are sometimes referred to as channel categories.

If you are involved in packaging and publishing channels, you can specify the group to which a channel belongs using the property category (usually in the channel properties.txt file) before you publish the channel to a transmitter. BMC Marimba Client Automation channels are usually assigned a group name that corresponds to the family of products in which they belong.

---

Note: You cannot use Tuner Administrator to create, rename, change, or delete groups for channels on remote tuners.

---

► **To filter the list of channels using groups**

On the Manage Channels page, click the list next to Packages to show or Channels to show, and select a group to display. To display all channels or channels, select All package groups or All channel groups.

## Sorting the list of channels

You might find a particular channel more easily if you sort the list displayed by Tuner Administrator. You can sort the list using the following columns:

- Name
- Status
- Last updated
- Size

► **To sort the list of channels on the tuner**

On the Manage Channels page, click the title the column you want to use for sorting.

If you sort using the Name or Status columns, the list is sorted alphabetically according to the name or status.

## Channel states

Channel states indicate the current condition of a channel. Usually, they indicate the type of operation the channel has recently run. The following states are common to all channels (even the BMC Marimba Client Automation components that are channels):

- available
- subscribed
- unsubscribed
- running
- updating

The other states are only available to packages created using Application Packager.

## States for Application Packager (any version) packages

The following states are available to packages created using any version of Application Packager.

State	Description
available	The channel is available for download and installation.
subscribed	The channel was successfully downloaded (subscribed), but installation was not attempted.
unsubscribed	The channel was uninstalled and unsubscribed from the workspace. No updates to the channel can be downloaded.
running	The channel is running, or the channel is installing, uninstalling, verifying, repairing, or launching an application.
updating	The channel is getting updates from a transmitter.
installed	The package successfully installed an application.

## States for Application Packager (version 4.6 or later) packages

The following states are available for packages created using only Application Packager version 4.6 or later.

State	Description
install-pending	The package was successfully downloaded, and a package update was downloaded into the tuner workspace and is awaiting installation.
failed (install)	The installation of the package failed.
failed (pre-install)	A pre-installation script included in the package failed, and the installation was aborted.
failed (post-install)	A post-installation script included in the package failed. The application installed by the package might be unusable.
failed (uninstall)	The uninstallation of the package failed.
failed (pre-uninstall)	A pre-uninstallation script included in the package failed, and the uninstallation was aborted.

State	Description
failed (post-uninstall)	A post-uninstallation script included in the package failed. The uninstall of the package must be attempted again to remove the package from the tuner workspace.
failed (verify)	The verification of the package failed.
failed (pre-verify)	A pre-verification script included with the package failed, and the verification was aborted.
failed (post-verify)	A post-verification script included with the package failed.
failed (launch)	The launching of the package failed. The operation was aborted.
failed (pre-launch)	A pre-launch script included with the package failed, and the launch was aborted.
failed (post-launch)	A post-launch script included with the package failed.
failed (repair)	The repair of the package failed.
failed (pre-update)	A pre-update script included with the package failed, and the update was aborted.
failed (post-update)	A post-update script included with the package failed.
> aborted (<operation>)	The Application Installer was interrupted or stopped before it could write out one of the following <operation> states:
<ul style="list-style-type: none"> <li data-bbox="400 865 544 891">n pre-install</li> <li data-bbox="400 900 544 926">n install</li> <li data-bbox="400 934 544 960">n post-install</li> <li data-bbox="400 969 544 995">n pre-verify</li> <li data-bbox="400 1003 544 1029">n verify</li> <li data-bbox="400 1038 544 1064">n post-verify</li> <li data-bbox="400 1073 544 1099">n pre-uninstall</li> <li data-bbox="400 1107 544 1133">n uninstalled</li> <li data-bbox="400 1142 544 1168">n post-uninstall</li> <li data-bbox="400 1176 544 1202">n pre-update</li> <li data-bbox="400 1211 544 1237">n post-update</li> </ul>	The specified operation was aborted.

# Performing actions on channels

One of the important uses for Tuner Administrator is performing actions on channels on a remote tuner. This section describes the actions you can perform on channels:

- “Subscribing to channels” on page 307
- “Starting and stopping channels” on page 309
- “Updating channels” on page 309
- “Unsubscribing channels” on page 311
- “Deleting channels” on page 312
- “Verifying and repairing packages” on page 312

---

Note: The actions that you can perform depend on the channel or package that you select. Some actions cannot be performed while another action is taking place.

---

## Subscribing to channels

You can use Tuner Administrator to subscribe a remote tuner to channels. When you subscribe to a channel, the tuner downloads the channel and saves it on your local hard drive. You can then configure the tuner and the channel to automatically download updates at scheduled intervals.

Before you can subscribe to a channel, you must know either:

- The URL for the channel (for example, `http://server:5282/applications/FinanceApp`).
- The host name and port number for the transmitter that hosts the channel (for example, `http://server:5282`).

### ► To subscribe to a channel

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 271.
- 2 After specifying the tuner you want to connect to, click Manage Channels.
- 3 Click the Packages tab or BMC Marimba Client Automation Channels tab depending on what you want to subscribe.

- 4 Click Subscribe to a Package or Subscribe to a Channel.
- 5 If you know the URL, in the Package URL or Channel URL field, enter the URL for the channel.

The URL usually consists of the host name of the machine on which the transmitter is running, the port number for the transmitter, the name of any channel folders, and the name of the channel (for example, `http://server:5282/applications/FinanceApp`).

- 6 If you do not know the URL, you can browse for a channel:
  - a Click Browse.
  - b In the Connect to field, enter the host name and port number for a transmitter, and click Go.

The channels on the transmitter that you specified appears.
  - c Choose a channel, and click Select.

The package or channel URL appears in the Package URL or Channel URL field.
- 7 If the channel comes from a transmitter with restricted access, enter the subscribe user name and password.
- 8 Click Subscribe.

The tuner subscribes to the channel you specified.
- 9 After you finish managing channels, click Done to disconnect from the tuner.

Note: It is recommended that you wait for the tuner to complete the subscription or installation process for a channel before subscribing to or installing another channel. Performing channel subscriptions or installations concurrently might result in problems with the channels. For example, depending on how your system administrator has packaged a channel, installing a channel might require rebooting your system. This reboot might disrupt any channel subscriptions or installations that the tuner is concurrently performing.

## Starting and stopping channels

You can start or stop a channel on a remote tuner. If you are connecting to tuners that run on users' machines, use caution when starting or stopping a channel because of what users might experience. For example, if users are running a channel and you stop it without warning them, they might think their system or tuner has crashed. If you start a channel, the user might see windows appear and then close them. Inform users before starting or stopping a channel on their tuner.

### ► To start or stop a channel

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 271.
- 2 After specifying the tuner you want to connect to, click Manage Channels.
- 3 Click the Packages tab or BMC Marimba Client Automation Channels tab depending on what you want to start or stop.
- 4 Right-click the channel and choose one of the following operations:
  - **Start.** The channel you specified starts on the remote tuner.
  - **Start with args.** If you choose this option, you are asked to specify the arguments that you want to start the channel with. The channel you specified starts on the remote tuner with the arguments you specified.
  - **Stop.** If the channel is currently running, it stops on the remote tuner.You can also start or stop multiple channels by clicking the check boxes beside the channels and clicking the Start or Stop button.  
When the Tuner Administrator page refreshes, it displays the new status of the channel.
- 5 After you finish managing channels, click Done to disconnect from the tuner.

## Updating channels

You can use Tuner Administrator to update a channel on a remote tuner.

---

Note: To update a channel, the channel must *not* be running. If necessary, stop the channel before starting an update.

---

## ► To update one or more channels

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 271.
- 2 After specifying the tuner you want to connect to, click Manage Channels.
- 3 Click the Packages tab or BMC Marimba Client Automation Channels tab depending on what you want to update.
- 4 Click the check boxes beside the channels you want to update and click the Update button.

The channels you specified check for an update from the transmitter, and, if updates are available, downloads them. When the Tuner Administrator page refreshes, it displays the new date or time in the Last Updated column for the channels.

- 5 After you finish managing channels, click Done to disconnect from the tuner.

## Changing a channel URL

If you want a channel to update from a different URL, you can use Tuner Administrator to change the transmitter and channel location where a channel gets updates. For example, after you move a channel from one transmitter to another.

---

Note: To change the URL for a channel, the channel must *not* be running. If necessary, stop the channel before changing its URL.

---

## ► To change the URL for a channel

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 271.
- 2 After specifying the tuner you want to connect to, click Manage Channels.
- 3 Click the Packages tab or BMC Marimba Client Automation Channels tab depending on what you want to change the URL for.
- 4 Locate the channel, and, under the Actions column, choose Update from.

A dialog box appears prompting you for the new URL. Usually, it displays the current URL for the channel.

- 5 Enter the new URL for the channel.

The channel you specified checks for an update from the new URL you specified, and, if there is an update, downloads the update. When the Tuner Administrator page refreshes, it displays the transmitter for the channel in the Name column.

The tuner immediately tries to update the channel to make sure the channel URL you specified is correct. If the URL is not valid, you get an error message and the tuner changes the URL back to the original URL.

- 6 After you finish managing channels, click Done to disconnect from the tuner.

## Unsubscribing channels

When you unsubscribe from a channel, the tuner keeps a copy of the channel data on your local hard disk, but does not update it from that point on. Some channels create documents or preferences that you want to keep even if you do not want the main part of the channel. To keep the data created by a channel but delete the channel itself, you *unsubscribe* from the channel.

---

Note: To unsubscribe a channel, the channel must *not* be running. If necessary, stop the channel before unsubscribing it.

---

### ► To unsubscribe from a channel

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 271.
- 2 After specifying the tuner you want to connect to, click Manage Channels.
- 3 Click the Packages tab or BMC Marimba Client Automation Channels tab depending on what you want to unsubscribe.
- 4 Locate the channel, and, under the Actions column, choose Unsubscribe.

When the Tuner Administrator page refreshes, it displays the new status of the channel. The tuner deletes the main channel files, and the channel status changes to unsubscribed.

- 5 After you finish managing channels, click Done to disconnect from the tuner.

## Deleting channels

Tuner Administrator lets you remove channels from a tuner. When the tuner deletes a channel, it deletes all of the files for the channel, including any files created by the channel while it was running on your machine. For example, some channels might store user preferences or other information based on how you used the channel. However, exactly what is deleted can depend on the channel—deleting some channels deletes all data, including any files you create using the channel, while deleting others deletes only the preferences or settings used by the channel.

---

Note: To delete a channel, the channel must *not* be running. If necessary, stop the channel before removing it.

---

### ► To remove a channel

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Manage Channels.
- 3 Click the Packages tab or BMC Marimba Client Automation Channels tab depending on what you want to remove.
- 4 Locate the channel, and, under the Actions column, choose Delete.

When the Tuner Administrator page refreshes, the channel no longer appears in the list. The tuner deletes the channel files.

If the channel you’re deleting was created using Application Packager, the channel uninstalls in silent mode.

- 5 After you finish managing channels, click Done to disconnect from the tuner.

## Verifying and repairing packages

Tuner Administrator lets you verify and repair packages on a tuner. This operation is only available for packages that were created using Application Packager. Sometimes applications and content that you package and distribute to users as channels might become unusable or not run properly. You can use the verify and repair capabilities to automatically check and fix problems, such as missing or corrupted files.

**What does verify do?** When you verify a channel, the file and registry objects in the channel are compared with the file and registry information for the channel when it was originally installed. Any object mismatches found are recorded in the log files.

**What does repair do?** When you repair a channel, the file and registry objects in the channel are first verified as described previously. After verification is complete, one of the following occurs:

- There are no object mismatches. No repairs are needed.
- There are object mismatches. The tuner re-installs the affected files or registry entries if they are available from the Tuner storage. If not, the tuner contacts the transmitter to download the files or registry entries needed to complete the repair.

---

Note: To verify or repair a package, the package must *not* be running. If necessary, stop the package before verifying or repairing it.

---

### ► **To verify or repair a package**

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Manage Channels.
- 3 Click the Packages tab.
- 4 Locate the package, and, under the Actions column, choose one of the following operations:
  - Verify
  - Repair

The tuner verifies or repairs the package files.

- 5 After you finish managing channels, click Done to disconnect from the tuner.

## Viewing and changing channel-specific information

You can use Tuner Administrator to view and change information that applies to individual channels. You can view and change the following information:

- The schedule for updating a channel.

- The security and capabilities for a channel.

You can view only general information for a channel. This information includes the channel name, URL, size, and the date of the last update.

This section includes the following topics:

- “Viewing general channel information” on page 312
- “Setting the update schedule for a channel” on page 315
- “Viewing and setting the capabilities for a channel” on page 318

## Viewing general channel information

You can view general information about a channel using Tuner Administrator. The following information appears for the channel:

- **Transmitter** shows the name of the transmitter where the channel comes from. This is typically the host name of the machine where the transmitter is running.
- **Channel** is the name of the channel. This is set by the person who created and published the channel.
- **Channel URL** is the complete URL for the channel.
- **Publish date** lists the date and time the channel was published to the transmitter.
- **Date last updated** lists the date and time the channel was last updated.
- **Date last checked** lists the date and time when the tuner last checked if there was an update available on the transmitter for the channel. This information is useful if you set the channel update schedule (see “Setting the update schedule for a channel” on page 312 for more information) to check for updates only and not actually download updates.
- **Next scheduled update** lists the date and time for the next update.
- **Channel size** is the amount of disk space that the channel is using on your system. If you have disk compression software, this number might not be accurate.
- **Data size** is the amount of disk space for files created by the channel. These files are normally kept in the `data` directory of the channel.

- **Type** describes the type of the channel (for example, it says “packaged” for packages created using Application Packager). This value can be applet, application, presentation, or other channel types not yet defined.
- **Author** is usually the name of the person who created and published the channel.
- **Administrator** is the person to contact if you have problems with the channel.
- **Copyright** lists legal information about the channel.
- **Version** is the version number for the channel as specified by the person who published it.
- **Channel description** is a description of the channel written by the person who published it.

#### ► To view general information about a channel

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 271.
- 2 After specifying the tuner you want to connect to, click Manage Channels.<sup>3</sup> Click the Packages tab or BMC Marimba Client Automation Channels tab depending on what you information you want to view.
- 4 Click the channel name to see the General Information page.
- 5 After you finish managing channels, click Done to disconnect from the tuner.

## Setting the update schedule for a channel

When you subscribe to a channel, the tuner automatically manages the updates for that channel. However, you can set specific times or day/time ranges during which you want a specific channel to update.

In addition to specific update times, the tuner has update restrictions that override any channel-specific settings. For more information, see “Setting update restrictions for channels” on page 324.

#### ► To schedule channel updates

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Manage Channels.

- 3 Click the Packages tab or BMC Marimba Client Automation Channels tab depending on what you information you want to view.
- 4 Locate the channel, and, click the channel name.
- 5 Click the Schedule tab.
- 6 In the Update Schedule section, specify the update schedule for the channel. Some of the options are as follows:
  - **Never.** The tuner never updates the channel automatically; you have to manually update the channel when necessary.

---

Note: When the network.notify channel property is set to its default value of true, and when the tuner goes from offline to online, the Infrastructure Service starts, even if the update schedule is set to Never.

---

- **Daily.** The channel can be updated every day, only on weekdays (Monday through Friday), or every 1 to 9 days, depending on the number you set. You can specify the time of day when updates occur.
  - **Weekly.** The channel gets updated every 1 to 9 weeks, depending on the number you set. During the week of the update, the update occurs only on the days you select. You can specify the time of day when updates occur.
  - **Monthly.** The channel can be updated every 1 to 99 months on the day you set. If you choose day 30 or 31 and the month when the update occurs does not have that day, the update occurs on the first day of the next month. You can specify the time of day when updates occur.
- 7 In the Update Options area, select the check boxes you want:
    - Check for updates but do not actually download them

The tuner checks the transmitter and finds out if an update is available, but it does not download the update.
    - Vary update time to improve network performance

The tuner spreads out updates so that they do not occur all at the same time. This is useful if you have many tuners in an enterprise running a channel that is set to update at the same time. For example, if a channel on multiple tuners updates every Monday between 8 am and 9 am, it is possible that on Monday the network load might spike.
  - 8 Click Save to set the update schedule for the channel.

A channel updates according to the schedule you set unless one of the following situations occurs:

- If the tuner is not running when an update is set to occur, then updates occur the next time the tuner is started.
  - If tuner update restrictions prevent an update from occurring, then the update happens at the next available time determined by the update restriction settings.
- 9 After you finish managing channels, click Done to disconnect from the tuner.

## How time changes (Daylight Saving Time) affect scheduled channel updates

Time changes, such as those associated with switching from Daylight Saving Time to Standard Time (and vice-versa), might affect scheduled channel updates. This section gives some examples of how channel updates might be affected.

Tuner Administration will use the 2007 (and beyond) Daylight Saving Time schedule if you apply the appropriate vendor-supplied patches. Third-party tools are compliant with this change. The new Daylight Saving Time schedule applies to all supported platforms.

### Daylight Saving Time to Standard Time

- The channel is set to update at 10:00 am. The tuner adjusts to the time change, and the update takes place correctly at 10:00 am.
- The channel is set to update every one hour, for example, at 12:30 am and at 1:30 am. At 2:00 am, the time is set back to 1:00 am. The next update occurs at 2:30 am. However, the time between the 1:30 am update and the 2:30 am update is two hours, not one hour as expected.

### Standard Time to Daylight Saving Time

- The channel is set to update at 10:00 am. The tuner adjusts to the time change, and the update takes place correctly at 10:00 am.
- The channel is set to update every one hour, for example, at 12:30 am and at 1:30 am. At 2:00 am, the time is set forward to 3:00 am. The next update occurs at 3:30 am.

## Viewing and setting the capabilities for a channel

Some channels require capabilities to run properly on users' machines. These can include the following capabilities:

- Access to the local file system.
- Ability to execute other programs.
- Unrestricted access to the network.

### ► To view and set capabilities for a channel

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 271.
- 2 After specifying the tuner you want to connect to, click Manage Channels.
- 3 Click the Packages tab or BMC Marimba Client Automation Channels tab depending on what you information you want to view.
- 4 Click the channel name.
- 5 Click the Security tab.

If the channel requires capabilities to run properly, they are shown here.

- 6 If you or the user had previously granted the channels capabilities, you can deny them by selecting the Deny access to capabilities listed above check box and clicking Save.

The channel might no longer run properly if you deny it access to capabilities. If the channel comes from a trusted transmitter, you cannot deny it access to capabilities. For more information, see “Specifying the trusted transmitters for the tuner” on page 339.



# 18 General tuner settings

This chapter describes the general tuner settings you can configure using Tuner Administrator.

The following topics are provided:

- Choosing a user interaction mode (page 321)
- Setting update restrictions for channels (page 324)
- Specifying tuner reboot options (Windows only) (page 326)

# Choosing a user interaction mode

You can use Tuner Administrator to specify how much interaction you want users to have with the tuner. This section contains the following topics:

- “What is the user interaction mode?” on page 321
- “Specifying a user interaction mode for a tuner” on page 322

## What is the user interaction mode?

You can choose one of the following user interaction modes:

- **Silent.** The tuner runs in the background and is invisible to users. This mode is useful for machines that usually do not have a display, such as servers.
- **Semi-interactive.** This mode is almost the same as the silent user interaction mode, except that on platforms that support taskbar icons (such as Windows), an icon that represents the tuner appears in the task bar.
- **Fully interactive.** The tuner is visible on the desktop, and users can fully interact with it. This mode is useful if you want to give users control over what applications are installed and updated on their machines. If you choose this mode, you must specify the URL for the user interface that you want the tuner to use.
- **Custom.** This option is selected if the tuner you connect to uses a user interaction mode that is not covered by the previously described options. For example, if you have customized a tuner for user interaction, and it uses aspects of more than one of the options described, then this option is selected when you connect to the tuner. Usually, this a read-only option that is available for backwards-compatibility, and you should not use it to change the user interaction mode for the tuner.

For more information, see “Advanced: tuner properties for each user interaction mode” on page 322.

## Specifying a user interaction mode for a tuner

### ► To specify the user interaction mode for the tuner

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click **Edit Settings**.
- 3 Click the General > User Interaction Mode tab.
- 4 Choose the user interaction mode you want for the tuner. For more information, see “What is the user interaction mode?” on page 318.
- 5 If you choose the Fully interactive mode, enter the URL for the tuner user interface.
- 6 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 264.

To see the effects of the user interaction mode that you selected, you must restart the remote tuner. For more information, see “Restarting a tuner” on page 286.

## Advanced: tuner properties for each user interaction mode

This topic is provided for your reference and to help you complete the procedure described in “Choosing a user interaction mode” on page 318. Choosing a user interaction mode for the tuner affects the following tuner properties:

`marimba.tuner.enabletaskbaricons`—if set to `false`, suppresses the display of taskbar icons. The property applies to the tuner icons and channel icons. It overrides properties for icon display that might exist at the channel level.

`marimba.tuner.display.noerrors`—if set to `true`, prevents error and warning dialog boxes from appearing. The messages are instead printed out to a system console and to the tuner logs.

`marimba.tuner.display.nowarnings`—if set to `true`, prevents warning dialog boxes from appearing. The messages are instead printed out to a system console and to the tuner logs.

`marimba.tuner.display.noprogress`—if set to true, the tuner does *not* show a progress bar when channels are being subscribed to or are being updated.

`marimba.primary.url`—is the URL of the tuner primary channel, which is the first channel started when the tuner starts.

For more information, see the chapter about tuner properties in the *BMC Marimba Client Automation Reference Guide*, available on the Marimba Channel Store.

The following table compares how the user interaction modes set each of the tuner properties.

Property	Silent	Semi-Interactive	Fully interactive
<code>marimba.tuner.enabletaskbaricons</code>	false	true	true
<code>marimba.tuner.display.noerrors</code>	true	true	false
<code>marimba.tuner.display.nowarnings</code>	true	true	false
<code>marimba.tuner.display.noprogress</code>	true	true	false
<code>marimba.primary.url</code>	omitted	omitted	<channel_URL>*

The custom interaction mode differs from the other user interaction modes in that it is a read-only option that is available for backwards-compatibility. It usually does not change any of the mentioned tuner properties, as shown in the following table.

Property	Value
<code>marimba.tuner.enabletaskbaricons</code>	unchanged
<code>marimba.tuner.display.noerrors</code>	unchanged
<code>marimba.tuner.display.nowarnings</code>	unchanged
<code>marimba.tuner.display.noprogress</code>	unchanged
<code>marimba.primary.url</code>	<channel_URL>*

\* The channel URL is not required for either the fully interactive or custom interaction modes. If a channel URL is entered in the field on the User Interaction Mode tab, that URL is set as the value for the property. If the field is left blank on the User Interaction Mode tab, any value for this property is removed.

To customize a user interaction mode. For any of the user interaction modes, you can use tuner properties to customize the interaction even further. Customizing the user interaction mode is different from using the custom interaction mode.

For both semi-interactive mode and fully interactive mode, you can set the following additional properties, which affect the pop-up menu that appears when you right-click the tuner icon in the system tray:

- `marimba.tuner.trayicon.menu.about.enabled`—if set to `false`, removes the “About” menu item from the system tray icon. The default is `true`.
- `marimba.tuner.trayicon.menu.exit.enabled`—if set to `false`, removes the “Exit” menu item from the system tray icon. Selecting Exit from the menu causes the tuner to exit. The default value is `true`.
- `marimba.tuner.trayicon.menu.open.enabled`—if set to `false`, removes the “Open” menu item from the system tray icon. Selecting Open from the menu causes the channel for the tuner user interface to be displayed. The default value is `true`.

For the fully interactive mode only, you can set the following property:

- `marimba.tuner.display.nocancel`—if set to `true`, a cancel button does *not* appear in the progress indicator box that appears when installing or updating a channel. The default is `false`.

For information on setting the tuner properties to customize the interaction mode, see “Tuner properties” on page 329.

For more information, see the chapter about tuner properties in the *BMC Marimba Client Automation Reference Guide*, available on the Marimba Channel Store.

## Setting update restrictions for channels

You can set update restrictions and options for channels on the remote tuner. The settings you specify on the General > Channel Update Restrictions tab, to some extent, override any channel-specific update and start schedules that might later be applied to the channels installed on the endpoint tuner. Use this tab to specify the period of time during which channels are allowed to start or update. (This setting corresponds to the tuner property called `marimba.schedule.filter`, which controls when the tuner scheduler is active.)

## ► To set the update restrictions for packages and channels

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Edit Settings.
- 3 Click the General > Channel Update Restrictions tab.
- 4 For the update frequency, choose one of the following options:
  - **Manual updates only.** If you choose this option, packages and channels never update automatically. You must use Tuner Administrator (or the tuner user interface, if there is one) to manually update packages and channels. For more information, see “Updating channels” on page 306.
  - **Inherit from channel.** If you choose this option, packages and channels update according to their own schedules. For more information, see “Setting the update schedule for a channel” on page 315.
  - **Only at certain times.** If you choose this option, you can specify a specific time when packages and channels can update.
  - **Within a time window.** If you choose this option, you can specify the start and end times for a time window when packages and channels can update.

- 5 Select the Try to connect to the network with a modem if offline at update time check box if the tuner you are configuring is not always connected to the network, and you want it to connect using a modem when it is scheduled to perform updates.

If an update is scheduled but the tuner is offline, the tuner attempts to dial in, connect to the network, and then perform the update.

- 6 In the Minimum update interval list, specify the number of minutes you want the tuner to wait between updates.

This option is useful if you want to limit the number of times a package or channel updates within a given period of time. For example, if you specify 30 minutes, then the tuner waits at least 30 minutes between updates, even if updates are scheduled more frequently.

- 7 In the Days list, select the days you want channel updates to occur.
- 8 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 266.

# Specifying tuner reboot options (Windows only)

The Common Reboot Service runs on the tuner and manages endpoint reboot requests from Patch Management, Policy Administrator, and Application Packager. This service queues up reboot requests so that fewer reboots are necessary. The service also ensures that service channels running on an endpoint are not interrupted by a reboot request from another service channel.

You can configure the Common Reboot Service through a profile in Setup & Deployment -> Profiles. You can also configure the service for an endpoint from Tuner Administrator, and you can override the settings from Policy Manager.

From Tuner Administrator, you can configure settings such as

- whether or not to allow the machine to automatically reboot after an update
- whether or not to display alert messages to end users before rebooting the machine, and if so, for how many minutes before the reboot
- whether or not to allow end users to postpone the reboot
- Allow end users how long they can postpone the reboot and also set maximum attempts an end user can defer the maximum snooze limit
- what message appears to the end user about their reboot options
- setting a reboot schedule when you want to avoid reboot pop-up messages during business hours and to ensure a reboot occurs after multiple patches have been deployed over a period of time

## ► To specify the reboot options for the tuner

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click **Edit Settings**.

---

Note: The following steps also apply to reboot settings in Infrastructure -> Setup & Deployment -> Profiles.

---

- 3 Click the Common Reboot Service > Reboot Settings tab.

- 4 Choose one or both of the following options to enable the desired reboot behavior:
  - Allow the machine to automatically reboot after installing updates—If you do not select this option, automatic reboots will not occur after updates are installed.
  - Display alert messages to end users before rebooting the machine—Displays a pop-up window informing the user that a reboot is required.
- 5 Click one of the following options under Reboot Postponement Policy:
  - Do not allow the end user to postpone the reboot if one is required—Displays the Restart window without a snooze option to postpone the reboot.
  - Allow users to postpone the reboot for a total time of \_\_minutes and skip snooze max time for \_\_times—Displays the Snooze window to allow users to postpone the reboot until the configured time elapses. Users can also set the maximum number of attempts to defer the reboot after the configured time elapses.
  - Allow user to postpone the reboot indefinitely—Displays the Snooze window to allow the user to postpone the reboot with no time restrictions.
- 6 Choose a Reboot Countdown time period to display on the reboot window.
- 7 If you prefer to schedule reboots, select and configure a daily, weekly or monthly Reboot Schedule using the options provided.

---

Note: When the global property, marimba.schedule.filter, is set to NEVER, the value set in the marimba.reboot.schedule.at property is ignored, which causes the Snooze window to pop up immediately.

---

- 8 (optional) Click the Custom Messages tab to change the text on the Snooze and Restart windows.
  - a Change the Snooze window title and message text as needed.
  - b Decide if the Snooze window can be placed behind other windows or if it can be minimized.
  - c Change the Restart window title and message text as needed.

- d Decide if the Restart window can be placed behind other windows or if it can be minimized.
- 9 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 264.

---

Note: If you snooze the reboot for a package and then deploy another package that is configured to reboot sooner than the snooze time of the first package, the endpoint waits for the snooze time to end before rebooting.

---

## Common Reboot Service properties

The following properties control the features of the Common Reboot Service:

`marimba.reboot.interact`—specifies whether or not an alert message that warns users about a reboot is displayed. The default value is `true` (an alert message is displayed).

`marimba.reboot.interact.allowSnooze`—specifies whether users are allowed to postpone a reboot. If set to `true`, a dialog box is displayed allowing users to postpone a reboot. If set to `false`, an alert dialog box is displayed that shows a timer counting down to the reboot. The default value is `true`.

`marimba.reboot.interact.snooze.maxTime`—specifies the maximum amount of time (in milliseconds) that you want to allow users to postpone a reboot. The default value is 0 (no maximum amount of time).

`marimba.reboot.interact.timer`—specifies the amount of time in seconds to wait or count down before rebooting. This value is the starting time displayed in the alert dialog box if you set

`marimba.reboot.interact.allowSnooze` to `false`. The default value is 60 seconds. If you set this value to 0, the machine reboots immediately.

`marimba.reboot.never`—specifies whether or not to automatically reboot the machine if one is required (for example, after installing patches). Set the value to `true` if you do not want to automatically reboot the machine.

`marimba.reboot.schedule.at`—specifies a reboot at particular time only. If reboot schedule is set, then any interaction with the user is carried out at the scheduled time. If the system is in hibernate state at the scheduled reboot time, then when the user logs in back, the user interaction is carried out. If the system is restarted before the scheduled reboot time, then the user interaction and restart requests are cancelled because the restart has already been done by user manually.

`marimba.snooze.title`—sets the snooze window title.

`marimba.snooze.message`—sets the snooze message for the user.

`marimba.snooze.allowontop`—allows the snooze window to go under other windows when set to `false`. When set to `true`, the dialog will be displayed top of all other window.

`marimba.snooze.allowMinimize`—allows the user to minimize the snooze window when set to `true`.

`marimba.reboot.interact.snooze.display.always`—displays a snooze window every time a reboot is needed when set to `true`.

`marimba.reboot.title`—specifies the reboot (alert) dialog's title.

`marimba.reboot.message`—specifies the text to display as a reboot (alert) message to the user.

`marimba.reboot.allowontop`—allows the reboot (alert) window to go under other windows when set to `false`. When set to `true`, the dialog will be displayed top of all other window.

`marimba.reboot.allowMinimize`—allows the user to minimize the reboot dialog box when set to `true`.

`marimba.reboot.interact.snooze.maxLimit`—specifies the number of times a user is allowed to defer the reboot after the configured time is elapsed. The default value of this property is 0.

## Common reboot service – Track History of Actions

You can track the history of actions related to Common Reboot Service using the log file located at `<tuner_workspace_directory>\crs\crs-*.log`. This log file keeps track of history of actions related to Common Reboot Service which includes:

- user selection in snooze dialog

- user selection in count-down dialog
- channels registered for reboot
- channel that caused reboot
- time at which CRS triggered reboot
- service channel(s) in running state, which is causing delay in reboot

**Note:**

The log roll policy for this CRS history log follows the log roll policy applied for tuner. You can also disable logging of CRS related actions to this log file by setting the following tuner property:

- `marimba.logs.disableCrsHistoryLog`

This property specifies whether the CRS related actions need to be logged in the history log file.

Values: true or false

Default value: false



# 19 Tuner properties

This chapter describes the tuner properties and how you can set them using Tuner Administrator.

The following topics are provided:

- What are tuner properties? (page 333)
- Adding tuner properties (page 333)
- Editing tuner properties (page 334)
- Deleting tuner properties (page 335)

## What are tuner properties?

Tuner properties qualify the appearance, the behavior, the log support, the generic HTTP and proxy behavior, the scheduling of events, the security details, and the runtime properties of the tuner.

Tuner properties are stored in different places, depending on how you set them. If you set tuner properties using Tuner Administrator, they are saved in the `prefs.txt` file in the tuner workspace directory. If you set tuner properties using profiles, they are saved in the `properties.txt` file in the tuner installation directory. Tuner properties set using Tuner Administrator always override those set using profiles. For more information, see Chapter 2, “Profiles and administration tools.”

You can use other BMC Marimba Client Automation components, such as Deployment Manager and Policy Manager, to set tuner properties.

For more information, see the chapter about tuner properties in the *BMC Marimba Client Automation Reference Guide*, available on the Marimba Channel Store.

## Adding tuner properties

Any changes that you make in the Custom Properties tab override any changes in the other tabs if there are conflicts. For example, you specify a URL in the URL for tuner user interface field on the General > User Interaction Mode tab and you specify a value for the property `marimba.primary.url` on the Custom Properties tab. The value you specify on the Custom Properties tab overrides the one that you set on the General > User Interaction Mode tab.

If an option or field for a configuration setting is available in one of the Tuner Administrator tabs, you should use that instead of specifying a property in the Custom Properties tab.

---

Note: If you add a tuner property and a value is already specified for that property on the Custom Properties tab, the new value that you specify when adding the property overrides the older value.

---

## ► To add properties for the tuner

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Edit Settings.
- 3 Click the Custom Properties tab.

The properties that are currently set for the tuner appear. To sort the properties alphabetically, click the column title Property Name.

- 4 Click Add Property.

A blank row appears at the top of the table.

- 5 In the blank row, enter the tuner property name and value under the corresponding columns.

Warning: No checking is done at this point to verify that the property name and value you enter are valid.

- 6 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 266.

## Editing tuner properties

Any changes that you make in the Custom Properties tab override any changes in the other tabs if there are conflicts. For example, you specify a URL in the URL for tuner user interface field on the General > User Interaction Mode tab and you specify a value for the property `marimba.primary.url` on the Custom Properties tab. The value you specify on the Custom Properties tab overrides the one that you set on the General > User Interaction Mode tab.

If an option or field for a configuration setting is available in one of the Tuner Administrator tabs, you should use that instead of specifying a property in the Custom Properties tab.

## ► To edit properties for the tuner

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Edit Settings.

- 3 Click the Custom Properties tab.

The properties that are currently set for the tuner appear. By default, the properties should be arranged alphabetically by property name. If not, to sort the properties alphabetically, click the column title Property Name.

- 4 Find the tuner property that you want to edit, and change either the tuner property name or value.

---

Note: If you modify the tuner property name, then the modified tuner property is added as a separate property. The property which you have attempted to modify does not change and is retained. If you do not want to retain the property, then you must delete the property.

---

Warning: No checking is done at this point to verify that the property name and value you enter are valid.

- 5 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 266.

## Deleting tuner properties

### ► To delete properties from the tuner

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Edit Settings.
- 3 Click the Custom Properties tab.

The properties that are currently set for the tuner appear. To sort the properties alphabetically, click the column title Property Name.

- 4 Find the tuner property that you want to edit, select the corresponding check box, and click Delete.

The tuner property no longer appears in the table.

- 5 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 266.





## Chapter

# 20 Tuner security

Tuner security falls into the following categories:

- **Trusted transmitters.** You can specify which transmitters host channels that tuners allow to run or to install.
- **Remote administration.** You can specify which users and groups can use Tuner Administrator to connect to the tuner and administer it.
- **Secure Sockets Layer (SSL) encrypted communication.** You can ensure that communication between the Tuner Administrator and the tuner is secure and encrypted.

The following topics are provided:

- Specifying the trusted transmitters for the tuner (page 339)
- Specifying remote administration access to the tuner (page 341)
- Working with SSL settings (page 345)
- Tuner robustness service protection (page 348)
- Tuner self-integrity check (page 350)

# Specifying the trusted transmitters for the tuner

This section contains the following topics:

- “What are trusted transmitters?” on page 339
- “Adding transmitters to the trusted transmitters table” on page 339
- “Editing transmitters in the trusted transmitters table” on page 340
- “Removing transmitters from the trusted transmitters table” on page 341

## What are trusted transmitters?

When a tuner trusts a transmitter, the tuner automatically grants any required capabilities to channels from that transmitter without requiring the channels to be signed. The capabilities can include allowing the channel to run on the tuner and allowing the channel to install files on the machine.

## Adding transmitters to the trusted transmitters table

You can specify trusted transmitters using DNS host names or netmask/IP address pairs.

### ► To add transmitters to the trusted transmitters table

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Edit Settings.
- 3 Click the Security > Trusted Transmitters tab.
- 4 Click Add a Transmitter.
- 5 In the area that appears, choose how you want to identify trusted transmitters:
  - **Host name.** Choose this option if you want to identify a trusted transmitter using the host name of the machine on which it is running. ny\_server and ny\_server.company.com are considered different transmitters. As a best practice, use the fully qualified domain name (ny\_server.company.com) for trusted transmitters.

- **Netmask/IP address.** Choose this option if you want to identify trusted transmitters using a netmask/IP address pair. The netmask represents 4 octets (8-bit numbers) for the 32 bits in an IP address. The 4 octets in the netmask specify the bits of the IP address to keep or discard when comparing IP addresses to the one that you specify. You usually specify the netmask using integers from 0 to 255.

For example, a netmask of 255.255.0.0 means that the first 16 bits are kept and compared, while the last 16 bits are discarded; a netmask of 255.240.0.0 means that the first 12 bits are kept and compared, while the last 20 bits are discarded. If you then specify a netmask of 255.255.0.0 and an IP address of 172.16.0.0, then transmitters whose IP addresses match the first 16 bits (172.16.X.X), such as 172.16.1.2, are trusted.

6 Enter either the host name or the netmask/IP address pair.

7 Click Save to List.

The trusted transmitter you added appears in the table.

8 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 266.

## Editing transmitters in the trusted transmitters table

You can change information for any of the trusted transmitters in the table.

### ► To edit transmitters to the trusted transmitters table

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Edit Settings.
- 3 Click the Security > Trusted Transmitters tab.
- 4 Select the check box that corresponds to the transmitter and click Edit.
- 5 In the area that appears, edit the information for the trusted transmitter.
- 6 Click Save to List.

The edits appear in the table.

- 7 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 266.

## Removing transmitters from the trusted transmitters table

You can remove transmitters from the table if you no longer want the tuner to trust them.

### ► To remove transmitters from the trusted transmitters table

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Edit Settings.
- 3 Click the Security > Trusted Transmitters tab.
- 4 Select the check box that corresponds to the transmitter and click Remove. The transmitter no longer appears in the table.
- 5 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 264.

## Specifying remote administration access to the tuner

Use the Remote Administration tab to enable remote administration, which means that someone on one machine can use a BMC Marimba Client Automation administration tool to change configuration settings on a tuner that is hosted on another machine. Remote administration enables the remote administrator to install, remove, update, or repair channels on another machine.

Before system administrators can administer remote tuners, however, they must enter a user name and password. The Remote Administration tab enables you to specify which users can remotely administer tuners, and you can set a password, if desired.

**Administration port.** By default, this port number is 7717. It is the port number that you must enter when you use a BMC Marimba Client Automation administration tool to connect to the tuner. You must enter this port number when you connect to the transmitters (including mirrors and repeaters), or proxies running on the tuner.

**Specifying which users are allowed remote administration access.** The following options are available for remote administration access to the tuner:

- **Anonymous.** Remote administration access to the tuner is not restricted. System administrators can connect to the tuner without specifying a user name or password.
- **A specified user.** Remote administration access to the tuner is restricted those who enter a single user name and password. System administrators can connect to the tuner by specifying this user name and password only.
- **Users and groups from a directory service.** Remote administration access to the tuner is restricted to users and groups defined in a directory service. You can give access to all users in the directory service, or selected users and groups only. For more information, see “Using a directory service for remote administration access” on page 340.
- **No one.** Remote administration is not allowed for the tuner. If you choose this option, you (or any other user) can no longer connect to the tuner using Tuner Administrator.

---

**WARNING:** If you choose and apply the No one option, you can no longer connect to the tuner using Tuner Administrator, even if you want to change the remote administration access later. You might have to go to the machine where the tuner is running locally to change the remote administration access.

---

## ► To specify remote administration access to the tuner

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 271.
- 2 After specifying the tuner you want to connect to, click Edit Settings.
- 3 Click the Security > Remote Administration tab.
- 4 If you want to change the administration port for this tuner, specify the port number that you want to use in the Administration port field.

Note: When you apply the changes to the tuner using Tuner Administrator, you are disconnected from the tuner. The next time you connect to the tuner, you must use the new administration port that you specified.

- 5 Select one of the remote administration access options:
  - **Anonymous.**
  - **A specified user.** Enter the user name and password that you want to use.
  - **Users from a directory service.** To use this option, choose from the available directory services and specify which users and groups you want to give access. For more information, see “Using a directory service for remote administration access” on page 343.
  - **No one.**
- 6 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 264.

Note: When you apply changes to the remote administration settings, Tuner Administrator warns you and disconnects from the tuner. If you want to continue administering the tuner, you must reconnect. If you have changed the administration port or remote administration access source, remember to use the new port, user name, or password when connecting to the tuner.

## Using a directory service for remote administration access

You can use a directory service to control remote administration access to a tuner. To use a directory service, you must specify the following information:

- The directory service to use.
- The users and groups that you want to give administration access.
- An emergency password to use if the directory service is not available.

**Directory service to use.** Choose a directory service from those available in the Directory service list. For directory services to appear in this list, you must add the information for them to the system settings (from the Applications menu, choose Console > System Settings > Data Source > Directory Services). For more information, see “Adding or editing a directory service” on page 145 and “Using automatic discovery for Active Directory” on page 152.

If you want to use Active Directory as the directory service, make sure that you do not use automatic discovery. The administration tools require that you explicitly enter the host name, port number, and base DN for Active Directory. For more information, see “Adding or editing a directory service” on page 144 and “Using automatic discovery for Active Directory” on page 152.

**Users and groups to give access.** When you are using a directory service for remote administration access, you have three options:

- 1 Option 1: You can give access to all the users in the directory service. To use this option:
  - a In the Allow remote administration for list, select Users from a directory service.
  - b Select Allow remote access for all users in the directory service
- 2 Option 2: You can give access to a specified user in the directory service. To use this option:
  - a In the Allow remote administration for list, select Users from a directory service.
  - b Select Allow remote access for the following user.
  - c Enter the name of one user in the directory service. You can use the following formats:
    - common name (CN)  
For example, user1
    - distinguished name (DN)  
For example, cn=user1,ou=people,dc=company,dc=com
- 3 Option 3: You can give access to users who are members of one or more groups in the directory service. To use this option:
  - a In the Allow remote administration for list, select Users from a directory service.
  - b Select Allow remote access for the following groups.
  - c Enter one or more group names. To specify multiple groups, enter a semicolon-separated list of groups. You can use the following formats:

- common names (CNs)

For example, group1 or group1;group2;group3

- distinguished names (DNs)

For example, cn=group1,ou=groups,dc=company,dc=com or

cn=group1,ou=groups,dc=company,dc=com;

cn=group2,ou=groups,dc=company,dc=com;

cn=group3,ou=groups,dc=company,dc=com

You do not need to use double quotation marks ("") even if the group name contains spaces. For example, group 1 or  
cn=group 1,ou=groups,dc=company,dc=com

**Emergency password.** Specify an emergency administration password for the tuner. Any user who specifies this password can administer the tuner.

Specifying an emergency password is useful in case the directory service is not available.

- 1 Select the Enable emergency password check box.
- 2 Enter an emergency password and confirm it.

## Working with SSL settings

If you want to ensure that communication between the Tuner Administrator and the tuner is secure and encrypted, you must obtain and install a Secure Sockets Layer (SSL) certificate on the machine that hosts the tuner.

---

Note: The administration tools mentioned throughout the rest of this section include Certificate Manager. The availability of Certificate Manager might be limited to a particular group of users in your company, such as system administrators.

---

To request and install a certificate, use Certificate Manager. Information for requesting, installing, and importing certificates, and for setting the certificate to be trusted for SSL, appear in the Certificate Manager Help (click the Help button from within Certificate Manager).

This section includes the following topics:

- “Enabling secure tuner administration” on page 346
- “Client-side certificates” on page 347

## Enabling secure tuner administration

You can enable secure (encrypted) administration of the tuner. To achieve this, you must import an SSL certificate into the tuner, enable secure administration for the tuner, and then use the secure tuner URL (starting with `https://` instead of `http://`) in Tuner Administrator.

To administer a remote tuner that has SSL enabled, the tuner running the Infrastructure Administration channel (which contains Tuner Administrator) must have the root certificate of the remote tuner in its certificate database.

### ► To configure a tuner to run in secure mode

- 1 Run Certificate Manager installed on the tuner, and import the SSL certificate (if you have not already done so). You must make sure that the root certificate is trusted for SSL.

For more information, see the Certificate Manager Help, available on the Marimba Channel Store.

- 2 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 3 After specifying the tuner you want to connect to, click Edit Settings.
- 4 Click the Security > SSL Settings tab.
- 5 Select the Use SSL Security check box.

You cannot select this check box if you do not have certificates installed.

- 6 From the SSL certificate list, select the certificate you want to use.
- 7 If you want, click View Certificate to see information about the selected certificate.

A new browser window appears and shows information about the selected certificate, including the serial number, valid dates, owner information, and issuer information.

- 8 In the Password field, specify the SSL certificate password and confirm it.
- 9 Select the Save SSL certificate password on tuner check box if you want to save and automatically use the password that you provided, so that you do not need to enter the password again when connecting to the tuner. The password is encrypted in the file system.

**Note:** If the password is not saved, then if the tuner is restarted, the tuner cannot enable SSL on its RPC port. You must then repeat this step.

- 10 From the Client certificates list, select one of the following options:

- Do not ask for client-side certificates
- Request client-side certificates, but do not require them
- Require client-side certificates

For more information, see “Client-side certificates” on page 347.

- 11 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 264.

**Note:** When you apply changes to the administration port SSL settings, Tuner Administrator warns you and disconnects from the tuner. If you want to continue administering the tuner, you must reconnect. If you have configured the tuner to use a secure port, remember to use `https` instead of `http` in the URL when connecting to the tuner.

## Client-side certificates

You can configure the tuner to require, request, or not ask for client-side certificates. Using Tuner Administrator, you can select one of the following options:

- **Do not ask for client-side certificates.** If you select this option, the tuner does not request certificates from clients (such as Tuner Administrator). However, the client must still provide the correct administration credentials (if required) to administer the tuner. For more information, see “Specifying remote administration access to the tuner” on page 341.
- **Request client-side certificates, but do not require them.** If you select this option, the tuner requests a client certificate. But if a client does not have one, the client can still access the tuner.
- **Require client-side certificates.** If you select this option, only clients that have a certificate can access the tuner. In this case, Tuner Administrator must have a valid client certificate to connect to the tuner. The Certificate Authority who issued the client certificate must match a root Certificate Authority that the tuner accepts.

# Tuner robustness service protection

The tuner has a protection mechanism that prevents users from terminating the tuner application through Service Control Manager and Task Manager. This protection mechanism is available to Windows users. The protection mechanism is disabled by default.

To enable the protection mechanism in the tuner, set the property `marimba.tuner.protect=true`. After the `marimba.tuner.protect` property is set, the tuner restarts automatically and applies the protection settings.

Enabling the protection mechanism has the following effect on the Service Control Manager and the Task Manager:

- **Service Control Manager:** If you have configured the tuner to run as an NT service on Windows, the **start** and **restart** options on the Service utility in the Control Panel are disabled, preventing users from stopping the tuner.
- **Task Manager:** The Task Manager does not display the `tuner.exe` tuner application, preventing users from killing the tuner application. However, `java.exe` and `minituner.exe` are not hidden from the user.

---

Note: If you have enabled the protection mechanism in the tuner, ensure that your applications do not depend on the existence of `tuner.exe` in the process list in Task Manager.

---

Note: Due to the nature of the tuner hiding feature, all the tuners running on that particular computer are affected if protection is enabled on a single tuner. In order to un-hide tuners, disable tuner protection by setting the following property: `marimba.tuner.protect=false`, for every tuner.

---

The user can stop the tuner indirectly in the following ways:

- **Tuner Quit through Tuner or Runchannel CLI Options**
  - **Tuner CLI:** The user can quit the tuner using the following tuner CLI option: `Tuner -quit -user <userName> -password <password>`

The credentials set on the tuner are authenticated when this CLI option is invoked.

- **Runchannel CLI:** The user can quit the tuner using the following runchannel CLI option: `runchannel -quit -user <userName> -password <password>`

The credentials set on the tuner are authenticated when this CLI option is invoked.

---

Note: Tuners that allow anonymous access do not require credentials.

---

- **Tuner exit through Tuner Icon:** The user can use the Exit option within Tuner Icon to quit the (Fully and Semi Interactive) tuner. If the tuner credentials have been set, specify those credentials in the dialog box that appears.

## Limitations

The tuner protection feature does not control the indirect ways to stop the tuner. Specifically, the tuner protection feature does not apply in the following cases:

- **Registry:** The tuner protection feature does not handle modifications to the registry values (externally).
- **Tuner Uninstall:** If the uninstallation property is set to `true`, the user can uninstall and thus indirectly stop the tuner.
- **Tuner as an Application:** The tuner protection applies only to the tuner running as a service, and not to the tuner installed to run as an application.
- **Startup Type options of the Service Control Manager:** The user can change the Startup Type of the Tuner Service to Manual/Disabled, thus indirectly stopping the tuner with the machine reboot. The tuner protection feature does not control this behavior.
- **Service Control Manager CLI delete option:** Executing the `delete` option of Service Control Manager CLI (via the `sc delete tunerServiceName command`), or running the `tuner -service uninstall` tuner usage command, deletes the Tuner service from the registry, and the service is not seen in the Service Control Manager. The tuner protection feature does not control this behavior.
- **Task Manager CLI - Taskkill:** The `prefs.txt` file contains the ID of the tuner. The user can use this ID to stop the tuner using the Taskkill CLI option of Task Manager. The tuner protection feature cannot prevent this.

- **Minituner:** When the tuner is in minimal mode, **minituner.exe** is visible in Task Manager. If the user stops **minituner.exe**, the Java tuner is launched.

## Tuner self-integrity check

The tuner has a self-integrity check mechanism that enables it to replace missing or changed tuner binaries before starting up. The self-integrity check mechanism also detects corruptions in the tuner's channel workspace and automatically fixes them.

The tuner self-integrity check mechanism operates under the following conditions:

- The self-integrity check does *not* occur when either **java.exe** or **minituner.exe** is running.
- The self-integrity check does *not* occur if **java.exe** or **minituner.exe** has exited with a valid exit code, as follows. A valid exit code implies that the tuner is behaving as expected, and an integrity check is not required.
  - exit code 0: stop the tuner
  - exit code 2: restart the tuner
  - exit code 4: going in/out of minimal mode
  - exit code 5: session migration
- The self-integrity check might occur if either **java.exe** or **minituner.exe** returned an abnormal exit code to the launcher. An abnormal exit code can be caused by a JVM hang, a forced minituner exit, forcible quit of the **java.exe** process, and other general errors.
- The self-integrity check happens only if one of the following conditions is met:
  - **java.exe** did not start properly, and stopped responding before it could do so.
  - If corruption of binaries was detected while the Java tuner was running.

If one of the preceding conditions is met, the tuner launcher performs an integrity check before handling the abnormal exit code. After the integrity check, the tuner launcher deals with the abnormal exit code in the usual manner (for example, on autorestart, **java.exe** is restarted after the hang, and when the minituner stops responding, the Java process wakes up).

---

Note: If **java.exe** starts properly and then hangs, it suggests an underlying issue that the self-integrity check mechanism cannot fix. In such cases, restarting the tuner is recommended.

---

When the self-integrity check occurs, the time taken to restart **java.exe** or **minituner.exe** is variable and depends on the time taken to fix the corruption.

# Advanced Tuner settings

This chapter describes the advanced tuner settings and how you can configure them using Tuner Administrator.

The following topics are provided:

- CMS UI Infrastructure Properties (page 353)
- Using a proxy with the tuner (page 357)
- Managing the bandwidth usage of the tuner (page 361)
- Specifying JVM arguments for the tuner (page 362)
- Viewing JVM properties (page 362)
- Specifying SNMP settings (page 363)
- Specifying ISM (Infrastructure Status Monitor) settings (page 364)
- Specifying vPro settings (page 365)
- Using the MESH feature to allow tuners to get content from peer tuners (page 366)
- Handling tuner corruptions (page 373)
- SMCA support for multihomed computer (page 379)
- Session isolation (page 380)
- Tuner behavior with session migration (page 386)
- Interactive Detection Service for Windows Server 2012 and Windows 8 (page 388)

# CMS UI Infrastructure Properties

## Introduction:

This is an enhancement to Common Management System where some more options are added to the UI to set properties from UI. Earlier all these properties had to be set through policy, command line or manually. You can now set the tuner properties by administer tuner or the properties can be set on profile. All Transmitter and proxy properties can be set by administer Transmitter and proxy.

## Pre-requisite

Infrastructure Administrator should be on 9.0.00 to configure properties from GUI.

## Tuner Administration

There is a list of Tuner properties that can be set through Tuner Administration ‘Advanced’. It is an enhancement in 9.0.00 where user can set properties through GUI instead of setting it through Command line or manually.

- 1 Network detection
- 2 Mesh
- 3 Architecture
- 4 Corruption
- 5 JRE
- 6 LWAC
- 7 Marimba Over Internet
- 8 Session Isolation
- 9 Network
- 10 User Centric Deployment
- 11 Inventory Plugin

1. **Network detection**- You can set Network detection policy from the drop-down list and some additional settings for network. You can set following network related property by selecting check box or by providing value.

Configure Network Detection

- Out going host
- Interval
- IP Delay
- Allow channels to update later after exited from sleep mode.

2. **Mesh** - Mesh functionality can be enabled\disabled by selecting check box in GUI. There are some additional settings that an user can do.
  - Mesh Broadcast Addr
  - Mesh Buffer Size
  - Mesh wait Tim
  - Allow tuner skips the File Peer Phase even when there are pending files after Channel Peer Phase
  - Allow files need for mesh.
- Note:** Tuner restart is mandatory in order for Mesh settings to be effective.
3. **Architecture:** Tuner architecture can be changed from 32-bit to 64-bit or vice versa through GUI by enabling\disabling check box at Tuner Administration page. You can also specify channel to user 32-bit segment. If this check box is enabled, tuner architecture will be 64-bit and if it is false, tuner architecture will be 32-bit.
4. **Corruption:** In order to monitor and repair tuner corruption, following settings can be done through GUI.
  - Tuner Repair Filter
  - Allow Infrastructure Service to check tuner workspace directory for corruption.
  - Allow Tuner to force update all corrupted channels.
  - Allow channel to update based on schedule even channel is corrupted.
5. **JRE:** By selecting this check box you can force tuner to use system JRE.
6. **LWAC:** Lite Weight Administration Console can be enabled or disabled by selecting check box. To access console you need to specify port number in “Lite Weight Tuner Administrator port”.
7. **Marimba Over internet:** You can enable\disable check box to allow operations over internet.
8. **Session Isolation:** Session isolation feature can be enabled or disabled from GUI by selecting check box on Tuner Administration page.
9. **Network:** User can Configure Network HTTP Timeout by specifying time in field. The connection will never get timed out only if the value is set to 0. The default value is 90.

All the above properties can be configured from setup & Deployment page while creating any profile.

## Advantages:

1. Property can be set through UI
2. No manual effort is required to set property.
3. There is no need to remember the property to be set, you just need to Enable\Disable property.

## Inventory Plugin

### **1. Enable Inventory Plugin Forward URL**

Enable/disable this option to enable plugin insertion or forward report to another inventory plugin URL in LAN(Local Area Network).

### **2. Handle Batch Exception**

If this option is enabled, plugin will try to insert the reports failing with primary key exception by forcing full report from the endpoint.

### **3. Dictionary Cache**

The memory caching mechanism introduced has the inserter plugins from 8.3.01 version onwards. This will hold all the dictionary objects (along with their ids) in an in-memory cache. Inventory plugin upon processing each node will try to locate the dictionary object by looking-up the cache with the list of field values that are used to locate a record. Check the box to enable this option.

### **Advantage:**

Database Procedure calls from the plugin can be avoided to a possible extent. With this cache in place, it will have a good impact while processing data to be inserted.

### **Disadvantages:**

- The memory and CPU load caused by the cache and its relatives. However the data will be limited as the cache holds only dictionary information.
- Plug-in start up will take more time as it has to initialize cache.
- Cache will be refreshed on a periodical basis and will have appropriate memory and CPU consumption.

#### 4. Patch History

This option enables the patch history related table data insertion.

**Warning:** If you enable this property and data is populated in database, performance or upgrade issues will occur during an upgrade in a later version of the database schema.

#### 5. Spilt Checksum Sync

This option splits the checksum file found in Inventory Plugin data directory in specified size in KB and send to lower tier (mirror/repeater). The default value is 4046 KB.

All the above inventory plugin properties can be configured from setup & Deployment page in Transmitter settings advanced tab while creating any profile.

**Note:** Restart the Tuner after setting plug-in property(s).

### Proxy Administration

A custom property tab is added in proxy administration to set or change property value from GUI.

### Transmitter

A custom property tab is added in Transmitter administration to set or change property value from GUI.

### Limitation

This UI change can only be seen with 9.0.00 infrastructure Administration.

# Using a proxy with the tuner

If your computer is behind a firewall (such as at most companies), and you use a proxy server to access the Internet, you can configure tuners to use the proxy. If you are not sure whether your computer uses a proxy server, consult the network administrator. You might also be able to find out by viewing the proxy settings for the web browser; consult the web browser help for more information.

You can configure settings for three types of proxy connections:

- HTTP is for standard HTTP proxies.
- HTTPS is for secure proxies using HTTPS (encrypted) communications.
- SOCKS is for any proxy using the SOCKS protocol.

---

Note: If you want to specify multiple proxies for failover, see “Specifying multiple proxies for failover” on page 359.

---

## ► To use a proxy with the tuner

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Edit Settings.
- 3 Click the Advanced > Proxy tab.
- 4 Select the Use a proxy check box.  
Important: If you want to specify more than one proxy, for fault-tolerance purposes, see “Specifying multiple proxies for failover” on page 359.
- 5 Enter information for the proxy that you want to use. For more information, see “Proxy settings for the tuner” on page 358.
- 6 If there are situations when you do not want the tuner to use the proxy, specify them in the Proxy Exceptions area. For more information, see “Proxy exceptions for the tuner” on page 358.
- 7 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 266.

## Proxy settings for the tuner

For each proxy type, you can set the following options:

- **Host** is the fully qualified name of the proxy server (for example, proxy.company.com).
- **Port** is a port number that the proxy server uses (for example, 1234).
- **(Optional) User name** is the name the tuner uses when accessing the proxy. Not all proxy servers require user names. For example, SOCKS proxies do not require user names.
- **(Optional) Password** is the password the tuner uses when accessing the proxy.

## Proxy exceptions for the tuner

You can set the following proxy exceptions:

- **Do not use HTTP or HTTPS for hosts that match.** Enter a comma-separated list of host names or domains that the tuner accesses directly (not through the proxy server). You probably want to exclude any transmitters that reside within the firewall. For example, to exclude three transmitters within your company, you might enter the following:

ny\_server.company.com, ca\_server.company.com,  
az\_server.company.com

- **Allow proxy to resolve hosts.** Select this check box to direct the proxy server to resolve the host name instead of the tuner. This is necessary if the firewall does not allow DNS lookups for hosts (transmitters) that are outside of the firewall. For example, if you access a transmitter that is outside the firewall, you might be required to allow the proxy to perform DNS lookups. This can be a security risk because you're trusting the proxy server to return valid host lookups. For example, if someone wanted to, they could program the proxy to return malicious or invalid IP addresses.

- **Do not use HTTP or HTTPS for unqualified host names.** Select this check box to direct the tuner to use normal network connections rather than the proxy server when communicating with transmitters that were not specified with a fully qualified domain name. For example, if your company has a transmitter called ny\_server, and you (or someone in your company) did not specify the fully qualified domain name (such as ny\_server.company.com) when subscribing to a channel. When you type only ny\_server, the tuner does not use the proxy server for that connection. In this way, the company can regulate network traffic that goes outside the firewall (for example, when you use a full host and domain name like ny\_server.company.com).

## Specifying multiple proxies for failover

If you want to specify multiple proxies for a tuner, you must specify some custom tuner properties along with enabling the User a proxy setting on the Advanced > Proxy tab.

### ► To specify multiple proxies for failover

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Edit Settings.
- 3 Click the Advanced > Proxy tab.
- 4 Select the Use a proxy check box.

Do not enter any more settings on this tab when you want to specify multiple proxies. If you do enter settings this tab, they take precedence over the custom tuner properties that you will set in step 6.

- 5 Click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 266.
- 6 Set the following list of custom tuner properties to specify multiple proxies:
  - marimba.proxy.http.list (for a list of HTTP-proxy hosts for proxy failover) or marimba.proxy.https.list (for a list of HTTPS-proxy hosts; that is, proxies to which you are making an SSL connection)

Set the property to a string that lists the proxies by using the form:

<host1>:<port1>;<host2>:<port2>;<host3>:<port3>

where <host1> is the host name of the first proxy, <port1> is the port number for the first proxy, and so on.

- `marimba.proxy.http.password` (if proxy authentication is required for connecting to an HTTP proxy) or `marimba.proxy.https.password` (for connecting to an HTTPS proxy)

Use this property only if proxy authentication is required. The valid value for this property a Base64-encoded string of the form:

<*user\_name*>:<*password*>

where <*user\_name*> is the user name, and <*password*> is the proxy password. This means that you need type the user name and password as shown, and then encrypt it to a Base64 encoded string, and then copy and paste that string into the property setting.

---

Note: The proxy password must be the same for all the proxies in the list.

---

- Other optional proxies properties might include `marimba.proxy.exceptions` and `marimba.proxy.notforunqualifiedhosts`. Descriptions of the properties and other proxy properties are provided in the *BMC Marimba Client Automation Reference Guide*, available on the Marimba Channel Store.

For more information, see “Adding tuner properties” on page 333.

# Managing the bandwidth usage of the tuner

You can specify how much of the available bandwidth you want the tuner to use when downloading channels and channel updates. You can manage the bandwidth usage using one of the following options:

- **All available bandwidth.** You can choose not to limit the amount of network bandwidth that the tuner uses.
- **Percentage of the bandwidth.** With this option, you specify the available bandwidth for the tuner based on the type of connection for the tuner. Then, you specify what percentage of that bandwidth is available for the tuner to use.
- **Maximum throughput.** With this option, you specify the maximum throughput that you want the tuner to use in kilobits per second (Kbps).

## ► To specify the bandwidth usage for the tuner

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Edit Settings.
- 3 Click the Advanced > Bandwidth tab.
- 4 If you do not want to limit the amount of network bandwidth that the tuner can use, from the Manage by list, select All available bandwidth.
- 5 If you want to specify the percentage of the total network bandwidth that the tuner can use, do the following:
  - a From the Manage by list, select Percentage of bandwidth.
  - b From the Available bandwidth list, select the type of network where the tuner is running. If the network type is not listed, use the one whose bandwidth is closest to yours. The bandwidth values are optimum settings, and the network available bandwidth is some number lower than this.
  - c In the Percentage to use field, specify the percentage of the bandwidth that the tuner can use. You can enter a value from 1 to 100. A value of 100 indicates that the tuner can use the maximum bandwidth for the specified network type (for example, 56 Kbps for a 56K modem).
- 6 If you want to specify the number of kilobits per second (Kbps) that the tuner can use, do the following:

- a From the Manage by list, select Maximum throughput.
  - b In the Use no more than field, specify the number of kilobits per second that the tuner can use.
- 7 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 266.

## Specifying JVM arguments for the tuner

You can use Tuner Administrator to pass arguments to the tuner Java Virtual Machine (JVM). You can use the arguments to change settings, such as the heap size of the JVM.

### ► To specify JVM arguments for the tuner

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Edit Settings.
- 3 Click the Advanced > JVM tab.
- 4 In the JVM arguments field, enter the arguments that you want to pass to the tuner JVM. Multiple arguments must be separated by spaces.
- 5 After you finish editing tuner settings, click Preview to review the changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 264.

## Viewing JVM properties

You can use Tuner Administrator to view properties of the tuner Java Virtual Machine (JVM). You can use the properties to diagnose and troubleshoot problems with the tuner.

---

Note: You can only view, not change, JVM properties using Tuner Administrator.

---

## ► To view JVM properties for the tuner

- 1 Use Tuner Administrator to connect to the tuner you want to configure as described in “Connecting to one or more tuners” on page 273.
- 2 After specifying the tuner you want to connect to, click Edit Settings.
- 3 Click the Advanced > JVM tab.

The JVM Properties table shows the property names and corresponding values. For example, if you must find the version for the tuner JVM, you can look for the `java.vm.version` property.

- 4 After you finish, click one of the other tabs to make any changes and then click Apply to confirm the changes and apply them to the tuner. For more information, see “Previewing and applying configuration settings” on page 264.

## Specifying SNMP settings

You can monitor your BMC Marimba Client Automation infrastructure (servers and endpoints) using SNMP.

If your SNMP agent has been configured with a port other than the default of 161, then you must change the value in **SNMP Agent Port** to match the new port number. You can set the **SNMP Agent Port** on the **Advanced > SNMP** tab in Tuner Administration.

This port receives SNMP data requests from SNMP managers such as the Infrastructure Status Monitor or a 3rd party SNMP manager.

The preferred method for changing the **SNMP Agent Port** is through a profile.

## Using a 3rd party SNMP manager

If you want to use a 3rd party SNMP manager to monitor your infrastructure, you can configure the settings in Tuner Administration on the server or endpoint that you want to monitor. Then you can access the data with the following request types:

- SNMP GET—retrieves statistics
- SNMP GETNEXT—iterates through the transmitter statistics
- SNMP GETBULK—requests multiple statistical values

- SNMP WALK—enables a manager to automatically traverse the transmitter statistics using a combination of SNMP GET and GETNEXT requests until the end of the tree is reached

### ► To configure SNMP monitoring using a 3rd party SNMP Manager

- 1 Log in to Tuner Administrator on the machine that you want to monitor or create a profile.
- 2 Ensure that no other product is using the default SNMP port of 161 or change the **SNMP Agent port** field on the **SNMP** tab.
- 3 On the **ISM** tab, find the **Server** field and enter the name of the host computer where the SNMP manager stores data. The SNMP manager is any third-party application that you use to get SNMP data.
- 4 On the **ISM** tab in the **Port** field, enter the port used by the SNMP manager to listen for SNMP notifications.

The default is 162. The port value you enter here sets the following tuner property: `snmp.manager.port`.

For information about SNMP monitoring using a 3rd party SNMP Manager refer to the *BMC Marimba Client Automation Transmitter and Proxy User Guide*.

## Specifying ISM (Infrastructure Status Monitor) settings

The Infrastructure Status Monitor provides health-related metrics about your BMC Marimba Client Automation infrastructure, including Master transmitters, Repeaters, Mirrors, Proxies, and Tuners. You can access the Infrastructure Status Monitor from the CMS console as described in Chapter 14, “Infrastructure Status Monitor.”

Before you can monitor a server or client machine with the Infrastructure Status Monitor, you must configure the ISM settings for that machine’s tuner. The preferred method for configuring ISM settings for tuners is through a profile as described in “Configure Infrastructure Status Monitor profile settings for server and client components” on page 204.

However, you can also configure these settings for individual machines through Tuner Administration as described in the following procedure.

## ► To configure ISM settings in Tuner Administration

- 1 In Tuner Administration, click the Advanced > ISM tab.
- 2 In Server, type the host name or IP address of the master transmitter on which the Logging Service is running.
- 3 In Port, type the dashboard port number. This can be configured to any valid port value. Default value is 162. Leave this field blank for proxy and client machines.
- 4 In URL, type the URL where Logging Service is running. For example:  
`http://<transmitter-or-loadbalancerhost>/ISM/LoggingService`
- 5 Under Component Reporting Schedule - Send Status, set the schedule for the components to send their status to the plug-in.
- 6 Configure other details in the profile as needed.
- 7 Click Preview and then Apply.

## Specifying vPro settings

By specifying Intel AMT vPro settings in Tuner Administration, you can allow BMC Marimba Client Automation to use vPro features to wake vPro PCs for policy updates and have the tuner shut them down afterwards. You can also launch the vPro management console from Tuner Administration, the Infrastructure Status Monitor Dashboard, or from the Machine Details page in Report Center.

---

Note: These features are also available for “pre-vPro” machines running Intel AMT 1.0.

---

The preferred method for configuring these settings for tuners is through a profile as described

## ► To specify vPro settings

- 1 From the Edit Settings page in Tuner Administration, click the Advanced and vPro tabs.
- 2 Provide information for the following fields:

- **User**—Enter a user name with credentials to access the vPro Management server.
- **Password**—Enter the password.
- **Management Port**—Lists the port number on which the vPro Management server is running. The port number is read and filled in automatically. You cannot edit this field.
- **Enable TLS**—Shows a check mark if you are using Transport Layer Security (TLS). You cannot change this setting here.

3 Click Preview and then Apply.

---

Note: You must restart the tuner for user name or password changes to take effect.

---

## Using the MESH feature to allow tuners to get content from peer tuners

The tuner's multi-endpoint synchronized host (MESH) capabilities enable you to reduce the number of dedicated servers required to maintain your BMC Marimba Client Automation infrastructure. When enabled, MESH allows a tuner on an endpoint to request content and provide that content to other endpoints. MESH enabled tuners can also replace proxies except when the proxy is used to route network traffic around a firewall.

Endpoints with MESH-enabled tuners first search for content in their own subnet rather than going directly to a mirror or repeater. This mechanism provides the following advantages over the conventional distribution mechanism:

- Without MESH, connections between endpoints in the same network can reach orders of magnitude of 1Gps or more. With MESH enabled, content obtained from adjacent endpoints could compare favorably against the time it takes to obtain content from servers sitting in different geographical locations.

- With MESH, the number of connections for content requests from a server could dramatically decrease, reducing load. Consequently, the number of servers required to service the same number of endpoints could be reduced, which reduces the costs associated with maintaining such servers in an organization.
- Based on detailed performance metrics when MESH is enabled on all the tuners in a subnet, it is possible to increase the number of managed endpoints without the need for adding new (mirror or repeater) servers to service those endpoints.

## Enable the MESH feature in tuners

### MESH architectural overview

After MESH is enabled, the BMC Marimba Client Automation infrastructure performs the following content distribution workflow.

At intervals, usually defined by the update.vary property, the following occur:

- A subset of endpoints makes content requests via a package's update schedule. This subset is the group of endpoints that are making content requests at the same time. Having multiple subsets (groups with different schedules) in the infrastructure can improve the performance of MESH distribution.
- New policies from the Policy Service request that additional packages be installed on endpoints. These endpoints go through the normal ADP mechanism for figuring out the details of the content to be downloaded from servers. The tuners go to the Transmitter to get the channel index. Prior to the MESH feature, all the endpoints would have gone back to the server for content download.

- Endpoints with the `marimba.tuner.p2p.enabled=true` tuner property set are MESH-enabled. When the endpoint is MESH-enabled, the tuner instead of directly communicating with the Transmitter to get the required files, initially enter a phase where it attempts to discover peers. This phase is divided into two sub-phases. The first sub-phase is known as Channel Peer Phase where the tuner broadcasts a UDP packet on a configured UDP port. You can use the `marimba.tuner.p2p.bcast.addr` tuner property to view or change the UDP port. The UDP packet contains the URL of the channel being updated or subscribed, and the root-level channel checksum. The second sub-phase is known as the File Peer Phase and is an optional phase.
- During both Channel Peer Phase and File Peer Phase, the tuner sends UDP packets and receives replies from other tuners depending on the availability of the channel or file. In Channel Peer Phase, MESH enabled send out a single UDP. MESH-enabled tuners receive the UDP packet (the tuners listen on the same address and port as configured using the `marimba.tuner.p2p.bcast.addr` property), and using the channel URL and checksum, determine if they have the required channel. If the tuners have the required channel, they reply back to the requesting tuner using UDP reply packets.
- During File Peer Phase, the tuners can select peers for downloading individual files that were not downloaded successfully during Channel Peer Phase. You can enable or disable the File Peer Phase using the `marimba.tuner.p2p.filepeerphase.disabled` tuner property. The File Peer Phase occurs only if the property is set to false or is not set, and if either no peers are found in the Channel Peer Phase, or not all files were downloaded during File Peer Phase. In this phase, the tuner calculate how many files of the channel were not downloaded at the end of Channel Peer Phase, and then broadcasts UDP packets, one for each required file. Other MESH-enabled tuners receive this packet, and check if they have the required file. If a MESH-enabled tuner has the required file, it sends UDP reply packets back to the tuner. In the File Peer Phase, three kinds of tuners can respond:
  - Tuners that are in full mode, and have the file.
  - Tuners that are in full mode, and are in the process of downloading the file.
  - Tuners in minimal mode and if they have the file.

- In both sub-phases, while handling the reply packets from the peers, the tuner classifies the tuners into separate categories. For each category, the tuner maintains the data of peers segregated in tables, because more than one tuner may have the required channel or file. The tuner waits for a default time of 15 seconds after sending UDP packets for the replies to come from the responding peer tuners. You can control the default waiting time using the `marimba.tuner.p2p.udp.waittime` tuner property. Once the waiting period has finished, the tuner iterates through each peer available and then connects to a specific peer and downloads the required files. This iterative process takes place till the following conditions are satisfied:
  - It has downloaded all the required files
  - It has searched all the available peers. Inspite of searching all the peers, if the tuner still needs to download files, the tuner connects to the Transmitter and download the required files. The tuner traverses each peer table in the following order:
    1. First peers that responded in Channel Peer Phase.
    2. Full mode tuners.
    3. Tuners that are currently downloading the required files.
    4. Tuners in minimal mode that have the required files.
- The first subset of endpoints get the required content from the server (the Transmitter), because there are no peers at that instant. However, when another subset of endpoints request for content, instead of going to the Transmitter, the endpoints actively query other endpoints in the network having the required content. After identifying endpoints from the first subset, the second subset of endpoints will then directly download content from the endpoints in the first subset. The Transmitter need not service any files to the second subset of tuners. Whenever updates are published to content on the transmitter, the updated files would also be obtained through this MESH mechanism.

In this way, content distribution is directed by both the Transmitters and all MESH-enabled endpoints in the organization. This MESH mechanism reduces the load on the servers and results in optimized usage of server resources. In addition, since content is now distributed within a network without explicitly needing local servers, the need for such servers is reduced. In situations where existing serviced endpoints in the network do not have the latest version of content, and when new endpoints request full downloads, the requests are distributed.

## MESH prerequisites/limitations

- To ensure that peers respond to UDP packets and reply back to the requesting tuner, they must share the same broadcast address and UDP port. The broadcast address and UDP port are determined using the `marimba.tuner.p2p.bcast.addr` property value.
- There is no load-balancing on peer tuners. When the peers are connected in MESH, the tuner attempts to download the maximum files available from that peer, and will only fail over to the next peer if it could not get all the required files.
- Files downloaded from peer tuners are streamed in full and uncompressed. As a result, it may take a little longer to download channels when MESH is enabled.

## Enabling the MESH feature in tuners

You enable MESH in tuners by setting tuner properties.

### ► To enable MESH in a set of tuners

- 1 Decide which endpoints you want to participate in MESH.

Not all endpoints have to participate in MESH, but the more endpoints that use MESH, the bigger the load reduction will be on traditional content servers (mirrors and repeaters). You could start by enabling MESH on a group of tuners in a particular subnet to test the results.

If you plan to enable MESH on many or all of your endpoint, you should consider splitting endpoints into groups that have different update schedules to improve the performance of MESH distributions.

- 2 Edit the profile for the set of tuners for which you want to enable MESH.
- 3 Add the following property in the profile to enable MESH:  
`marimba.tuner.p2p.enabled=true`
- 4 Determine if other properties need to be set:

- a By default, the `marimba.tuner.p2p.bcast.addr` property is set to `255.255.255.255:3323`. If you wish to change the broadcast address, add and set this property:  
`marimba.tuner.p2p.bcast.addr=broadcastaddress:UDP port.`
- b Set the `update.vary` channel property to true.  
For channels which are being updated using MESH, it is recommended to set the `update.vary` channel property to true.
- c Set the `update.vary.max` channel property.  
This property is used with `update.vary` and sets an update time offset in minutes. For example, if you set this value to “30,” the update will occur approximately 30 minutes later than the regular update time.

---

Note: Even when using the `update.vary` and `update.vary.max` channel properties, performance issues can occur with MESH in large environments when a large number of endpoints are being updated at the same time. In this situation, you can further improve performance by splitting endpoints into groups that have different update schedules.

---

## 5 Save the profile and update the Infrastructure Service.

After the Infrastructure Service update completes, MESH is enabled on the endpoints associated with the updated profile.

## Getting MESH status

When MESH is enabled, it sets the following informational properties which are listed in the `channel.txt` file in the channel directory for the tuner. These properties contain cumulative data for all the subscribe and update operations performed on a channel since you subscribed to it.

- **p2p.enabled:** Indicates whether the channel was last subscribed to or updated in MESH mode or not. Possible values are “true” or false.”
- **p2p.nopeers:** Indicates the total number of peers that the requesting tuner can communicate to, for downloading the files.
- **p2p.totalfiles:** Indicates the cumulative number of files requested since you subscribed to the channel for all the operations performed on the channel.

- **p2p.peerpc:** Indicates the average percentage of files that have been successfully obtained from peers. This value is updated after every channel update. The calculation for this metric is

(a/b) \* 100, where

a=number of files successfully downloaded from peers

b=total number of files successfully downloaded (whether from peers or a Transmitter)

The value range is 0 to 100. This value is set automatically (after calculation) on the first channel update. On subsequent updates, the calculated value is averaged with the last value (set for that channel property).

- **p2p.peername.filegroup:** Indicates which peers and transmitter were contacted for files, the total number of files requested, and the actual number of files successfully obtained since you subscribed to the channel. A typical value would be  
`p2p.peername.filegroup=peer1:8:8;peer2:4:2;peer3:5:3;tx:5:5` .
  - **p2p.tx.filegroup:** Lists the total number of files which were requested to be downloaded directly from the transmitter and the actual number of files successfully obtained since you subscribed to the channel. A typical value would be `p2p.tx.filegroup=20:20`.
- This channel property is deprecated.
- **p2p.file.nopeers:** Provides the number of tuners from which the tuner received at least one file.

# Handling tuner corruptions

The tuner:

- Recovers from the storage and channel corruption.
- Repairs storage database and inodes if a channel is corrupted.
- Repairs and updates the channel if it is corrupted.

You can use command-line options to repair the storage spaces that are corrupted.

When the tuner starts, it checks whether the `runtime.kernel.corruption.forcerestart` runtime property is set to `true`. If the property is set to `true`, the tuner starts the reconstruct process, and then repairs the channel. After the channels are repaired, the tuner updates the inconsistent channels.

While updating the channel, the tuner checks whether the `marimba.tuner.corruption.channels.forceupdate` tuner property is set to `true`. If the property is set to `true`, the tuner updates all those channels whose `corrupt` flag is set to `true`.

## Types of tuner corruptions

The tuner can get corrupted because of the following reasons:

- Inconsistent tuner

Inconsistencies can occur in the tuner when:

- The tuner binary files are missing or get corrupted.
- The tuner contains inconsistent binary files due to an incomplete upgrade of the binary files.

- Inconsistent storage space

Inconsistencies can occur in the storage space when:

- The index file is corrupt.
- The database file is corrupt.

- Inconsistent channel

Inconsistencies can occur in the channel when:

- Some of the files in the installation directory of the tuner are missing or corrupt.
- The channel failed to receive the updated **index.mrb** file from the server, or the **index.mrb** file is incomplete or corrupt.

**Note:** The tuner immediately updates the channel only when the **channel.verify.update** global property is specified. If you do not specify the global property, the tuner updates the channel according to a predefined schedule.

If you do not want to update a specific channel even when the channel is corrupted, use the **channel.verify.update=false** channel property to overwrite the **marimba.tuner.corruption.channels.forceupdate** tuner property for specific channels. If you set the **channel.verify.update** channel property to **true**, the channel updates according to a schedule. However, if the **corrupt** flag is set to **true** for the corrupted channels, then the tuner repairs the channels before updating the channels.

## Repairing various types of corruptions

### Repairing an inconsistent channel

To repair an inconsistent channel, use the following command-line options:

- **checkchannels**

When you use the **checkchannels** command on a running tuner, the **checkchannels** command performs the following actions:

- 1 Restarts the tuner.
- 2 Verifies the tuner storage.
- 3 Repairs the tuner storage.
- 4 Logs the details of the corrupted channels in the tuner's history log file.

**Note:** The **checkchannels** command does not immediately repair the corrupted channels, but the command repairs the corrupted channel only when the corrupted channel is subsequently updated or started. The storage verification process of the tuner, transmitter, or proxy, consists of the following two steps:

- 1 Verify

The verify step checks for the consistency of the inodes and database files.

The inode and database files are two parts of the storage structure. The inode file is similar to a lookup table (hash table), and the database file is the actual file where the data is stored. The storage structure may consist of multiple database files and only one inode file. The verify process checks whether all the entries in an inode have a corresponding reference in the database file, and then marks the inconsistencies.

## 2 Repair

The repair step uses any of the following techniques to ensure consistent storage structure:

- Remove incorrect references.
- Recreate the references.

`repairchannels`

When you use the `repairchannels` command on a running tuner, the `repairchannels` command performs the following actions:

- 1 Runs the actions of the `checkchannels` command
- 2 Instructs the tuner to check whether the corrupted channels satisfy both of the following conditions:
  - The `channel.verify.update` channel property is set to `true` for the corrupted channel.
  - The corrupted channel either does not have an update schedule, or if it has an update schedule, then the update schedule is not set to `never`.

If the corrupted channel satisfies both the conditions, the `repairchannels` command repairs and updates the channel. If either of the preceding conditions is not satisfied, the `repairchannels` command does not update the corrupted channel automatically.

`repairchannels force`

When you use the `repairchannels force` command on a running tuner, this command forces the tuner to update the corrupted channels automatically, even if the conditions specified in the preceding bullet point are not satisfied for the corrupted channels.

## Repairing an inconsistent storage space

To repair inconsistent storage space, you can use the following command-line options:

## repairWorkspace

You can use the repairWorkspace command on a running tuner to repair a corrupted storage space. This command restarts the tuner and triggers the actions required to repair the storage structure. Both repairWorkspace and fsck commands perform the same functions. However, you can use the repairWorkspace command on a running tuner to set the tuner properties, so that the command performs the repair process after the tuner restarts.

You must use the repairWorkspace command along with the runchannel command and the URL of the Infrastructure Service channel.

For example, `runchannel.exe <url of InfrastructureService> -repairWorkspace`

**Note:** The syntax of this command is case sensitive.

## fsck

You can use the fsck command only if the inode is consistent because the fsck command uses inode-related data to resolve the database references.

The fsck command resolves storage corruption problems that are caused by the following scenarios:

- Synchronization conflict when the tuner downloads data.
- Termination during storage operation, such as compaction.

**Note:** You must manually execute the fsck command. When the tuner detects that it must be started in fsck mode, the tuner's history log reports an appropriate message. However, if the tuner's `marimba.tuner.force.repair` property is set to `true`, the tuner restarts and automatically executes the reconstruct command.

## reconstruct

The reconstruct command resolves corrupted storage structure problems even when the inode that is specific to the tuner is corrupted. The reconstruct command uses the database to resolve the problems related to the corrupted inode. The reconstruct command deletes the inode and recreates the inode.

This command resolves the storage corruption problems that are caused by the following scenarios:

- The tuner is abnormally terminated.
- The data download is interrupted.

**Note:** The reconstruct command starts automatically when:

- The tuner recovers from an abnormal termination.
- The tuner receives a channel corruption notification.
- The tuner terminates abnormally during minimal mode or java mode.

The tuner receives a storage corruption notification for any channel and the `marimba.tuner.force.repair` tuner property is set to `true`.

You can also use the reconstruct command to manually start the tuner.

## Repairing a corrupted tuner

To repair a corrupted tuner, use `fixtuner` command.

- `fixtuner`

You can use the following parameters with the `fixtuner` command:

- `-proxy <host[:port]> [<user>:<passwd>]`
- `-socks <host[:port]>`
- `-recvRate <bytes_per_second>`
- `-sendRate <bytes_per_second>`
- `-auth <user>:<passwd>`
- `-timeout <ms>`

## Repairing a corrupted tuner

You can repair a corrupted tuner when the binary files of the tuner are:

- Missing
- Partly upgraded

You can use the following process to repair the binary files of a corrupted tuner:

- 1 Find a working tuner.
- 2 To create a Local Server Index (LSI) file, subscribe a channel on the working tuner.
- 3 Copy the LSI file and use the `fixtuner.exe` command to repair the broken tuners.

**Note:** You can use this process to upgrade the tuners to any version.

To repair a corrupted tuner, perform the following steps:

- 1 Obtain the **fix.zip** file from the BMC Support team.
- 2 Create a temporary folder.
- 3 Extract and copy the contents of the **fix.zip** file into the temporary folder.
- 4 Obtain the Golden Image Channel Archive (CAR) file.
- 5 Publish the Golden Image CAR file to the local transmitter.
- 6 Find a tuner that is working properly and which you can use as a golden tuner.
- 7 To create an **lsi.mrb** file in the tuner workspace, use the golden tuner to subscribe to the Golden Image CAR channel.
- 8 From the tuner workspace directory, copy the **lsi.mrb** file into the temporary folder.
- 9 Copy the **fixtuner.exe** file from the **tuner\lib** directory into the temporary folder, and then run the following command:

```
C:\fix> fixtuner -service Marimba -url https://localhost:9282/
<username>/InfrastructureService > output.log
```

**Note:** You must use the same URL (-url option) which you have used to create the golden LSI.

For example, if you have used a golden image channel on a 8101001 tuner, you must use the same infrastructure service URL to execute the **fixtuner** command.

If the tuner workspace and the lib location are different, use the **-libPath** command to specify the path of the **lib** directory.

In case you already have **fixtuner** present in the tuner lib directory:

- 1 Copy the **lsi.mrb** from the following tuner workspace:  
**tuner\marimba\<Tuner\_name>** to **tuner\lib** directory.
- 2 Execute the following command line from **tuner\lib** directory

```
C:\Tuner\lib> fixtuner -service Marimba -url https://localhost:9282/
<username>/InfrastructureService > output.log
```

# SMCA support for multihomed computer

## Multihomed computer

A computer with more than one network interface card (NIC) and connected to more than one network is known as a multihomed computer. If a computer has multiple NICs but is attached to only one network, then it is not known as multihomed. A computer must be connected to more than one network if it has to be multihomed. The standard home version of a multi-homed computer connects to the Internet and also connects separately to a local network.

## Support for multihomed computers

SMCA offers limited support for multihomed computers. A multihomed computer can have more than one SMCA server and can still use its basic capabilities, so that you can exploit the features of high end servers. The SMCA tuner has the capability to bind to a specific outgoing host for all outgoing communications. You can use the `marimba.tuner.outgoing.host <string null>` property to configure the binding to a specific outgoing host. The tuner's `HTTPEnvironment` interface uses this property to configure the default outgoing IP address. Most non-RPC outgoing tuner connections use the value configured in this property as the outgoing address. It is useful to configure this property when you use multihomed computers with multiple (virtual or non-virtual) IP addresses.

This property allows:

- The tuner to bind to one of the available NICs and use it for all communication.
- Multihomed computers to have multiple tuners so that the Report Center can report the tuners as different entities.

## Limitations of using multihomed computers

The limitations of using multihomed computers are:

- SMCA offers limited support for multihomed computers.
- SMCA provides limited ability to manage the agents. Infrastructure Administration can connect to only one of the tuners, or the Server channel running over the Infrastructure Administration.

- It is strongly recommended to keep different tuners running on different Infrastructure channels. You can have multiple transmitters on a multihomed computer but ensure that the transmitters run on separate tuners.
- It is not recommended to run more than one Infrastructure channel over a single tuner. For example, Infrastructure channels like Transmitter, Proxy, and CMS.
- Report Center reports the tuners in a multihomed computer under one computer entry.
- SMCA does not support client profile on multihomed computer.

## Session isolation

### Background information

Prior to introduction of the Session Isolation feature, SMCA handled the isolation of services from user interface (UI) elements in Windows Vista and above platforms by a process called session migration. The session migration process involved stopping the tuner and restarting it in the newly logged on user's session. This process ensured that the UI was visible to the user, however this process resulted in the need for the tuner to maintain the state of ongoing requests and activity, which was not always successful and resulted in problems like tuner corruptions and sometimes the UI incorrectly displayed.

The session isolation feature aims to overcome all the overheads and complications of the earlier technique. The session isolation feature uses the Microsoft recommended approach of separating the UI components from the service application. The tuner along with the dependent java process continuously runs in session 0 irrespective of any user activity like user log on.

The marimbaclient.exe is a new executable that triggers the java process and which then encapsulates the UI functionality for marimba tuner. It also interacts with the tuner and handles all communication and events between the tuner and the UI.

## Architecture of Session Isolation

In Windows operating systems like Windows Vista and above, the Windows services run in the first session of the operating system (OS). The first session of the OS is also known as Session 0. The users who are logged on to the OS operate in separate user sessions, thus effectively isolating them from Windows services.

When session isolation is disabled, the tuner operates in session 0 while the Java executable operates in the logged in user's session. The tuner handles session change events by session migration. When a session event like a user log-in or log-off occurs, the tuner forces the java process to quit, and then restarts the java process in the new user session. This functionality ensures that the Tuner can collect the logged-on user's information, and display user interfaces like dialogs in the logged-on user's session. However, in this design the Java executable stops and restarts whenever a session event occurs. Session Migration also handles cases like interrupted operations, delays to allow critical functionality to complete, and down-time in tuner operations.

### Tuner operations when session isolation is enabled

The tuner operates in session 0, however the UI component of the tuner or the Marimba Client operates in the logged in user's session. The tuner does not enter the user session. The advantage of session isolation feature ensures that the tuner need not stop and restart whenever a session change occurs. This features effectively handles the following user log on and log off scenarios:

- User log on and log out
- Multiple users logged on, thus handling active and disconnected users
- Tuner Icons in every session
- Marimba client executable in every active or disconnected session.

The tuner runs silently and handles tasks such as triggering events like channel updates and stats reports on schedule, and hosting tuner services that are responsible for UI events like CRS and UCS. The Tuner services send instructions to the Marimbaclient.exe.

## About Marimba Client

The Marimba Client module is an executable which handles the user interface elements of the Tuner. Marimba Client supports both the user interface interactions from the users, and the UI elements which are initiated within the tuner or by channels hosted on the tuner. Since the Marimba Client launches its own JVM, it uses a maximum memory of 128 Mb.

The Marimba client handles all interactions with the tuner and acts as an interface between the tuner and the user. The Marimba Client executable starts on an endpoint only if session isolation is enabled on the endpoint. The tuner icon now includes an additional Manage option which you can use to open the Lite Weight Tuner Administrator console.

The Marimba Client executable operates if the tuner is configured in fully-interactive or semi-interactive mode. the Marimba Client auto starts on log on using a Windows registry key.

You can enable session isolation on an endpoint by setting the **marimba.tuner.sessionisolation.enabled** tuner property. When session isolation is enabled on an endpoint, the tuner and Java executable operate in session 0, while the Marimba Client operates in the active or disconnected user's session. The marimba client starts whenever a new session starts. If the session ends or the user logs off, the Marimba Client executable for this session quits.

---

Note: Once you disable session isolation, the tuner reverts to pre-8.3.0.0 functionality.

---

Marimba client does not handle the UI for server channels like Application Packager, Channel Copier, Certificate Manager, Channel Manager, and Publisher.

---

Note: When Session Isolation is enabled, custom channels which do not use the UI elements provided by the Tuner, and use separate and complicated UI elements may not work properly. If the custom channel uses only the UI components provided by the tuner like UCS and CRS, then the custom channel will work properly when session isolation is enabled.

---

## Workflow of Session Isolation

The following is the workflow of Session Isolation feature:

- 1 If Session Isolation is enabled, the tuner and java executable start in session 0.
- 2 When a new session starts, the new Marimba Client executable starts in the new session.
- 3 Marimba Client handles all user interactions like icon events, CRS dialogs, UCS dialogs, scan permission and progress dialogs, information dialogs, and package installations.
- 4 If the session ends or the user logs off, the Marimba Client executable for this session quits.

---

Note: The Marimba Client will also quit whenever the tuner quits. On tuner restart, Marimba Client will also restart.

---

## Session Isolation for minimal mode tuner

In tuner minimal mode, if session isolation is enabled, the minituner.exe runs in session 0. The minituner interacts with the Marimba Client to check for icon tuner events.

## Platform support

SMCA supports Session Isolation only on Windows operating systems. Session isolation supports the following Windows operating systems:

- Windows 8
- Windows 8.1
- Windows 7
- Windows Vista
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2008
- Windows 8 Embedded

## Limitations

- Server type of channels like Application packager, Channel Copier, Publisher, Channel Manager, and Certificate Manager, and custom UI channels do not run with session isolation because of Interactive Services Dialog.
- If the packages created using Application Packager version prior to 8.3.00 are deployed on a tuner which has the `marimba.packages.autoupgrade` tuner property set to false, Session Isolation does not work properly. It is recommended to disable Session Isolation if this tuner property is set to false.
- In operating systems like Windows Server 2003, Windows Server 2008, and Windows Server 2012, which support simultaneous logged in users, when Session Isolation is enabled, and operations involving UI events like a package installation, or CRS/UCS are triggered, the associated UI dialog will pop up in all the logged in users' sessions. Since all such users are capable of interacting with the UI simultaneously, this behavior will cause unpredictable results. This limitation does not apply to operating systems where only one user is active at a time and other users are in a disconnected or logged off state.
- When Session Isolation is enabled, the marimba client may fail to start if the `-Dcom.sun.management.jmxremote.port` Java argument is added as part of the tuner's start up arguments. This option is usually specified when the tuner is being analyzed for memory leaks using the VisualVM tool.
- If session isolation is enabled, and when a user clicks right-clicks the tuner icon and clicks on one of the menu options that appear in the context menu, the dialog prompting for admin credentials appears in all logged in user sessions.
- When session isolation is enabled on a tuner hosting a Transmitter, Proxy, or CMS, the icon associated with the Transmitter, Proxy, or CMS fails to appear in the user session.

## Prerequisites

- Ensure that the tuner is running as a service.
- Set the `marimba.tuner.sessionisolation.enabled` property to true.
- Ensure that the following channels are upgraded to 8.3.0.0

- Inventory Service
- Subscription Service
- To avoid the Interactive Services Dialog, it is recommended to disable session isolation on computers on which server type of channels run. Server type of channels include:
  - Application Packager
  - Channel Copier
  - Publisher
  - Channel Manager
  - Certificate Manager

## Enabling Session Isolation

You can enable Session Isolation by using the following property:  
`marimba.tuner.sessionisolation.enabled`

To enable Session isolation, set the `marimba.tuner.sessionisolation.enabled` property to true and restart the tuner. Once the tuner restarts, the tuner and Java executables launch in Session 0 and Marimba Client starts in the current logged-on user session.

## Disabling Session Isolation

To disable session isolation, set the `marimba.tuner.sessionisolation.enabled` property to false and restart the tuner.

## Log messages and debug information

The log messages specific to session isolation include the `marimbaclient` notification text in the log message.

For example:

```
[03/Oct/2013:11:42:39 +0530] - info insbishihoi 1001 Kernel arguments received: marimbaclient notification: icon_open  
[03/Oct/2013:11:43:20 +0530] - info insbishihoi 1001 Kernel arguments received: marimbaclient notification: tuneractions_perms_input
```

## Debug flags

To get debug information, set the following debug flag:

- TUNER/MARIMBACLIENT

## Tuner behavior with session migration

This tuner behavior is applicable to only 8.1.01.006, 8.2.00, or later.

---

Note: SMCA supports session migration only on Windows Vista and Windows 7 platforms. For platforms where session migration is not supported, if the tuner is configured in full or semi-interactive mode and the tuner is running in session 0, and if the user logs in that machine, then the user cannot see the tuner icon in the system icon tray. This behavior was observed on Windows XP SP3, Windows 2003, and Windows 2008 server.

---

## Session affinity property

If you set the marimba.tuner.session.affinity property to true, the tuner icon does not appear in any user session. All tuner dialogs, and the Channel Manager appear in session 0. The user can view these interfaces only if the Interactive Services Detection service is running. If session affinity is enabled, the tuner does not restart abruptly when a user logs on or logs off.

The following table describes the behavior of the tuner based on the value of the marimba.tuner.session.affinity property:

### Tuner is started in session0 automatically

---

marimba.tuner.session.affinity	No User logged-in(Session0 in(	User1 login(sessi on1)	User2 login(sessi on2)	Log-off User2	Log-off User1	Login Again(say session1)
--------------------------------	--------------------------------------	------------------------------	------------------------------	------------------	------------------	---------------------------------

---

**Tuner is started in session0 automatically**

True	java.exe	In session0	In session0	In session0	In session0	In session0	In session0	In session0
	tuner.exe	In session0	In session0	In session0	In session0	In session0	In session0	In session0
	tuner restart	Not Applicable (NA)	NO	NO	NO	NO	NO	NO

False	java.exe	In session0	In session1	In session2	In session1	In session0	In session1	
	tuner.exe	In session0	In session0	In session0	In session0	In session0	In session0	In session0
	tuner restart	Not Applicable (NA)	YES	YES	YES	YES	YES	YES

**Tuner started manually in a user session**

marimba.tuner.session.affinity	No User logged-in(Session0 )	User1 login(session1)	User2 login(session2)	Log-off User2	Log-off User1	Login Again(say session1)		
	java.exe	Tuner not yet started	If tuner started here, in session1	In session1	In session1	In session0	In session0	
	tuner.exe	Tuner not yet started	If tuner started here, in session0	In session0	In session0	In session0	In session0	
	tuner restart	Not Applicable (NA)	NA	NO	NO	YES	NO	

## Tuner started manually in a user session

False	java.exe	Tuner not yet started	If tuner started here, in session1	In session2	In session1	In session0	In session1
	tuner.exe	Tuner not yet started	If tuner started here, in session0	In session0	In session0	In session0	In session0
	tuner restart	Not Applicable (NA)	NA	YES	YES	YES	YES

## Interactive Detection Service for Windows Server 2012 and Windows 8

By default, in Windows Server 2012 and Windows 8, Interactive Service Detection Service is disabled. If you want to access a fully interactive tuner running in service session, you must enable this service to get the Interactive Service dialog to switch to service session. To enable the Interactive Service Dialog box in user session, perform the following steps.

**Note:** You must have administrator rights to perform the following steps.

### ► To enable the Interactive Service Dialog box in user session

- 1 Set the marimba.tuner.interactiveservicesdialog.enable tuner property to true.
- 2 If the startup type of Interactive Service Detection Service is set to Manual, use Service Control Manager to change the start type to Automatic.

Open Service Control Manager in the Windows operating system, locate the Interactive Service Detection in the list of services. Right-click on the service and open the properties. The Interactive Service Detection Properties dialog appears. In the **Startup type** list, select **Automatic**, and click **Ok**.

- 3 Restart the tuner.

After the tuner is restarted, the registry is modified to enable the Interactive Detection Service on the computer. You can view the following confirmation log message in Tuner's History Log file which requests for system reboot:

1037 Kernel will activate Interactive Services Dialog via registry, but the machine must be rebooted in order to complete activation message.

- 4 Restart the computer.

Chapter

# 22 Tuner background information

The following topics are provided:

- Tuner diagnostics (page 384)
- Tuner logging (page 389)
- Tuner background (page 396)

## Tuner diagnostics

You can get different diagnostic reports, depending on the level and type of information you need.

- advancedDiagnose.bat file — captures the thread dump of the tuner
- Status report — general information; checks if the tuner is running
- Debug report — specific information; checks for problems with the tuner
- Log report — tuner and channel history logs

If the remote tuner RPC port is SSL-enabled, enter `https://` in the browser; if not, enter `http://`. This is shown in procedures and examples as `<http|https>://`.

**Tuner access.** If the tuner is not configured to allow anonymous access, then you must log in before you can access any diagnostic reports. The browser prompts you the same way as when you access an access-controlled web server. You must authenticate to the tuner using the same set of credentials that you use with Tuner Administration.

The console and the transmitters do not have to be running to generate a tuner status report. Any version 7.0 tuner, even one with no subscribed channels, can generate reports.

**Minimal mode and SSL.** On Windows, if you try to retrieve tuner diagnostics using the browser and the following conditions are met for the remote tuner

- In minimal mode
- RPC port is SSL enabled

then the browser displays an error message stating that no diagnostics are available until the tuner wakes up from minimal mode. Tuners that have secure RPC ports, however, are typically server endpoints, for example, a transmitter, which never go into minimal mode.

If the RPC port is not secure, or if the tuner is not in minimal mode when you try to connect using the browser, then this is not an issue.

**Disabling tuner diagnostics.** You can disable the tuner diagnostics by setting the `marimba.tuner.status.enable` property to `false`. By default, the property is set to `true` so diagnostics are available.

## Using advanceddiagnose.bat

The advancedDiagnose.bat file captures the thread dump of the Tuner. You can find this batch file in the tuner directory. Ensure that you run this batch file from the same session in which java.exe runs. The advancedDiagnose.bat file does not capture the thread dump when you run the command in a session which is different from the session in which java.exe runs.

For example, if java.exe is running in session 0, then you can execute the advancedDiagnose.bat file from a command prompt where the command prompt also runs in session 0. If you want to run a command prompt in session 0, you can use the psexec.exe command. For example, the psexec.exe -s cmd.exe command launches the command prompt in session 0 and under SYSTEM users context.

## Status reports

A status report contains general information about a tuner, and tells you if the tuner is running. A status report includes the tuner version, the release date, the VM version, the heap-size, arguments, and operating system information.

Status reports are returned to a browser in XML.

For example:

```
<?xml version="1.0" encoding="UTF-8" ?>
- <tuner-status host="acme-xp/000.00.00.000" timestamp="Fri, 27 Jan
2006 09:49:30 PST" port="7717">
- <tuner>
    <param name="version" value="7.0" />
    <param name="release-date" value="2006/01/18 18:04:50" />
</tuner>
- <vm>
    <param name="vendor" value="Sun Microsystems Inc." />
    <param name="version" value="1.4.2_08" />
    <param name="thread-count" value="21" />
    <param name="heap-total" value="10551296" />
    <param name="heap-available" value="1581008" />
    <param name="arguments" value="-Xdebug" />
</vm>
- <os>
    <param name="name" value="Windows 2000" />
    <param name="version" value="5.1" />
    <param name="architecture" value="x86" />
</os>
</tuner-status>
```

## ► To generate a status report

To generate a status report, use the following format. You cannot set any options.

- `<http|https>://<host>:<rpcport>/?status`  
where *host* is the host machine and *rpcport* is the RPC port number.

## Debug reports

A debug report collects information about specific areas of a tuner, useful when you think there might be a problem with the tuner. You can select options, which correspond to tuner objects (features), for the report. One use for a debug report to get information to send to Technical Support when you open a support case.

Debug reports are available only with a working RPC port. If a tuner is not working because of a problem with RPC itself, then you can get debug information by running `tuner -getDebug <file>` where `file` is the file to which you want to write the debug information. If you want only threaddumping information, run `tuner -getDump` (written to the tuner log file).

Debug reports are returned to a browser in XML.

## Threaddumping

You can get threaddumping information remotely from both client endpoints and servers.

### ► To generate a debug report

To generate a debug report, use the following format:

- `<http|https>://<host>:<rpcport>/?debug[options]`  
where `host` is the host machine, `rpcport` is the RPC port number, and `options` request specific information.

If no options are specified, then a full debug report is generated.

You specify options by setting them to true or false. Use an & (ampersand) to separate the options; do not include spaces between the options.

- `&<option>=t` includes the option
- `&<option>=f` excludes the option

For example, to include only the config and workspace options, use  
`https://<host>:<rpcport>/?debug&config=t&workspace=t`

For example, to include all information but exclude the workspace option, use `https://<host>:<rpcport>/?debug&workspace=f`

The options for a debug report are:

- config – tuner properties (combination of properties.txt and prefs.txt)
- internal – runtime information about the Java VM and tuner, storage and thread pools
- launcher – information about applications; for example, running channels
  - mrbmacprops – machine ID for Intel AMT
  - rpc – RPC configuration and connections
  - scheduler – when events (channel start, update, and so on) are going to occur
  - threaddump – information about all Java threads (written to the tuner log file)
  - workspace – information about tuner logs and channels in the workspace
  - vm – information about the VM itself
- netstat – the output from running a `netstat -an` command

## Log reports

Log reports contain the tuner and channel history logs. You can download them remotely. The logs are returned as a zip file.

To generate a tuner log, use the following format.

- `<http|https>://<host>:<rpcport>/workspace?log[=<name>]`  
where `host` is the host machine, `rpcport` is the RPC port number, and `name` is a specific tuner.

For example, to generate all tuner logs, enter `https://pluto:7717/workspace?log`. To generate only the `history-1.log` tuner log, enter `https://pluto:7717/workspace?log=history-1.log`.

To generate a channel history log, use the following format.

- `<http|https>://<host>:<rpcport>/workspace/<channelURL>?log[=<name>]`  
where `host` is the host machine, `rpcport` is the RPC port number, and `name` is a specific channel.

For example, to generate all channel history logs for the entered channel URL, enter `https://pluto:7717/workspace/<URL>?log`. To generate only the `history-1.log` channel history log, enter `https://pluto:7717/workspace/<URL>?log=history-1.log`.

## Tuner logging

Each tuner maintains log files for the tuner and the channels on it. The log files contain information about events such as starting the tuner and subscribing to a channel, as well as any problems associated with those events. There are three types of log files maintained by the tuner (described in more detail later in this section):

- “Tuner history logs” on page 398
- “Tuner audit logs” on page 399
- “The individual channel history logs” on page 401

In addition, certain channels, such as the transmitter, generate log files that contain information specific to that channel. Depending on the channel, there can be different ways of controlling whether log files are generated and how the log files are rolled. For example, you can use Transmitter Administration to control how the transmitter log files are rolled. (For more details about transmitter log files, see the *BMC Marimba Client Automation Transmitter and Proxy User Guide*.)

The information in the log files includes the log ID, the corresponding log message, and the severity level. You can use this information to monitor and troubleshoot problems with your system.

For a list of the logging information (log ID, the corresponding log message, and the severity level) that appears in the log files, see the *BMC Marimba Client Automation Reference Guide*, which is available from the Marimba Channel Store.

## Platform-specific log files

Additional log files exist on particular platforms only.

## UNIX tuner.log file

On UNIX, the `tuner.log` file records events about the tuner (the tuner's standard output is redirected to this file when you start the tuner using `-start`). The `tuner.log` file rolls

The log files are named by the order in which they are created. For example, the first log file is named `tuner-1.log`, the second one `tuner-2.log`, and so on.

## Windows only log files

On Windows, the tuner workspace directory can contain the following Windows-only log files:

- `stdout.log`, which contains standard output that is stored to this file if it is not directed to a console.
- `launch.log`, which contains information about the tuner when it goes into minimal mode.

There is no default value to this property. By default, the `launch.log` file is always created in the tuner workspace only on the Windows platform.

When you set the value of the `marimba.launch.logFile` property to “no”, no launch file is created in the tuner workspace. Setting any value other than “no” to the `marimba.launch.logFile` property does not affect the default behavior of creating the launch file.

You can specify the amount of detail in this log file by setting the tuner property `marimba.launch.logLevel`. For more information, see the tuner properties chapter of the *BMC Marimba Client Automation Reference Guide*, available on the Marimba Channel Store.

**Best practice for managing platform-specific log files:** Currently, there is no automatic way to roll the `stdout.log` file on Windows. Depending on how much log information the tuners and channels generate, you should manually roll the log files by stopping the tuner, renaming the log files, and restarting the tuner so that the files do not grow to an unmanageable size.

For example, if the log files typically grow to a certain size every week, you might want to rename the log file by adding the date (`stdout_20031212.log`) every week. Then, you restart the tuner so that it creates a new `stdout.log` file. On Windows, you should follow this best practice for tuners that host server components such as transmitters, proxies, and other channels that typically must run all the time. Typical desktop tuners go into minimal mode when no channels are running, which allows the `stdout.log` file to be truncated.

## Tuner history logs

The tuner `history.log` files record tuner events, such as when a tuner subscribes to or starts a channel. The files are located in the tuner workspace directory. For more information, see “Tuner workspace directory” on page 250.

The log files are named by the order in which they are created. For example, the tuner’s first log file is named `history-1.log`, the second one `history-2.log`, and so on.

The log files begin with a four-line header:

- Host — The name of the host machine on which the tuner is installed.
- Created — The date the log was created. You can ignore the long code number at the beginning of the line.
- Version — The version field is not used right now, so you can ignore it.
- Roll — The log-rolling policy for this log file, including the frequency of rolling, the maximum size of the log file, and the number of previous log files that can exist.

For example:

```
Host: acme
Created: 975534251518; Wed Nov 26 13:44:11 PST 2003
Version: 0
Roll: bysize,128;1
```

The actual log entries vary depending on the event recorded. Usually, they include the following information about each entry:

- The date and time
- The severity level
- The user ID

- The log ID
- The log message

If you turn on debugging, you might see additional information (usually preceded by #).

For more details about the log IDs and severity levels, see the logging codes chapter of the *BMC Marimba Client Automation Reference Guide*, which is available from the Marimba Channel Store.

Here are some examples of log entries:

```
[26/Nov/2003:13:44:11 -0800] - audit spiky 1000 Kernel started
[26/Nov/2003:13:44:11 -0800] - audit spiky 1718 Certificate
issuers updated: c:\Program
Files\BMC_Software\BBCA\Tuner\.marimba\Marimba\certDB
[26/Nov/2003:13:44:11 -0800] - audit spiky 1400 RPC listener
started: ServerSocket[localport=7717]
[26/Nov/2003:13:44:11 -0800] Storage audit spiky 13100 Storage
opened: c:\Program
Files\BMC_Software\BBCA\Tuner\.marimba\Marimba\store
[26/Nov/2003:13:44:11 -0800] LicenseManager audit spiky 1600
License Manager has been initialized
e:\Tuner_Workspace\.marimba\Marimba4610\ch.2\data
[26/Nov/2003:13:44:42 -0800] LicenseManager audit spiky 1601
Trying to get license for: Marimba Transmitter 6.0
[26/Nov/2003:13:44:48 -0800] LicenseManager audit spiky 1603
Installed license for: Marimba Transmitter 6.0
```

## Tuner audit logs

The tuner workspace directory also contains an audit log that is populated with messages that contain the “AUDIT” severity level from the tuner and channels. Audit logs are named by the order in which they are created. For example, the first audit log file is named `audit-1.log`, the second one `audit-2.log`, and so on.

An audit log entry contains the following information:

- time stamp for when the message was logged
- severity level (AUDIT)
- user ID
- message ID

- message text
- 

Note: There are a few UI parameters which are derived from more than one property value. In such cases, the audit log will show that more than one parameter has changed.

There are some properties which are not present in the files but are needed for display in the UI with default values. These properties may be listed as changed properties even though a user has not necessarily changed them.

---

## Controlling how tuner logs roll

You control how the `tuner.log`, `history.log`, and `audit.log` files are rolled by using the following tuner properties:

- `marimba.tuner.logs.roll.policy`

This property specifies the policy for rolling the tuner log files. You can set it to one of the following values:

- hourly
- daily
- weekly
- monthly
- yearly
- manually
- never

If you choose `manually` or `never`, the log entries are recorded in a single file, which is never automatically rolled.

- `bysize` (Default)

If you choose `bysize`, the log file is rolled automatically when it reaches the size specified in `marimba.tuner.logs.roll.size`.

- `marimba.tuner.logs.roll.size`

This property specifies the size in kilobytes the tuner log file must reach before it is rolled automatically. By default, it is 128 kilobytes. The value of this property is used when `marimba.tuner.logs.roll.policy` is set to `bysize`.

- `marimba.tuner.logs.roll.versions`

This property specifies the number of previously rolled log files that can exist for the tuner. By default, it is 1. If you set the value to 0, all versions are kept.

## The individual channel history logs

Each channel that the tuner has subscribed to has `history-n.log` files. The log files record channel events, such as when a channel is started or updated. The files are located in each channel directory inside the tuner workspace directory. The channels' directories are numbered by the order in which the tuner subscribed to the channels. (The first channel subscribed to has the `ch.1` directory, the second one the `ch.2` directory, and so on.) To find out which directories correspond to which channels, use the `map.txt` file in the tuner workspace directory. For more information, see “Tuner workspace directory” on page 250.

The log files are named by the order in which they are created. For example, the channel first log file is named `history-1.log`, the second one `history-2.log`, and so on.

## Controlling how the channel history logs roll

You control how the log files for all the channels in the tuner are rolled by using the following tuner properties:

- `marimba.logs.roll.policy`

This property specifies the policy for rolling the log files for all the channels in the tuner. You can set it to one of the following values:

- `hourly`
- `daily`
- `weekly`
- `monthly`
- `yearly`
- `manually`
- `never`

If you choose `manually` or `never`, the log entries are recorded in a single file, which is never automatically rolled.

- `bysize` (Default)

If you choose `bysize`, the log file is rolled automatically when it reaches the size specified in `marimba.logs.roll.size`.

- `marimba.logs.roll.size`

This property specifies the size in kilobytes the log file must reach before it is rolled automatically. By default, it is 32 kilobytes. The value of this property is used when `marimba.logs.roll.policy` is set to `bysize`.

- `marimba.logs.roll.versions`

This property specifies the number of previously rolled log files for the channel that can exist. By default, it is 1.

There are equivalent channel properties for controlling the log files (`logs.roll.policy`, `logs.roll.size`, `logs.roll.versions`). The channel properties take precedence over the tuner properties.

## Reading a channel history logs

The log files begin with a five-line header:

- Host — The name of the host machine on which the tuner is installed.
- Created — The date the log was created. You can ignore the long code number at the beginning of the line.
- Version — The version field is not used right now, so you can ignore it.
- Roll — The log-rolling policy for this log file, including the frequency of rolling, the maximum size of the log file, and the number of previous log files that can exist.
- Source — The channel URL.

For example:

```
Host: acme
Created: 975534525432; Wed Nov 26 13:48:45 PST 2003
Version: 0
Roll: bysize,32;1
Source: http://trans.acme.com/Current/ChannelManager
```

The actual log entries vary depending on the event recorded. Usually, they include the following information about each entry:

- The date and time
- The severity level
- The user ID

- The log ID
- The log message

If you turn on debugging, you might also see additional information (usually preceded by #).

For more details about the log IDs and severity levels, see the logging codes chapter of the *BMC Marimba Client Automation Reference Guide*, which is available from the Marimba Channel Store.

Here are some examples of log entries:

```
[26/Nov/2003:13:48:45 -0800] - audit spiky 1100 Channel created
[27/Nov/2003:16:27:01 -0800] - audit spiky 1101 Channel update
started
[27/Nov/2003:16:27:13 -0800] - audit spiky 1107 Channel index
installed: <index id="urn:idx:UVlBpSwFj19TCjzNjxkh1A==" 
size="4065722">
[27/Nov/2003:16:27:13 -0800] - audit spiky 1102 Channel update
finished
[07/Dec/2003:16:15:21 -0800] - audit spiky 1110 Channel checkpoint
created: signed
[07/Dec/2003:16:15:21 -0800] - audit spiky 1150 Channel instance
started
#CHANNEL INSTANCE
#ArchiveFS Load Time: 711 ms
#XML Load Time: 1983 ms
#XML Load Time: 100 ms
#ArchiveFS Load Time: 130 ms
[07/Dec/2003:16:16:17 -0800] - audit spiky 1152 Channel instance
stopped
```

## Tuner background

This section discusses additional facts about the tuner that have not been covered elsewhere but might be of general interest to you when you're administering a tuner.

## Tuners and Intel AMT

BMC Marimba Client Automation Infrastructure 7.x and later detects if the Intel® Active Management Technology (Intel® AMT) chip is present on a machine, and if it is, stores the machine ID there.

There are two main uses.

- When you image machines, you can avoid the imaged machines having the same machine ID as the original.

- You can store information in the flash storage so the data does not get copied to another machine during an image. This information can be sensitive or confidential data that you want to keep only on the machine, and machine-specific information such as the machine ID.

## Imaging machines using Intel AMT

Running a tuner for the first time and then imaging a machine differ between version 7.x and pre-version 7.0.

- With version 7.x, the first time you run the tuner on a machine, the tuner checks the Windows registry and the Intel AMT flash memory. If the ID is not present in flash memory, then the tuner creates and stores an Intel AMT ID (specific for that machine) in flash storage and copies the ID to the Windows registry. If you create a ghost image of a tuner that already has a machine ID, then the machine ID in flash memory is not captured in the image, although the machine ID in the registry is. When the image is installed on new machine, the tuner generates a new machine ID.
- With version 6.x and earlier, the first time you ran the tuner on a machine, the tuner created the machine ID and copied the ID to the Windows registry. If you created a ghost image with ID, the registry was copied and the second machine had the same ID as the first machine.

If Intel AMT is available and can be accessed, the tuner starts and sets `runtime.tuner.intelamt=presentenable`. This is the default. When the tuner starts on an imaged machine, the tuner detects if the machine ID in the registry matches what is in the local Intel AMT chip. If the IDs do not match, then the tuner knows the registry version is incorrect and generates a new machine ID. If the machine ID does not exist in flash memory, then the tuner generates a new ID and stores the new value in both flash memory and the registry, overwriting any value that was captured during the imaging process. IDs are stored in the registry under

`HKEY_LOCAL_MACHINE\Software\Marimba\Inventory\MachineID`.

If the machine ID is in the registry when you image the machine, the ID is included in the image. Even though this ID is updated by the tuner after the ID is installed, you should delete the ID using tuner anonymization prior to imaging.

If Intel AMT is available and cannot be accessed, for example, because of a hardware error, then the tuner starts and sets `runtime.tuner.intelamt=presentdisable`.

## Imaging machines without Intel AMT

If Intel AMT is not available, the tuner sets `runtime.tuner.intelamt=notpresent`. With an image, the machine ID is part of the image that is copied (by the administrator or a provisioning utility) to new machines.

To avoid duplicating information, use tuner anonymization, a process that removes the tuner unique ID (captured in Scanner Service reports) and other identifying information.

### Removing identifying information

#### ► **To remove identifying information**

Before you image a machine, you should remove the machine ID and other identifying information from the Windows registry by doing one of the following:

- Run `tuner -anonymize`
- Use anonymizing software

### Viewing machine details

After you have connected to a tuner, you can view detailed information at any time about the machine on which the tuner is running. To do this, click the tuner URL (for example, `http://ny_trans:7717`) displayed on the top of the page in Tuner Administration. The Report Center Machine Details page for that machine appears, showing you information such as its model, speed, memory, and so on. See the Report Center documentation for information.

## Tuner IDs

When requesting channels or updates from a transmitter, each tuner sends an ID (sometimes known as a *cookie*) by which it uniquely identifies itself to the transmitter. For security, a tuner sends a unique ID to each transmitter. If you want a tuner to send the same ID to specific transmitters, use the `marimba.security.identity.transmitters` property.

Transmitters record the IDs when logging connections that tuners make to them. Each time you install a tuner, it creates a new, unique ID. However, if you install a new tuner and configure it to use an existing tuner workspace directory, the new tuner uses the same ID that was created by the previously installed tuner.

## Network detection in the tuner

The tuner has an automated network detection feature that lets it try to determine if a network connection is currently available. If the tuner detects that it does not have a network connection, the tuner does not waste time attempting to update channels or perform unnecessary address lookups.

There are two methods of network detection that the tuner can use:

- **Ping.** For more information, see “Using ping for network detection” on page 399.
- **Multicast.** For more information, see “Using multicast for network detection” on page 401.

The detection feature is repeated every minute when the network is detected and every 30 seconds if the network is not detected. You can set the timing with the `marimba.network.detection.delay.online` and `marimba.network.detection.delay.offline` tuner properties.

### Using ping for network detection

In tuner versions 4.6 and later, there is an alternative network detection policy that addresses previous limitations. The new policy works by attempting to *ping* a specified host.

The benefits of using this policy include the following:

- It overcomes false positives in static addresses.
- It is sensitive to cable disconnection or real network outage.

Using this policy requires the following:

- Winsock 2 (ws2\_32.dll) must be installed. ICMP Echo is sent over a raw socket; the older Winsock does not support raw sockets.
- For Windows NT and Windows 2000, the tuner must be running as an service or the user must have administrative privileges. The platforms do not allow non-administrators to create raw sockets.

- Currently, `marimba.network.detection.address` must be specified.

If any of the above requirements are not met, the tuner reverts to the multicast test (used by the network detection policy described in “Using multicast for network detection” on page 401) and logs a message indicating that it did so.

This policy is activated by setting the following tuner properties:

- `marimba.network.detection.policy` is set to `ping`.
- `marimba.network.detection.address` specifies the desired address (not a host name). The address of a router is a good choice for the value to use.
- `marimba.network.detection.ping.retries` specifies the number of times to try the ping before concluding there is no network available. The default number of retries is 3.

For example:

```
marimba.network.detection.policy=ping  
marimba.network.detection.address=216.200.61.168  
marimba.network.detection.ping.retries=2
```

The settings enable the ping detection policy which sends ping packets to 216.100.61.168 with a maximum of two retries.

## How the ping network detection policy works

Network detection is performed using a low-overhead data exchange with the designated address. Specifically, the tuner transmits an ICMP (Internet Control Message Protocol) echo message and wait for an echo reply message. If a reply is not received within 1 second, the tuner transmits another echo message and wait again up to the number of times specified by `marimba.network.detection.retries`. The tuner sets `runtime.network.detected` to `true` if it receives a reply and sets `runtime.network.detected` to `false` if the retries are exhausted without receiving a reply.

Like the multicast test (used by the network detection policy described in “Using multicast for network detection” on page 401), this test is repeated every minute when the network is detected and every 30 seconds if the network is not detected.

Using this method, the tuner transmits from 1 to 3 packets per minute while `runtime.network.detected=true`.

## Using multicast for network detection

Network detection is performed using a low-overhead multicast operation. If the tuner is successful in its attempt to join and then leave a multicast group, it knows it has a network connection. The tuner uses the multicast address 228.200.200.201 for this test. This test is repeated every minute if the network is detected and every 30 seconds if the network is not detected.

Network detection using the multicast test results in one to three packets per tuner per minute sent directly to the router. Because the TTL (Time To Live) on the packets is set to 1 (the multicast default), packets should not go beyond the target router and therefore should not propagate throughout the network.

Network detection can be disabled (in tuner 4.5.0.3 or later releases) by setting the tuner property `marimba.network.detection.policy` to a setting other than `detect`.

For more information, see the tuner properties chapter of the *BMC Marimba Client Automation Reference Guide* on the Marimba Channel Store.

An alternative network detection policy that is available in tuner 4.6 and later releases is described in “Using ping for network detection” on page 399.

## Tuner properties for network detection

The following properties appear in the `tuner.properties.txt` file (usually in `C:\Program Files\BMC_Software\BBCA\Tuner\lib\tuner\properties.txt` on Windows). By setting the properties, you can control the network detection behavior of a tuner. If you are creating an installer during setup and deployment, you can use the properties to create an installer with the desired network detection settings.

- `marimba.network.detection.policy` (available in tuner 4.5.0.3 or later)
  - This property determines the tuner's network detection behavior. All other platforms default to `detect`, as does the behavior if the property is not set. Setting the property to `detect` tells the tuner to use multicast to detect the network.

The property can be set to `on` or `off`, which forces the tuner to act as if it is online or offline, respectively, by setting `runtime.network.detected` to `true` or `false`.

- `runtime.network.detected` — This property can be true or false, as determined by the tuner property `marimba.network.detection.policy`.
- `runtime.network.online` — This property can be true or false, depending on the Options Manager configuration.
- `runtime.network.enabled` — This property is true if `runtime.network.detected` and `runtime.network.online` are both true.

## Network detection and missed events

If the tuner misses certain events, such as a scheduled update or an inventory scan, because a network connection is not available, it keeps track of those missed events. When a network connection becomes available, the tuner runs the scheduled update or inventory scan.

For tuner versions 6.0 and higher, if the tuner cannot detect a network connection and it goes into minimal mode, it periodically tries to detect a network connection. When the tuner detects a network connection, it wakes up from minimal mode and runs any missed events.

## Tuner detects subnet change and flushes repeater properties

The tuner detects when the subnet on which it resides has changed. If the subnet has changed, the tuner flushes all repeater properties for every channel in its workspace. For example, if a Subnet-based Repeater Policy (SBRP) has been set and a tuner's machine is moved out of one subnet and into another, then the tuner will flush its set of repeaters in order to be redirected to the repeater associated with its new subnet. This applies to any repeater policy.

## Minimal mode

Minimal mode is a separate process known as `minituner.exe` and is no longer part of the tuner. This makes minimal mode more robust and the tuner more reliable.

In Windows XP SP2 and later and Windows Server 2003 SP1 and later, the firewall is enabled by default. The first time you use a tuner, you are prompted to enable or disable the firewall. The first time a tuner goes into minimal mode, you get the same prompt.

If you try to retrieve tuner diagnostics using the browser and the remote tuner is in minimal mode and the RPC port is SSL enabled, then the browser displays an error message stating that no diagnostics are available until the tuner wakes up from minimal mode. Tuners that have secure RPC ports, however, are typically server endpoints, for example, a transmitter, which never go into minimal mode.

## Garbage collection

*Garbage collection* refers to the tuner removal of channel files that are no longer used because the channel was deleted (or updated to a version that no longer uses those files).

Different channels on the same transmitter can share files, so even though one channel is no longer using a file, another channel might still be using it. The tuner does not delete a file until there are no longer any references to it.

The tuner performs garbage collection whenever an action occurs that might result in some files becoming garbage. Such actions include adding, deleting, updating, and unsubscribing a channel. After such an action occurs, the tuner waits about three seconds before doing garbage collection. If an action occurs (for example, a channel is added or removed) when the tuner is already in the process of garbage collection, garbage collection stops and the tuner waits three seconds before resuming.

---

Note: The transmitter does garbage collection, but differently from the tuner: whereas the tuner deletes the files immediately, the transmitter keeps some files around, depending on its cache size.

---

## Application distribution protocol

Application Distribution Protocol (ADP) is the protocol used for communication between the tuner and the transmitter. It is a versioned protocol; typically transmitters and tuners support multiple versions of it, enabling an older tuner to communicate with a newer transmitter and vice versa.

ADP was designed by BMC Marimba Client Automation to run on top of HTTP. This makes it possible for clients (tuners) to connect to transmitters through the most common firewall solution: the HTTP proxy. ADP works in a simple request/response mode.

## Behavior of autostart channels with the tuner minimal mode

The behavior of channels with regard to the tuner minimal mode depends on its type. There are four possible types:

- autostart only channels (which have the channel property `service.autostart.order` set to an integer value)
- daemon only channels (which have the channel property `service.daemon` set to true)
- both autostart and daemon
- neither autostart nor daemon

In version 6.0.3SP1, the new behavior is that only channels that were running before the tuner goes into minimal mode are restarted when the tuner wakes up from minimal mode. This change affects the following types of channels only:

- If a channel is both autostart and daemon (for example, Logging Service) and it is not running before the tuner went into minimal mode, then the tuner does not restart the channel when the tuner wakes up from minimal mode.
- If a channel is autostart only (for example, CMS and transmitter) and it is not running before the tuner went into minimal mode, then the tuner does not restart the channel when the tuner wakes up from minimal mode. Before version 6.0.3SP1, the tuner always restarts channels that are autostart only.

However, if you want a channel to maintain the behavior before 6.0.3SP1, you can set the channel property `service.autostart.wakeup` to true. This channel property causes the tuner to restart the channel (autostart only or both autostart and demon) when it starts from minimal mode even if the channel was not running previously.

# Chapter 23 Lite Weight Administrator Console

The following topics are provided:

- Introduction to Lite Weight Administrator Console (page 413)
- Advantages of LWAC (page 413)
- Browser support (page 414)
- Logging into the LWAC to perform operations on the transmitter (page 414)
- Logging on to Lite Weight Tuner Administrator (page 425)

# Introduction to Lite Weight Administrator Console

To administer a remote tuner with 9.0.00 Marimba releases, you must ensure to adhere to the following prerequisites:

- You must use the Infrastructure Administration channel.
- The CMS channel must be available in the tuner.

The Infrastructure Administrator connects to a computer that has CMS, and the CMS then connects to the endpoint. This two stage process consumes more bandwidth. However, to perform most of the basic channel operations, you do not need a CMS. All Web application channels run on the CMS console. The performance of CMS responsiveness is impacted if:

- More channels are running, and
- Multiple users are logged in and are performing operations

The Lite Weight Administrator Console allows you to perform commonly and frequently operations on the tuner and the transmitter.

The Lite Weight Administrator Console (LWAC) can run on any browser. Instead of using the remote administrator, you can use LWCA to manage the endpoint channels and packages on both transmitter and the tuner.

LWAC consists of the following two modules:

- Lite Weight Transmitter Administrator

You can use the Lite Weight Transmitter Administrator to:

- View and edit transmitter settings
- Edit transmitter properties
- Manage channels
- Transmitter diagnostic options
- Lite Weight Tuner Administrator

Using Lite Weight Tuner Administrator, you can administer the endpoints directly on the specified port of the end-point.

## Advantages of LWAC

The advantages of the LWAC are:

- Uses a light weight console.

- You can use LWAC it on any browser on any machine.
- When you use LWAC in the same subnet, the performance increases.

## Limitation

LWAC is not supported on the tuner which hosts the CMS channel.

## Browser support

LWAC supports the following versions of browsers:

**Figure 1 Support for Browser Versions**

Browser	Versions
Internet Explorer	10, 11
Mozilla FireFox	30, 31, 32, 33, 34
Chrome	27, 31, 33, 34, 35, 36, 37, 38, 39

## Logging into the LWAC to perform operations on the transmitter

Before you start the LWAC to perform operations on the transmitter, ensure that the transmitter is running.

### ► To use the Lite Weight Transmitter Administrator:

- 1 Type the following URL in the address bar of any browser:

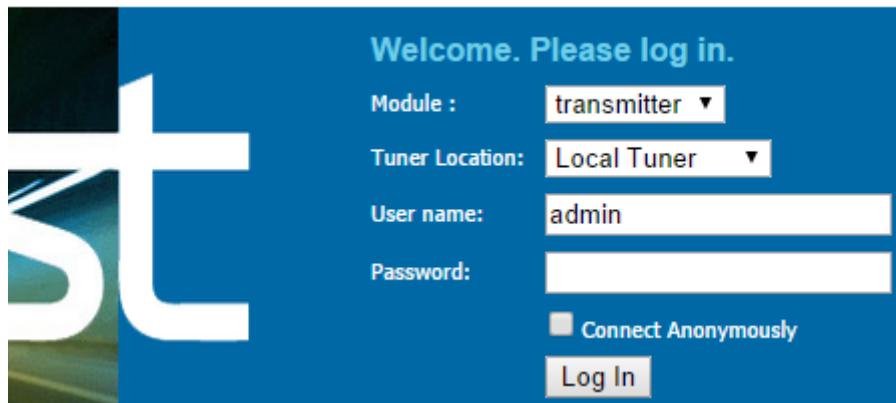
URL format: http://  
<tuner\_host\_name>:<marimba.tuner.administrator.port>

For example, http://localhost:7799

Note:

- LWAC uses 7799 as the default port number. However, you can use the marimba.tuner.administrator.port property to specify the port for LWAC.
- If you want to connect to an SSL enabled transmitter, use HTTPS in the URL.
- If the tuner is in fully interactive mode, you can right-click on the tuner icon and click Manage to open LWAC in the default browser.

The LWAC Logon page appears.



- 2 In the Module list box, select Transmitter.
- 3 In the Tuner location list box, select any of the following option.
  - Select Local Tuner if you want to connect to the Tranmsitter on the local tuner.
  - Select Remote Tuner if you want to connect to the transmitter on a remote tuner. If you select Remote Tuner, the Login page displays Tuner RPC address text box where you can specify the RPC address of the remote tuner.
- 4 If the user credentials are set on the transmitter, type the logon credentials in the User name text box and the Password text box, .
- 5 Select Connect Anonymously check box if you want to connect anonymously.
- 6 Click Log In.

The LWAC View and Edit Transmitter Settings page appears by default.

## Navigating in the Lite Weight Administrator Console

To navigate in LWAC, you can use links on the left hand side of the page.



You can click on the required link to navigate to the respective page.

## Editing Transmitter settings

To edit Transmitter settings, click Edit Settings link in the left side menu. By default, LWAC displays the Transmitter information.

The screenshot shows a web-based interface titled "Edit Transmitter settings running on http://localhost:7717". At the top, it displays the current state: "Transmitter State: On", "Transmitter Type: Master", "Transmitter Version: 8.3.02", and "Channel Count: 7". Below this, there is a section titled "Change Transmitter Settings" containing fields for "Transmitter Status" (radio buttons for On and Off, with On selected), "Transmitter Port" (text input field set to 5282), "Simultaneous connections" (text input field set to 1024), and "Cache Settings" (links to "Clear Index Cache" and "Clear File Cache"). A "Apply" button is located at the bottom of this section.

In the Edit Settings page you can perform the following actions:

- View the following Transmitter details:

- Transmitter state: whether it is switched on or off
- Transmitter type: specifies the type of transmitter such as master, mirror or proxy.
- Number of channels: The number of channels the transmitter hosts.
- Edit transmitter settings

In this page, you can perform the following actions:

- Change the status of transmitter to on or off.
- Start replication.

Note: If the transmitter type to which you are connecting is Master, then the Start Replication link does not appear.

- Perform the following operations on transmitter cache:
  - Clear index cache
  - Clear file cache
- Set the transmitter port.
- Set the number of simultaneous connections that the transmitter can handle.

Note: Once you make any changes in this page, click Apply to save the changes.

## Editing transmitter properties

You can use LWAC to view and edit transmitter properties. To view and edit transmitter properties, click Edit Properties link in the left hand side menu. LWAC displays the Edit Transmitter Properties page.

**Edit Transmitter Properties Running on <http://localhost:7717>**



**Transmitter State:** On  
**Transmitter Type:** Master  
**Transmitter Version:** 8.3.02  
**Channel Count:** 7

[Add New Property](#) [Delete Property](#)

Show [10](#) entries

	Property
<input type="checkbox"/>	<a href="#">log.access.channel.version</a>
<input type="checkbox"/>	<a href="#">log.access.name</a>

You can perform the following operations in this page:

- Add a new property.
- Delete a property.
- Edit a property.
- Search for a property.

#### ► To add a new property:

- 1 In the Edit Transmitter Properties page, click Add New Property button. A new row consisting of blank property name text box and values text box appears.
- 2 Type the property name and the property value in the respective text boxes.
- 3 Click Apply.

#### ► To delete a property:

- 1 In the Edit Transmitter Properties page, select the property which you want to delete.
  - 2 Click Delete Property button.
- LWAC deletes the selected property.

► **To modify the value of a property:**

- 1 In the Edit Transmitter properties page, select the property which you want to modify. You can also use the Search feature to search for a transmitter property.
- 2 Make the required changes in the Values text box for the required property.
- 3 Click Apply.

LWAC saves the modified property values.

Note:

The LWAC does not display non-transmitter properties.

For example: Any property which is not prefixed with transmitter, mirror, repeater, and log.

However, you can edit and add these types of properties. Even after you use LWAC to add and edit the non-transmitter property, LWAC does not display the property. To edit these types of properties, add the property with the new value and LWAC overwrites the existing property with the new value.

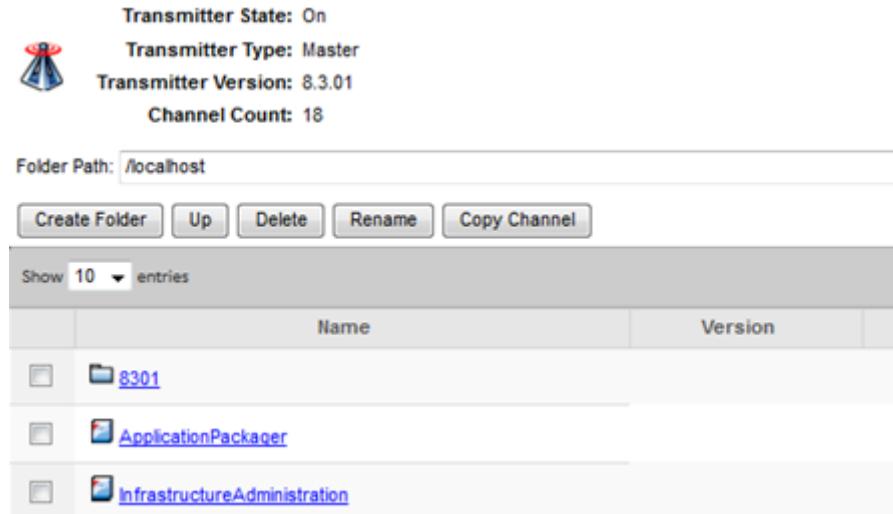
## Managing channels in the transmitter

You can use LWAC to manage channels on the transmitter. To view the Manage Channels page, click Manage Channels link in the left side menu.

### Viewing the details of the channel

LWAC displays the list of channels available in the root folder. To view more details of any channel, click on the required channel. LWAC displays the following details for the selected channel:

- Name of the channel
- Channel version
- Size of the channel
- Publish time of the channel



In this page, you can perform the following operations :

- Navigate to a folder.
- Create a folder.
- Delete a Channel.
- Rename a channel.
- Copy a channel.
- Search for channel.

Note: To refresh the page, click the Refresh button.

#### ► **To navigate to a folder**

To navigate to a folder on the transmitter, type the folder path in the Folder Path text box and click Go button.

#### ► **To create a folder**

- 1 To create a folder at the transmitter root level, select the check box next to the transmitter and click Create Folder.
- 2 To create a subfolder (inside an existing folder), select the check box next to that folder and click Create Folder.

The Create Folder text box appears.



- 3 Type the name of the folder along with the path in the Create Folder text box.
- 4 Click Create Folder button.

LWAC creates the new folder and displays a confirmation message if the create folder operation is successful.

#### ► To delete a channel

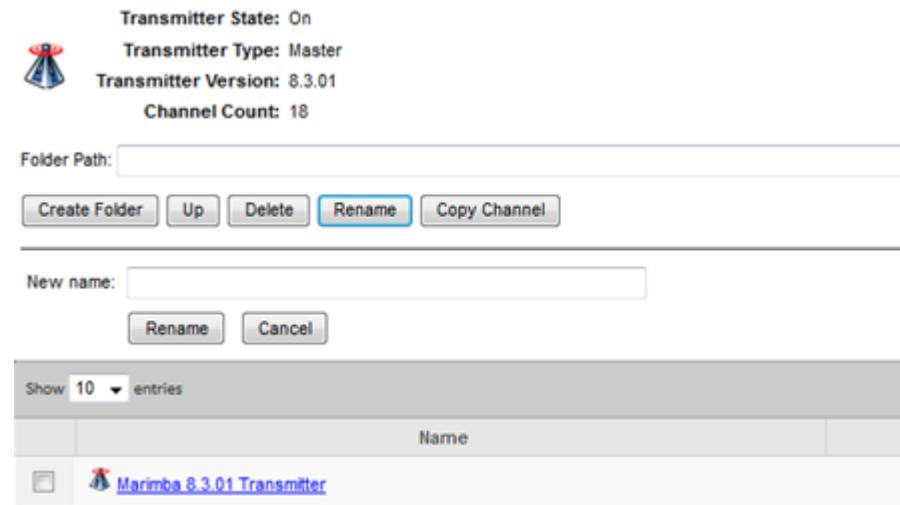
- 1 In the Manage Channels page, search for and select the channel which you want to delete.
- 2 Click Delete button.

LWAC deletes the selected channel and displays a confirmation message if the deletion operation is successful.

#### ► To rename a channel

- 1 In the Manage Channels page, search for and select the channel which you want to rename.
- 2 In the Manage Channels page, click Rename button.

The Rename Channel text box appears.

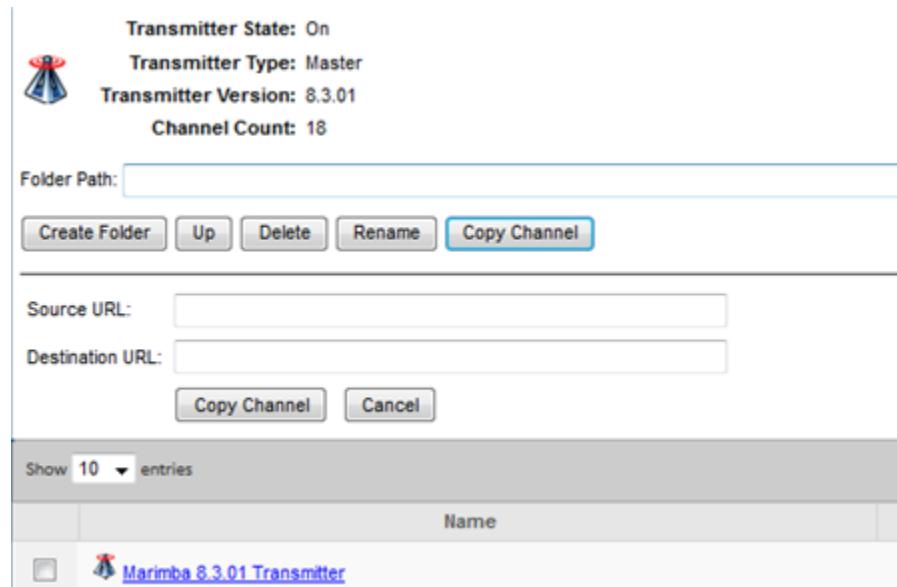


- 3 Type the new name of the channel in the New name text box.
- 4 Click Rename button.

LWAC renames the selected channel and displays a confirmation message if the rename operation is successful.

#### ► To copy a channel

- 1 In the Manage Channels page, click Copy Channel button.  
The Source URL and Destination URL text boxes appear.



- 2 In the Source URL text box, type the source URL of the channel which you want to copy.
- 3 In the destination URL text box, type the destination URL of the location where you want to copy the channel.
- 4 Click Copy Channel button.

LWAC copies the specified channel and displays a confirmation message if the copy channel operation is successful.

## Transmitter diagnostic options

You can view the transmitter diagnostic options in the Transmitter Diagnostic Options page. To view the transmitter diagnostic options, click Transmitter Diagnostic Options link in the menu which is available at the left hand side of the page.

## Diagnose transmitter running on <http://localhost:7717>

	Transmitter State: On
	Transmitter Type: Master
	Transmitter Version: 8.3.02
	Channel Count: 7
Actions	Description
<a href="#">?status</a>	Get Status Report containing general information about the transmitter.
<a href="#">?xml</a>	Get XML listing of all channels present on this transmitter
<a href="#">?viewLog=access</a>	View Transmitter Access Logs
<a href="#">?viewLog=admin</a>	View Transmitter Admin Logs
<a href="#">?viewLog=plugin</a>	View transmitter logs
<a href="#">?seginfo</a>	Get transmitter segmentation information

You can use the following diagnostic options:

- ?status
- ?xml
- ?viewLog=admin
- ?viewLog=access
- ?viewLog=plugin
- ?seginfo

Once you click on the required diagnostic link, an XML file opens in a new browser window.

Note: When you use the ?viewLog=plugin option, you can also specify the channel name as the argument in the Argument text box.

For example:

If you are specifying the channel name, then use the following format:

For example:

Channel=/Marimba/8.5.00/Inventory Service

Note: If you want to specify a channel name which is located in the root folder of the transmitter, then use the following format:

Channel=/Inventory Service

## Logging on to Lite Weight Tuner Administrator

### Prerequisites

Prior to using the Lite Weight Tuner Administrator, ensure the following:

- Upgrading the Tuner to the Infrastructure Service 8202 or higher.
- Assigning values to the following properties:

`marimba.tuner.administrator.port`

Specifies the port on which the Lite Weight Tuner Administrator needs to administer an endpoint tuner.

Default value: 7799

**Note:** After you change the values of the properties, restart the tuner.

## Using the Lite Weight Tuner Administrator

You can use the Lite Weight Tuner Administrator to:

- Manage SMCA channels on tuners

You can perform the following actions on SMCA channels on a tuner:

- Subscribe
- Start
- Stop
- Delete
- Update

- Manage Packages

You can perform the following package related operations:

- Install

- Un-install
- Verify
- Repair
- Edit general tuner settings

You can perform the following change configuration operations on a tuner:

- Edit tuner user interaction mode
- Change trusted transmitter settings
- Add, Delete, Edit custom properties
- Configure dependencies

When you want to perform channel operations in a sequential order, you can specify the dependencies between channels or packages.

- Perform tuner operations

You can perform the following tuner operations:

- Tuner commands such as Restart or Stop Tuner, Launch Console, Update Policy, and Scan machine
- Storage commands such as -fsck, -reconstruct, and - repairchannels
- Perform tuner diagnostics

You can perform tuner diagnostic using the following options:

- ?status
- ?channelstatus
- ?debug
- ?log requests

#### Note:

- Prior to administering a tuner in minimal mode, you must wake-up the tuner.
- Before you start the Lite Weight Tuner Administrator, ensure that the Tuner is started and is working.

## Prerequisites

Prior to using the Lite Weight Tuner Administrator, ensure the following:

- Upgrading the Tuner to the Infrastructure Service 8202, or higher.
- Assigning values to the following properties:

`marimba.tuner.administrator.port`

Specifies the port on which the Lite Weight Tuner Administrator needs to administer an endpoint tuner.

Default value: 7799

**Note:** After you change the values of the properties, restart the tuner.

### ► To use the Lite Weight Tuner Administrator:

- 1 Type the following URL in the address bar of any browser:

URL format: `http://<tuner_host_name>:<marimba.tuner.administrator.port>`

For example, `http://localhost:7799`

The LWAC login page appears.

- 2 In the Module list box, select Transmitter.
- 3 In the Tuner location list box, select any of the following option.
  - Select Local Tuner if you want to connect to the tuner on the local tuner.
  - Select Remote Tuner if you want to connect to a remote tuner. If you select Remote Tuner, the Login page displays Tuner RPC address text box where you can specify the RPC address of the remote tuner.
- 4 If the user credentials are set on the tuner, type the logon credentials in the User name text box and the Password text box, .
- 5 Select Connect Anonymously check box if you want to connect anonymously.
- 6 Click Log In.

On successful login, the Lite Weight Tuner Administrator page appears.

You can now administer the tuner.

**Note:** To indicate the status of tasks, in the browser, click Refresh button to refresh the page. Lite Weight Tuner Administrator displays the updated status.

## Known issues

For the Lite Weight Tuner Administrator, you must open a new port on the endpoints. The endpoints are administered on this new port. By default, the Lite Weight Tuner Administrator runs on the 7799 port. However, you can change the port by using the `marimba.tuner.administrator.port` property.



# 24 Handling JRE

The following topics are provided:

- Introduction (page 431)
- Upgrade scenario (page 432)
- Prerequisites (page 432)
- Property to specify use of the installed JRE on an endpoint (page 432)
- Workflow of JRE detection and starting the tuner (page 433)
- How to find the JRE version which the Tuner is currently using on an endpoint? (page 433)
- Can I uninstall JRE on an endpoint? (page 434)
- JRE handling while creating a profile for an endpoint tuner (page 434)
- Log messages (page 434)

## Introduction

Prior to 9.0.00, the JRE is bundled with the tuner. However, from 9.0.00 Marimba provides a feature which allows you the following options:

- Use JRE that is installed on the machine instead of the JRE bundled with the Marimba installer.
- Use the JRE bundled with the installer.

This advantage of using the JRE installed on the machine is that you can use the latest JRE available. The minimum version of JRE supported is 1.7.0 or higher.

If you choose to use the JRE that is installed on the machine but in some scenarios where the tuner tuner cannot detect the JRE installed on the machine, then the tuner uses the fallback mechanism where it uses the JRE bundled with the tuner. The common factors responsible for the tuner not detecting the JRE may include scenarios such as :

- The JRE version available on the machine is lower than than the minimum supported version
- The JRE path could not be found or is incorrect.

You can enable this feature by setting the following property to true or false:

**marimba.tuner.use.installedJRE**

You can set this property either through profile or policy. If this property is set to true, tuner detects the JRE version installed on the system and if it matches the minimum JRE verion required, then the tuner uses the JRE. If the tuner is unable to find the correct JRE on the machine, it uses the JRE bundled with the tuner. If this property is not set or is set to false, tuner uses the JRE which is bundled with the tuner.

The existing feature where only the bundled JRE is used can have the following disadvantages:

- The JRE bundled with the tuner is not updated due to which an organization may face security compliance problems. Some software compliance tools might report an older version of JRE in use as a security threat.
- Whenever there is a need to update JRE, a new version of Infrastructure Service has to be released, and hence the user needs to install updated Infrastructure Service.

However, during a fresh tuner installation if the JRE is not present in the system, then an option to bundle JRE is provided. If the JRE is not present on the machine, this feature provides the administrator with a configurable option for the tuner profile to bundle the JRE installer with the tuner and the tuner will install it at the time of installation.

---

Note: Marimba 9.0.00 has not certified this feature with JRE 1.8 and higher.

---

## Upgrade scenario

When the tuner is upgraded from 8.2.02, 8.3.00, 8.3.01, 8.5.00 to 9.0.00 there can be the following two scenarios:

- The system contains JRE

After the tuner is upgraded, it uses the JRE which is installed in the system

- The system does not contain JRE

## Detection of JRE

Once the JRE is detected, the tuner.exe uses this JRE to launch the JVM.

## Prerequisites

The minimum JRE version required for tuner 9.0.00 to start is JRE version 1.7. You must ensure that any JRE version equal to or higher than 1.7 is already installed on the endpoint if you want to use the JRE installed on the machine. If the JRE version is less than 1.7, then tuner will use the fallback mechanism where it uses the bundled JRE.

## Property to specify use of the installed JRE on an endpoint

You can use the following property to enforce the use the installed JRE on an endpoint:

**marimba.tuner.use.installedJRE**

Values: true, false

Default value: not set

For example:

**marimba.tuner.use.installedJRE=true**

If this property is set to true, then the tuner will check if the installed JRE on an endpoint is suitable to use.

## Workflow of JRE detection and starting the tuner

The whole process of detecting the JRE and starting the tuner consists of the following steps:

1 Checks the value of the **marimba.tuner.use.installedJRE** property.

2 JRE detection

If the **marimba.tuner.use.installedJRE** property is set to true, as a first step the JRE is detected which is required to launch the tuner.

3 Initialization

In this stage, configure and set JVM launch arguments, class path, library path, OS Name etc. and then these arguments are used to launch the JVM.

4 Starting tuner by java.exe

In this phase, using arguments configured in step 3 the tuner is started by launching java.exe.

## How to find the JRE version which the Tuner is currently using on an endpoint?

You can view the JRE version which the tuner is currently using on an endpoint from the following locations:

- Click Tuner tray Icon->About->Java Version.
- Navigate to Tuner Administration -> JRE version.
- Navigate to Tuner Administration -> Advanced->JVM->JRE version
- Navigate to ISM tab -> the required endpoint ->Java VM Version

---

Note: In the ISM tab, along with the Java version, you can also view the path of the JRE which the tuner uses.

---

## Can I uninstall JRE on an endpoint?

You cannot uninstall JRE on an endpoint if the tuner is running.

## JRE handling while creating a profile for an endpoint tuner

While creating or editing a profile, a new JRE tab is introduced under the Advanced tab. The JRE tab displays the Allow Tuner to use the installed JRE checkbox.

### When should I select this check box?

If you want the tuner to use the supported JRE which is installed on the machine, then select this check box. If this checkbox is selected, the JRE is not bundled with the Tuner installer.

---

Note: In a scenario where this check box is selected, and if the machine does not contain the supported JRE version, then the tuner installation fails.

---

By default, this checkbox is not selected, and in this scenario the JRE is bundled with the tuner installer. Once the tuner installation is complete, the tuner uses the JRE bundled with the tuner installer.

## Log messages

The log message in the launch.log file indicates the following:

- If tuner is using JRE installed on the machine or bundled with the tuner
- Location of JRE.

For example:

07/24/14 22:27:37 1680 INFO: Tuner is Using installed JRE

07/24/14 22:27:37 1680 INFO: Using JRE from location : C:\Program Files (x86)\Java\jre7  
07/24/14 22:33:47 3328 INFO: Tuner is Using bundled JRE

07/24/14 22:33:47 3328 INFO: Using JRE from location :  
C:\Win8\_StubHF\BBCA\Tuner\lib\jre

Chapter

# 25 Marimba Monitoring Service

The following topics are provided:

- Introduction to Marimba Monitoring Service (MaMoS) (page 437)
- The MaMoS Service (page 439)
- External Watchdog using OS specific scheduler (page 440)
- Key features of MaMoS (page 440)
- Advantages of MaMoS (page 441)
- Problem - Action matrix for critical Infrastructure Components in MaMoS (page 442)
- Modules registered with MaMoS (page 443)
- MaMoS components (page 443)
- Prerequisites (page 443)
- Configuring components for MaMoS (page 444)
- Configuring MaMoS through properties (page 444)
- Setting the debug flag (page 447)
- SNMP alerts for MaMoS in ISM (page 451)
- Using the ?status command (page 451)
- MaMoS Logging (page 452)

# Introduction to Marimba Monitoring Service (MaMoS)

## A typical use case

Large organizations typically have a huge IT infrastructure consisting of thousands of endpoints, sometimes numbering into 100's of thousands, and spread geographically all over the globe. Such companies usually keep on expanding and hence the number of endpoints keeps on increasing.

Sometimes the distribution patterns also continuously change over a period of time. Because of these continuously changing distribution patterns problems can occur on servers. Typical problems can be like some endpoints not synchronizing and their reports are inconsistent. In older versions of Marimba, the IT team had to search and identify the problematic servers or endpoints, and then apply the solution to the problem. Sometimes, the solution can be as simple as restarting servers or endpoints. However to identify and locate the problem might take a lot of time which consumes a lot of costly manual effort and time. The downtime which results because of these problems effects their daily deployments.

## The solution

The solution includes designing components in such a way that they are capable of identifying when they are going into a critical or bad state, and automatically trigger pre-configured actions that bring them back to a normal state. The advantage of this solution is that IT administrators need not spend time and effort in searching and identifying the problematic server or endpoint manually, thus reducing customer pain and reducing the occurrence of critical blockers in production.

### A short summary:

- Components detect if they are in a bad state and auto-correct themselves
- Customers need not spend time to identify and resolve the problem
- Most of the operations that Marimba performs can be classified as repetitive and cyclic because most of the operations are performed according to a schedule. Most of the problems in scenarios where the operations fail to recur as per the schedules.

For example: A typical Marimba operation running on schedule

The repeater sends a listing request to the mirror. Once the repeater receives the list of channels, it determines the missing content and then replicates the required content. Once the replication is completed, the repeater waits for the next replication schedule.

## How a problem is identified?

This solution utilizes the concept of a watchdog and works at two levels. While the Marimba components except tuner are monitored by Tuner level monitoring service, the Tuner itself is monitored by an OS level monitoring service. If any registered component fails to respond to the tuner level monitoring service, the tuner performs an action to overcome the problem. If the Tuner goes into an unresponsive state due scenarios like out of memory or deadlock, then the OS level monitoring service performs action such as restarting the tuner and sending an e-mail notification.

The tuner level monitoring service print the log messages in MaMoS log while the OS level monitoring service prints the log messages in the Windows event logs. The administrator can analyze the logs to understand the problem and resolve.

A watchdog is another component or service which tracks and identifies the component which is in a bad state. All components registered with the watchdog send timely updates or heartbeats to the watchdog to indicate that they are running as per schedule and properly, and are in a good state. To identify a problem from any of the components, the component must be registered with a watchdog. For example, in the preceding example, the mirror can send a heartbeat after every replication schedule to indicate that it is in good state. If the mirror fails to send a heartbeat, or if the watchdog fails to receive a heartbeat, an alarm is triggered to show that the mirror is not in a good state. Once an alarm is triggered, an action which is pre-configured can be triggered to resolve the problem and bring the component back to normal state.

## What is a Watchdog?

A Watchdog component is a service which monitors specific events and failures. The Watchdog service executes a pre-configured action only when a specific event occurs.

## What is a heartbeat?

A heartbeat is a signal or message generated by a Marimba component such as the tuner as per a pre-configured schedule or upon completion of an operation. The heartbeat is received by the watchdog.

## The MaMoS Service

Marimba Monitor Service (or MaMoS which is a new tuner service that in real-time monitors and remediates critical operations in Marimba components) helps the IT administrators on a real time basis to identify most of the common critical issues around Marimba components so that they do not have to spend time on searching and identifying the problem. The goal of MaMoS is to reduce downtime in the production lab and send appropriate notifications to the administrators through e-mail and for any problem occurring in the components and trigger appropriate pre-configured actions. MaMoS can be configured such that only notifications are sent and no action is taken till the Administrator intervenes.

The MaMoS feature is implemented as a watchdog that operates on two levels. All the Marimba components except the tuner is monitored by Tuner level monitoring service while the Tuner itself is monitored by an OS level monitoring service. If any component registered with MaMoS fails to respond to the tuner level monitoring service, then the tuner takes an action. If the tuner changes to an unresponsive state due to conditions such as out of memory or deadlock, then the OS level monitoring service performs a pre-configured action such as tuner restart or sending an e-mail notification.

MaMoS monitors the following parameters for Tuner and Transmitter modules of Infrastructure:

- Tuner Thread synchronization
- Tuner Memory utilization
- Tuner Storage corruption
- Tuner Session Isolation
- Tuner Scheduler operation
- Transmitter replication
- Transmitter storage corruption

**Note:**

The Tuner does not send heart beat to the external OS level MaMoS monitoring service. The external OS level MaMoS monitoring service periodically monitors tuner's MaMoS operations itself, and will restart the tuner if it detects that it is hung.

MaMoS does not support blackouts. Once MaMoS is enabled, the tuner sends heart beats even during blackout period.

The tuner in minimal mode does not send heartbeats.

## External Watchdog using OS specific scheduler

To implement an external watchdog, Marimba uses the APIs of the task scheduler application/service of the respective OS. The task scheduler periodically checks if a tuner has handled a scheduled event. The meaning of handled can include:

- A determination that a module has checked in with a heartbeat on time and that the Tuner observed it.
- A determination that a module has missed sending the heartbeat and the Tuner has noted the event.

In both of the above scenarios, the Tuner has handled a scheduled event. If this handling is missing, the monitor understands that the Tuner is unresponsive, and proceeds with the action of restarting the tuner.

Note:

All run-time MaMoS settings and external monitor's log file are stored in the following location:

For Windows platforms:

%ALLUSERSPROFILE%\Marimba\mamos\[servicename]

For non-Windows platforms:

The log files are stored inside the mamos folder located in the tuner's workspace.

## Key features of MaMoS

The key features of MaMoS include:

- Property driven configuration
- Tuner is responsive

- Minimal mode support
- Previous instance cleanup
- ISM support for MaMoS reporting
- Extended debugging
- No excessive action triggering
- Configurable actions such as restarting a tuner, and sending an e-mail.
- Ability to configure MaMoS on single or multiple components at a time (for example, Policy Administration, Profile Updates, etc.)
- Separate MaMoS logging
- ISM reports MaMoS actions using alerts or stats
- Collects the thread dump and heap dump before triggering an action like restarting a tuner so that the problem can be analysed.
- Ensure that MaMoS works even if the tuner itself is unresponsive by using an external monitor.

## Advantages of MaMoS

The advantages of MaMoS are:

- Highly configurable monitoring and auto correction system
- Marimba components attempt to auto-correct themselves
- Allows you to configure which components need to be monitored
- Allows you to configure the action to be taken when a component changes into a critical or bad state
- Saves time and effort of the IT team of administrators

## Limitations

- You cannot change the log roll policy for MaMoS. It will roll automatically.
- MaMoS is currently not supported on Mac OS platform.

- MaMoS related ISM alerts are displayed under the Transmitter down tab instead of a category of their own in Marimba Central Console.
- MaMoS external monitor is not supported on Windows XP machines.

## Problem - Action matrix for critical Infrastructure Components in MaMoS

The following table shows the critical section versus actions matrix:

Action Name	Memory Utilization	Thread Synchronization	Tuner Storage	Tuner Scheduler	Session Isolation	Transmitter Storage	Transmitter Replication	Proxy Storage
Restart tuner only	Yes	Yes	No	Yes	Yes	No	No	No
E-mail only	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Log message only	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Restart Transmitter	No	No	No	No	No	Yes	Yes	No
E-mail + restart tuner	Yes	Yes	No	Yes	Yes	No	No	No
Set debug + restart tuner	Yes	Yes	No	Yes	Yes	No	No	No
ISM alert + restart tuner	Yes	Yes	No	Yes	Yes	No	No	No
E-mail + log message	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Set debug + log message	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISM alert + log message	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Set debug + e-mail	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Set debug + ISM	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISM alert	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Repair Transmitter	No	No	No	No	No	Yes	No	No
Set force repair	No	No	Yes	No	No	No	No	No
Set force repair + e-mail	No	No	Yes	No	No	No	No	No
Set debug + set force repair	No	No	Yes	No	No	No	No	No
ISM alert + e-mail	No	No	Yes	No	No	No	No	No

---

Note: In case Debug and Restart action is set for any of the tuner's critical sections, sometimes tuner may fail to set debug flag before restarting tuner due to inconsistencies.

---

## Modules registered with MaMoS

Apart from the modules within the tuner, the following modules are mandatorily registered with the MaMoS service:

- Transmitter

## MaMoS components

The MaMoS feature consists of the following two components:

- MaMoS Schedule

This scheduler resides in the tuner and performs the following tasks:

- Receives requests for registration from modules that are monitored by MaMoS.
- Receives heartbeats from the registered modules.
- Detects that a heartbeat has been missed and triggers the pre-configured action.

- MaMoS Tuner Monitor

This component monitors the Tuner and uses the task scheduling capability of the OS to periodically monitors the Tuner for responsiveness, and thus determine the state of the monitor.

## Prerequisites

For MaMoS to operate, ensure the following:

- Infrastructure Service 9.0.00 is installed.

Since the functionality of MaMoS is dependent on an external task scheduler provided by the OS, you must ensure that the OS scheduler at the endpoint is working correctly.

You must restart the tuner once the MaMoS service is enabled.

## Configuring components for MaMoS

You can configure Modules for MaMoS from the following components:

- Tuner Administration page
- Profile Administration page
- Policy Manager (using properties)
- Lite Weight Tuner Administrator (using properties)

## Configuring MaMoS through properties

You need not set MaMoS properties manually if you are configuring MaMoS through Tuner Administration or Profiles in Setup and Deployment, as detailed in the next section.

You can use Policy Manager and Lite Weight Tuner Administrator to configure MaMoS using the following properties:

Note:

To set the schedule related properties, use the following syntax:

every <number> days update <every>

where:

<number> is an integer. Even if the number is 1, the word following it in the syntax must remain plural (for example: 1 days, not 1 day).

every <number> minutes

For example: every 1 days update every 10 minutes

### Transmitter storage

The following are the list of MaMoS properties related to transmitter storage:

- marimba.tuner.mamos.txstorage.module

Valid values: true, false

- marimba.tuner.mamos.txstorage.module.schedule
- marimba.tuner.mamos.txstorage.module.action

Valid values: log, email, ism, email\_log, debug\_log, ism\_log, debug\_email, debug\_ism, restarttx, repaixtx

## SMTP settings for sending E-mail action

Specify the following properties to configure SMTP settings for e-mail action:

- `marimba.tuner.mamos.smtp.host`

Specify the SMTP hostname in this property.

- `marimba.tuner.mamos.smtp.port`

Specify the SMTP port in this property.

- `marimba.tuner.mamos.smtp.useauth`

Set this property to true if user credentials are required for SMTP.

Valid value: true, false

- `marimba.tuner.mamos.smtp.user`

Specify the SMTP administrator's user name.

- `marimba.tuner.mamos.smtp.password`

Specify the SMTP administrator's password.

- `marimba.tuner.mamos.smtp.encryption`

Specify this property if you want to specify the encryption type used.

Valid values: tls, ssl

- `marimba.tuner.mamos.smtp.senderaddress`

You can use this property to customize the sender's e-mail address for mails sent by MaMoS.

Valid values: a valid e-mail address

- `marimba.tuner.mamos.smtp.subjectprefix`

You can use this property to customize the e-mail subject for e-mails sent by MaMoS.

Valid values: any valid text

- `marimba.tuner.mamos.smtp.destaddress`

This property is mandatory to set. You can use this property to specify a destination e-mail address for receiving MaMoS related e-mails. You can specify multiple recipient e-mail addresses separated by a comma or semi-colon.

## Memory utilization critical section

- marimba.tuner.mamos.oom.module

Valid values: true, false

- marimba.tuner.mamos.oom.module.schedule

- marimba.tuner.mamos.oom.module.action

Valid values: log, restarttuner, email\_restarttuner, email, debug\_restarttuner, ism\_restarttuner, email\_log, debug\_log, ism\_log, debug\_email, debug\_ism, ism

## Thread synchronization section

- marimba.tuner.mamos.deadlock.module

Valid values: true, false

- marimba.tuner.mamos.deadlock.module.schedule

- marimba.tuner.mamos.deadlock.module.action

Valid values: log, restarttuner, email\_restarttuner, email, debug\_restarttuner, ism\_restarttuner, email\_log, debug\_log, ism\_log, debug\_email, debug\_ism, ism

## Tuner session isolation critical section

- marimba.tuner.mamos.mclient.module

Valid values: true, false

- marimba.tuner.mamos.mclient.module.schedule

- marimba.tuner.mamos.mclient.module.action

Valid values: log, restarttuner, email\_restarttuner, email, debug\_restarttuner, ism\_restarttuner, email\_log, debug\_log, ism\_log, debug\_email, debug\_ism, ism

## Tuner storage critical section

- marimba.tuner.mamos.tunerstorage.module

Possible values: true, false

- marimba.tuner.mamos.tunerstorage.module.schedule

- marimba.tuner.mamos.tunerstorage.module.action

Valid values: log, restarttuner, email\_restarttuner, email, email\_log, debug\_log, ism\_log, debug\_email, debug\_ism, ism, forcerepair, email\_forcerepair, debug\_forcerepair, ism\_forcerepair

### Tuner scheduler critical section

- marimba.tuner.mamos.scheduler.module

Valid values: true, false

- marimba.tuner.mamos.scheduler.module.action

Valid values: log, restarttuner, email\_restarttuner, email, debug\_restarttuner, ism\_restarttuner, email\_log, debug\_log, ism\_log, debug\_email, debug\_ism, ism

### Transmitter replication critical section

- marimba.tuner.mamos.txrep.module

Valid values: true, false

- marimba.tuner.mamos.txrep.module.action

Valid values: log, email, ism, email\_log, debug\_log, ism\_log, debug\_email, debug\_ism, restarttx

## Setting the debug flag

If you have selected the debug action for any of critical sections, then you can use this property to specify the debug flags. You can specify multiple debug flags separated by a comma.

marimba.tuner.mamos.debugaction.args=<any valid debug flag>

### ► To configure MaMoS from the Infrastructure Administration:

- 1 Start CMS.
- 2 Navigate to the Tuner Administration.
- 3 Connect to the required tuner and click **Edit Settings**.  
The Tuner Administration page appears.
- 4 Click **Advanced** tab.

The Advanced tab appears.

- 5 Click MaMoS tab.

The MaMoS tab appear which displays the MaMoS configuration settings to monitor critical sections. You can configure the following critical sections:

- Thread Synchronization
- Memory Utilization
- Tuner Storage Health
- Tuner Scheduler
- Tuner Session Isolation
- Transmitter Replication
- Transmitter Storage

- 6 Select **Enable Critical Section** checkbox for the critical sections which you want MaMoS to monitor.

Once you select the **Enable Critical Section** checkbox, the **Action** list box and the **Schedule** text box appears.

- 7 In the **Action** list box, select the required action:

For the Thread Synchronization and Memory Utilization critical sections, you can configure or select from the following actions:

- Log a message
- send an e-mail
- Send an alert to ISM
- Log a message and send an e-mail
- Enable debug and log a message
- Send a message to ISM and log a message
- Enable debug and send an e-mail
- Enable debug and an alert to ISM
- Restart the tuner
- Send an e-mail and Restart the tuner
- Enable debug and restart the tuner
- Send an alert to ISM and restart the tuner

For the Tuner Storage Health critical sections, you can configure or select from the following actions:

- Log a message
- Send an e-mail
- Send an alert to ISM
- Log a message and send an e-mail
- Enable debug and log a message
- Send an alert to ISM and log a message
- Enable debug and send an e-mail
- Enable debug and an alert to ISM
- Set force repair property
- Send an e-mail and set force repair property
- Set debug and set force repair property
- Send ISM alert and set force repair property

For the Tuner Scheduler and Tuner Session isolation critical sections, you can configure or select from the following actions:

- Log a message
- Send an e-mail
- Send an alert to ISM
- Log a message and send an e-mail
- Enable debug and log a message
- Send an alert to ISM and log a message
- Enable debug and send an e-mail
- Enable debug and an alert to ISM
- Restart the tuner
- Send an e-mail and restart the tuner
- Set debug and restart the tuner
- Send ISM alert and restart the tuner

For the Transmitter Replication critical sections, you can configure or select from the following actions:

- Log a message
- Send an e-mail
- Send an alert to ISM
- Log a message and send an e-mail
- Enable debug and log a message
- Send an alert to ISM and log a message
- Enable debug and send an e-mail
- Enable debug and an alert to ISM
- Restart the transmitter

For the Transmitter Storage critical sections, you can configure or select from the following actions:

- Log a message
- send an e-mail
- Send an alert to ISM
- Log a message and send an e-mail
- Enable debug and log a message
- Send an alert to ISM and log a message
- Enable debug and send an e-mail
- Enable debug and an alert to ISM
- Restart the transmitter
- Repair the transmitter

- 8 To configure the heartbeat for each critical section, in the **Schedule** text box, type the heartbeat interval time.
- 9 To configure MaMoS e-mail settings, in the MaMoS Email settings section specify the following details in the corresponding text boxes:
  - Recipient's E-mail addresses
  - Sender's E-mail address
  - E-mail Subject prefix

Note: The MaMoS Email settings section appears only if you select any e-mail action while configuring the critical sections.

If you have selected debug action in any of the actions for critical sections, then you can view the Debug Flag Settings section where you can specify multiple debug flags separated by a comma.

Note: The Debug Flag Settings section appears only if you select any debug related action while configuring the critical sections.

- 10 Click Preview to view the settings.
- 11 Click Apply.
- 12 Restart the tuner once you configure MaMoS settings.

► **Configuring MaMoS from the Setup and Deployment page using profiles**

- 1 Start CMS.
- 2 Navigate to Setup and Deployment page.
- 3 Navigate to the Edit Profile page.
- 4 Click Advanced tab.
- 5 Click MaMoS tab.
- 6 Make the required MaMoS settings. The steps for configuring MaMoS are the same as specified in the preceding procedure.

## SNMP alerts for MaMoS in ISM

The ISM dashboard displays MaMoS related SNMP alerts for the registered components. The alerts description field for the MaMoS related SNMP alerts provide a short summary of the problem.

## Using the ?status command

When you request for the tuner's status using the ?status command through the RPC, the tuner responds by sending the status through XML file. The XML file provides the following information:

- The list of registered critical sections
- MaMoS critical section expected to check in

- Time at which the critical section was last processed by MaMoS
- Time at which the critical section is expected to be processed next by MaMoS
- Time at which critical section most recently checked in

The following snippet from the XML file shows the MaMoS related information:

```
<tuner-mamos>
<param name="registeredcriticalsections" value="tunerdeadlock"/>
<param name="mamosidentifier" value="tunerdeadlock"/>
<param name="checkpoint1" value="Tue, 30 Sep 2014 02:11:15 PDT"/>
<param name="checkpoint2" value="Tue, 30 Sep 2014 02:13:15 PDT"/>
<param name="lastheartbeat" value="Tue, 30 Sep 2014 02:11:16 PDT"/>
<param name="description" value="Tuner Health Statistics"/>
</tuner-mamos>
```

## MaMoS Logging

The tuner level monitoring service prints the logs in MaMoS log file and the OS level monitoring service prints the logs in Windows event logs. The MaMoS log messages are generated in a separate log file and indicate the timestamp and the operation undertaken such as tuner restart. Logs messages are generated for the following events:

- Internal MaMoS actions indicating when the action was performed, and the action performed and on which module.
- Success message when an action is performed successfully.
- Communication logs between the internal and external OS level MaMoS.

### Location of log files:

All run-time MaMoS settings and external monitor's log file are stored in the following location:

For Windows platforms:

%ALLUSERSPROFILE%\Marimba\mamos\[servicename]

Note: A log message is generated in the Windows Event Log if the external MaMoS has a problem.

For non-Windows platforms:

The log files are stored inside the mamos folder located in the tuner's workspace.

## MaMoS extended debugging

MaMoS collects the thread dump and heap dump before triggering actions like restarting a tuner. The thread dump and heap dump helps analyze and trouble shoot the problem.

## Optional Tuner property to configure MaMoS

To configure MaMoS to wait in milliseconds before processing a particular critical section (to determine if its heartbeat was missed or not), you can use the following property:

`marimba.tuner.mamos.waitbeforeprocessing`

Value: Milliseconds

You can use this property if you have a critical section that takes more time to perform an operation than the heartbeat schedule configured for it (i.e. a Transmitter replication of 15 minutes, which takes longer time due to replicating larger content). By default, if this property is not set MaMoS waits for 10 seconds.

# Index

## Numerics

- 7717 ( tuner default port) 259
- 8888 (CMS default port) 60

## A

- About page 61
- access control lists. *See* ACLs
- Access Control Read permissions 125
- Access Control Write permissions 125
- access log files, console
  - location of 78
  - reading contents 77
  - setting rolling policy 79
- access, limiting
  - Tuner Administration 193
- ACLs
  - assigning permissions 124
  - collections and 120
  - defined 118
  - deleting permissions 134
  - deleting users 136
  - directory service groups 119
  - inheritance 137
  - requirements 118
  - setting for targets 125
  - setting for users and groups 126
  - setting up 117
  - uses for 118
- Action Request System
  - console settings 142, 143
  - web services and 145

## action timeout

- Tuner Administration 198
- actions, monitoring multiple tuners 206
- Active Directory
  - automatic discovery and 105
  - troubleshooting 153
  - tuner remote administration access 261
- active limit for target endpoints 83
- adding
  - databases 111
  - directory services 100
  - users to local user database 90
- admin as login name 60
- administering the tuner
  - different ways for 184
  - general process for 189
  - limiting access for 258
  - multiple tuners 196
  - prerequisites for 188
  - securely over SSL 46, 263
- administration port, tuners
  - changing 259
  - default value 259
  - defined 259
  - SSL and 46, 263
- administration tools
  - defined 30
  - overriding profile settings 31
  - when to use 30, 31
- administration, emergency password

console 98  
administration, emergency user name  
    tuner 195  
administrator access  
    primary 86  
    standard 86  
    Tuner Administration 193  
advanced search for targets 123  
advanced settings for directory services 106  
All Endpoints group 120  
Allow (Report Read) permissions 129  
anonymization 295  
Application Packager channel states 226  
applications  
    assigning permissions 128  
    deleting permissions 134  
    version numbers of 66  
applications on console  
    configuring for Deployment Manager 82  
    removing 70  
    restarting after update 67  
    selecting starting 62  
    specifying URLs for 69  
    starting 66  
    stopping 66  
    subscribing 69  
    switching between 61  
    updating 67  
    viewing URLs for 67  
AR database  
    configuring 143  
    user name and password 144  
assigning permissions  
    ACLs 124  
    applications 128  
Atrium Web Service Registry 147  
audience 15  
audit log files, tuner  
    rolling policy for 290  
authentication  
    directory service and tuner 260  
    system settings 56  
authentication using a smartcard 93  
automatic discovery  
    Active Directory and 105  
    when not to use 105  
    when to use 105  
    automatic discovery for Active Directory 105

**B**

bandwidth usage, managing for tuners 270  
base DN  
    using 107  
basic search for targets 122  
binary files for tuners 214  
bind address  
    changing 72  
    defined 72  
bind DN  
    permissions 109  
    using 107  
bind DN user password  
    changing 109  
BMC Customer Support website channels  
    defined 178  
BMC Customer Support website Channels tab in Tuner Administration 224  
BMC Software, contacting 2  
browser access port  
    changing 72, 151  
    default 60  
    defined 72  
browser-based interface  
    CMS 54  
    console 54  
    system settings 54  
    Tuner Administration 184  
browsing for  
    targets 121  
    tuner channels 229

**C**

cache  
    expiration setting for directory services 107  
    new user login and 88  
capabilities, setting and viewing for channels 239  
categories, using to filter channel list 224  
Certificate Manager 45, 262  
certificates

- distributing root securely 40
  - wildcard 41
- certificates, best practices for
  - client-side 37
  - server-side 37
- certificates, console, SSL and 73
- certificates, tuners
  - client-side 47, 264
  - SSL and 45, 262
- changing
  - applications on console 61
  - bind address 72
  - browser access port 72
  - performance settings 75
  - profile with new profile 33
  - user passwords in local user database 91
  - user roles in local user database 92
  - user timeout 71
- channel categories, using to filter channel list 224
- channel groups, using to filter channel list 224
- channel signing 42
- channels
  - changing URLs 231
  - defined 178
  - directories 182
  - mapping between URLs and directories 181
  - signing 42
  - states 225
  - states for Application Packager 226
  - subscribing to 228
  - trusting content 41
  - unsubscribing from 232
  - updates and Daylight Savings Time 238
  - updating 230
  - URLS, specifying for applications 69
  - verifying and repairing 233
  - verifying examples 43
  - viewing URLs 67
- channels on transmitters
  - browsing 229
- channels on tuners
  - categories, using to filter channel list 224
  - changing information 236
  - deleting from tuner 233
  - garbage collection 300
- groups, using to filter channel list 224
- log files 291
- performing actions 228
- required for Tuner Administration 188
- restricting schedule for updates 245
- setting and viewing capabilities 239
- setting update schedule 236
- sorting channel list in Tuner Administration 225
- states 225
- stopping and starting 230
- updates and Daylight Savings Time 238
- viewing information 235
- viewing using Tuner Administration 224
- client-side certificates
  - best practices for 37
  - tuners 47, 264
- CMS
  - access port 72
  - cookies and 63
  - icon 54
  - logging in first time 60
  - logging in to Tuner Administration 194
  - maximum concurrent connections 75
  - overview 54
  - restarting 81
  - SSL and 39
  - timeout for connections 76
  - updating 82
  - updating applications 67
- collections
  - ACLs and 120
  - target type 120
- command-line interface
  - tuner 185
  - Tuner Administration 185
  - versus console 54
  - versus console (browser) 54
- Common Management Services. *See CMS*
- common names
  - remote administration access 261
  - user roles 97
- configuring
  - AR database 143
  - AR settings on console 142

- console to use SSL 73
  - Deployment Manager for console
    - applications 82
    - email notifications 79
    - multiple components 30
    - performance settings 75
    - refresh rate for status pages 210
    - tuners with profiles 184
  - connecting to
    - tuner 197
  - connections, simultaneous
    - Tuner Administration 198, 199, 205
  - console
    - See also* CMS.
    - access port 60, 72
    - configuring AR settings 142
    - configuring for AR database 143
    - configuring for SSL 73
    - defined
    - Getting Started page 62
    - icon of 54
    - log files 77
    - logging in first time 60
    - logging out 60
    - navigation 61
    - removing applications 70
    - restarting 81
    - setting preferences 62
    - subscribing to applications 69
    - system settings 54
    - updating 82
    - updating applications 67
    - versus command-line interface 54
  - console window, starting from
    - Tuner Administration 220
  - Contents button of help window 27
  - conventions for log names
    - channel 291
    - tuner 287, 288
  - cookies
    - CMS and 63
    - troubleshooting 152
  - corruption, checking for tuner workspace 182
  - creating
    - tuner diagnostic reports 282
  - user accounts in local user database 90
  - custom properties
    - deleting for tuners 254
    - tuners 252
  - custom user interaction mode for tuners 242
  - customer support 2
- D**
- data
    - encrypted on tuner 45, 262
  - data source settings 99
  - databases
    - adding 111
    - configuring console for AR System 143
    - editing 111
    - removing 112
    - Report Center and 56
    - synchronizing with directory service 113
  - Daylight Savings Time and schedules 238
  - debug reports
    - tuners 284
  - debugging
    - tuner 220
  - deleting
    - ACLs 134
    - ACLs users 136
    - databases 112
    - directory services 104
    - machine ID from registry 295
    - packages and channels from tuner 233
    - permissions 134
    - tuner custom properties 254
    - users from local user database 92
  - Deny (Report Read) permissions 129
  - Deployment Manager, integration with console 82
  - diagnostic reports
    - tuners 282
  - directories
    - channel for tuner 182
  - directory
    - installation for tuner 179
    - mapping between channels and directories 181
    - workspace for tuner 180
  - directory services

adding 100  
 advanced settings 106  
 automatic discovery and 105  
 base DN settings 107  
 bind DN permissions 109  
 bind DN settings 107  
 cache expiration 107  
 editing 100  
 failover 110  
 groups for ACLs 119  
 limitations 87  
 local user database versus 89  
 mapping users and groups to roles 96  
 Policy Manager and 56  
 remote tuner administration access 260  
 removing 104  
 role identification 108  
 synchronizing with database 113  
 user identification 107  
 disabling tuner diagnostics 282  
 disconnecting administration session  
     tuner 190  
 distinguished names  
     remote administration access 261, 262  
     user roles 97  
 DNS resolution 189  
 documentation 20  
     audience 15  
     organization 26  
 downloading  
     AR database security script 144

## E

editing  
     databases 111  
     directory services 100  
     profiles 32  
 email notifications 79  
 emergency administrator password  
     system setting 98  
     troubleshooting 149  
     Tuner Administration login 195  
 encrypted communication  
     configuring console for 73  
     passwords 36

tuner 45, 262  
 endpoints  
     active limit for 83  
     defined 120  
     response timeout 83  
     target types 120

## F

failover and multiple directory services 110  
 flash storage 294  
 fully interactive mode for tuners 242

## G

garbage collection  
     tuner 300  
 Getting Started page 62  
 groups  
     ACLs for directory service 119  
     filtering channel list with 224  
     mapping roles to 96  
     setting permissions for 126

## H

health-at-a-glance 155  
 help  
     Contents button in 27  
     Index button in 27  
     Search button in 27  
 Help link 27  
 help, online  
     overview of using 27  
 hiding info text 61  
 history log files, channel  
     reading contents of 292  
     rolling policy for 291  
 history log files, console  
     location of 78  
     reading contents 77  
     setting rolling policy 79  
 history log files, tuner  
     reading contents of 288  
     rolling policy for 290  
 HTTPS  
     tuner 46, 263

## I

### icons

- CMS 54
- console 54
- targets 120
- tuner 192

### ID, tuner

idle user timeout 71

imaging machines 293

### importing

SSL certificates 46, 263

inactive user timeout 71

Index button of help window 27

### information

viewing for tuners 211

informational (info) text 61

### Infrastructure Service

- assign profile using 33
- update profile using 32

Infrastructure Service channel, using to update tuners 213

### Infrastructure Status Monitor

tuner settings 273

### inheriting permissions

defined 137

overriding 139

installation directory, tuner 179

### installers

signing 44

interfaces, console (browser) versus command line 54

interfaces, console (browser) vs. command line 184

### introduction

guide 25

tuners 178

### Inventory

Scanner Service 215

scanning machines using Tuner Administration 215

## J

### job timeout

Tuner Administration 198, 200, 205

### jobs

overview 206

stopping, resuming, and retrying for tuners 209

viewing status details 206

JRE Up Since information, for tuners 211

JRE version, viewing for the tuner 211

JVM argument, specifying for tuners 271

JVM properties, viewing 271

## K

### keyword

name for tuner workspace directory 180

## L

launch.log 287

launch.log file (Windows only) 181

### LDAP

*See also* directory services.

SSL and 38

synchronizing data 113

using for remote tuner administration access 260

lib directory, tuner 179

### local user database

adding users 90

changing passwords 91

changing user roles 92

defined 89

directory services versus 89

removing users 92

searching for users 90

viewing logged in users 93

log files, channel 291

naming conventions for 291

reading contents of 292

rolling policy for 291

log files, console

access 77

changing location of 78

finding location of 152

finding storage location 78

history 77

rolling policy for 79

log files, tuner

audit 289

- history 288
    - naming conventions for 287, 288
    - reading contents of 288
    - rolling policy for 290
  - log reports, tuners 285
  - logged in users, viewing in local user database 93
  - logging in
    - console 60
    - Tuner Administration 193
  - logging out
    - console 60
    - Tuner Administration 193
  - login problems
    - multiple users and groups with same name 151
    - troubleshooting 149, 152, 153
  - Logout link 61
- M**
- machine ID 293
  - machine information in Report Center
    - tuner 295
  - mail server, configuring for email notifications 79
  - manually entering components for administration
    - list of tuners 197
  - map.txt file (Windows only) 181
  - mapping roles for directory service users and groups 96
  - marimba.network.detection.address property 297
  - marimba.network.detection.ping.retries
    - property 297
  - marimba.network.detection.policy property 297, 298
  - marimba.primary.url 244
  - marimba.proxy.http.list 268
  - marimba.proxy.http.password 268
  - marimba.proxy.https.list 268
  - marimba.proxy.https.password 268
  - marimba.security.cert.password.timeout 75
  - marimba.security.channels.onlytrusted
    - property 43
  - marimba.security.clientcertpw 75
  - marimba.security.ignoreExpiration property 44
  - marimba.security.noUserOverride property 44
  - marimba.security.ssl.matchdomainonly
  - property 44
  - marimba.security.sslcert 75
  - marimba.security.sslcert property 38
  - marimba.security.trusted.certs property 44
  - marimba.security.trusted.transmitters
    - property 44
  - marimba.tuner.display.nocancel 245
  - marimba.tuner.display.noerrors 243
  - marimba.tuner.display.noprogress 244
  - marimba.tuner.display.nowarnings 243
  - marimba.tuner.enabletaskbaricons 243
  - marimba.tuner.trayicon.menu.about.enabled 245
  - marimba.tuner.trayicon.menu.exit.enabled 245
  - marimba.tuner.trayicon.menu.open.enabled 245
  - marimba.tuner.update.profile property 34
  - maximum
    - concurrent connections 75
    - email body and attachment sizes 79
    - throughput for tuners 270
  - MESH 275
  - mid tier, configuring for 142
  - minimal mode 181
    - autostart channels and 301
    - interaction with network detection 299
    - separate process from tuner 299, 300
  - minituner.exe 299, 300
  - monitor resolution, recommended 61
  - monitor your environment 155
  - monitoring actions
    - for multiple tuners 206
  - multicast, using for network detection 298
  - multiple components
    - configuring 30
  - multiple infrastructure components
    - connecting to 197
    - monitoring actions on 206
    - performing actions on 196
    - resuming actions on 209
    - retrying actions on 209
    - stopping actions on 209
    - viewing action details for 206
- N**
- NAP integration in CMS 115
  - navigation, console 61

Network Access Protection, see NAP 115

network detection

- disabling for tuners 298

- minimal mode and 299

- ping policy 296

- running missed events 299

- tuner properties for 298

- tuners 296

notifications, email 79

NT service 192

## O

online help 27

operators

- capabilities in Tuner Administration 193

- overview of user role 87

overriding inherited permissions 139

overview

- guide 25

- targets 120

- tuners 178

## P

packages

- browsing 229

- changing URLs 231

- defined 178

- deleting from tuner 233

- performing actions 228

- restricting schedule for updates 245

- setting and viewing capabilities 239

- setting update schedule 236

- states 226

- stopping and starting 230

- subscribing to 228

- unsubscribing from 232

- updating 230

- verifying and repairing 233

- viewing information 234, 235

- viewing using Tuner Administration 224

Packages tab in Tuner Administration 224

passwords

- AR database 144

- changing in local user database 91

- emergency administrator 195

encrypted 36

endpoint tuners 83

setting emergency administrator 98

Patch Service

- defined 219

- updating 219

- updating using Tuner Administration 218

performance settings

- changing 75

- configuring 75

permissions

- Access Control Read 125

- Access Control Write 125

- assigning for ACLs 124

- assigning for applications 128

- bind DN 109

- collections and 120

- inheritance 137

- overriding inherited 139

- overview 118

- Policy Manager 128

- Policy Read 128

- Policy Write 128

- Report Center 129

- Report Read (Allow) 129

- Report Read (Deny) 129

- requirements 118

- setting for targets 125

- setting for users and groups 126

- uses for 118

ping network detection policy

- benefits 296

- overview 296

- requirements 296

policies

- log rolling for console 79

- updating using Tuner Administration 216, 218, 220

Policy Manager

- directory services and 56

- updating policies using Tuner Administration 216

- web services and 146

Policy Manager permissions 128

Policy Read permissions 128

- Policy Service
    - defined 216
    - updating 217
  - Policy Write permissions 128
  - port
    - changing for console 72, 151
    - CMS access 60
    - console 72
    - tuner administration 259
  - preferences, setting for console 62
  - prefs.txt file 180
  - prerequisites for administering
    - tuners 188
  - previewing changes
    - tuners 190
  - primary administrators
    - access to Tuner Administration 193
    - logging into the console 195
    - overview of user role 86
  - processing timeout
    - CMS connections 76
  - product support 2
  - profiles
    - changing tuner configuration with 184
    - defined 30
    - name for tuner workspace directory 180
    - overriding of settings 31
    - reassigning 33
    - updates to 214
    - updating 32
    - when to use 30
  - properties
    - tuner 252
    - viewing for the JVM 271
  - properties.txt file 181
  - proxies
    - configuring tuners to use 265
    - exceptions 267
    - types that configurable for tuners 266
    - updating 217
  - Proxy tab in Tuner Administration 265
  - Publish Web Service page 147
- R**
- for tuners 202, 203, 205
  - quorum 83
- R**
- read timeout for CMS connections 76
  - reassigning
    - profiles 33
  - recently used list
    - tuners 198
  - refresh rate
    - configuring for status pages 210
  - re-imaging machines 293
  - remote administration access
    - Active Directory for tuners 261
    - common names 261
    - distinguished names 261, 262
    - setting for tuners 258, 260
    - using common names 262
    - using directory service for tuners 260
  - removing
    - applications 70
    - databases 112
    - directory services 104
    - users from local user database 92
  - repairing
    - packages 233
  - Report Center
    - adding databases for 111
    - editing databases for 111
    - using databases with 56
    - using to define a query for tuners 203
  - Report Center permissions 129
  - Report Read (Allow) permissions 129
  - Report Read (Deny) permissions 129
  - resolution, recommended 61
  - response timeout for endpoints 83
  - restarting
    - applications after update 67
    - console 81
    - tuners 212
  - role identification 108
  - roles, user
    - See user roles*
    - Tuner Administration 193, 194
  - rolling policies for log files

- setting for console 79
  - root certificates, distributing securely 40
  - runchannel program 179
  - runtime.network.detected property 299
  - runtime.network.enabled property 299
  - runtime.network.online property 299
- S**
- Scanner Service
    - defined 215
    - starting 215
  - scanning machines using Tuner
    - Administration 215
  - Schedule tab in Tuner Administration 236
  - schedules
    - restricting for channel updates 245
    - setting for channel updates 236
  - Search button of help window 27
  - searching for
    - special characters in targets 124
    - targets 121
    - users in local user database 90
  - Secure Sockets Layer (SSL)
    - configuring the tuner to use 45, 262
  - security
    - client-side certificates 37
    - distributing root certificates 40
    - installer signing 44
    - script for AR database 144
    - server-side certificates 37
    - SSL and 36
    - SSL-enabled CMS 39
    - SSL-enabled LDAP servers 38
    - trusting channel content 41
    - tuner properties and 43
    - tuner settings 45, 255
    - wildcard certificates 41
  - selecting
    - starting application 62
  - semi-interactive user interaction mode for tuners 242
  - server-side certificates 37
  - Services Control Panel (NT service) 192
  - services, web
    - changing status of 146
- viewing 146
  - setting up ACLs 117
  - showing info text 61
  - signing
    - channels 42
    - installers 44
  - silent user interaction mode for tuners 242
  - Simple Mail Transfer Protocol (SMTP) server, configuring for email notifications 79
  - simultaneous connections
    - Tuner Administration 198, 199, 205
  - smartcard authentication for CMS 93
  - SNMP Agent port 273
  - special characters in search strings 124
  - SSL
    - client-side certificates 37
    - CMS and 39
    - configuring console for 73
    - configuring tuner for 45, 262
    - LDAP servers and 38
    - server-side certificates 37
  - standard administrators, access to
    - Tuner Administration 193
  - starting and stopping
    - applications 66
    - packages and channels 230
    - tuners 192
  - starting application 62
  - states, channels 225
  - status information
    - logged-in user 61, 62
  - status pages, configuring refresh rate 210
  - status reports, tuners 283
  - stdout.log file (Windows only) 181
  - subscribing
    - applications 69
    - packages and channels 228
  - support, customer 2
  - synchronizing data 113
  - System directory (tuner) 180
  - system settings
    - before using applications 56
    - data source 99
    - general 65
    - overview 55

- troubleshooting 149  
user authentication 56, 86
- T**
- tab, in online help window 27  
targets  
    advanced search for 123  
    All Endpoints group 120  
    basic search for 122  
    browsing for 121  
    collections 120  
    defined 120  
    icons for 120  
    searching for 121  
    searching using special characters 124  
    setting permissions for 125  
    types of 120  
taskbar icons  
    CMS 54  
    console 54  
    tuner 192  
technical support 2  
threaddumping 284  
timeout  
    action for Tuner Administration 198  
    endpoint response 83  
    idle users 71  
    job for Tuner Administration 198, 200, 205  
    values of CMS connections 76  
transmitters  
    trusted by tuners 256  
    updating 217  
    updating applications from source 67  
    updating applications from URL 68  
troubleshooting  
    Active Directory 153  
    automatic discovery for Active Directory 105  
    CMS performance settings and IE 76  
    cookies 152  
    finding log files 152  
    log files 77  
    login problems 149, 152, 153  
    multiple users and groups with same  
        name 151  
    new user login 88  
    system settings 149  
    trusting channel content 41  
    user timeout 152  
trusted transmitters  
    best practices for 42  
    defined 256  
    specifying for tuners 256  
Tuner Administration  
    access for operators 193  
    access for primary and standard  
        administrators 193  
    administering one vs. multiple tuners 196  
    browser-based interface 184  
    browsing for channels 229  
    changes requiring disconnecting from  
        tuner 190  
    changing the administration port 259  
    channels required 188  
    command-line interface 185  
    configuring tuners to use proxies 265  
    connecting to tuners 197  
    console (browser) vs. command-line  
        interfaces 184  
    deleting properties 254  
    general process 189  
    logging in 194  
    logging out 195  
    managing bandwidth usage for tuners 270  
    manually entering a list of tuners 197  
    monitoring actions for multiple tuners 206  
    overview 183  
    performing actions on channels 228  
    prerequisites for 188  
    previewing and applying settings 190  
    querying for a list of tuners 202  
    restarting tuners 212  
    scanning machines 215  
    selecting from list of recently used tuners 198  
    setting properties 252  
    setting remote administration access 258, 260  
    setting the user interaction mode for  
        tuners 243  
    specifying trusted transmitters 256  
    starting console window 220  
    stopping and retrying actions 209

- updating Patch Service 218
- updating policies 216
- updating proxies 217
- updating transmitters 217
- updating tuners 213
- user roles for 193, 194
- using a query from Report Center 205
- using SSL 46, 263
- viewing action details for multiple tuners 206
- viewing channel or package information 234
- viewing channels and packages 224
- viewing information about tuners 211
- viewing JVM properties 271
- viewing the date and time when the JRE started 211
- viewing the date and time when the tuner started 211
- viewing the JRE version 211
- viewing the version 211
- Tuner Administrationspecifying JVM arguments for the tuner 271
- tuner program 179
- tuner properties
  - defined 252
  - deleting for tuners 254
  - for user interaction modes 243
  - list of 252
    - marimba.network.detection.address 297
    - marimba.network.detection.ping.retries 297
    - marimba.network.detection.policy 297, 298
  - network detection 298
    - runtime.network.detected property 299
    - runtime.network.enabled 299
    - runtime.network.online 299
    - setting for tuners 252
  - tuner.checkrepair property 182
  - tuner.log file (UNIX only) 287
  - tuner.repairfilter property 182
- tuners
  - Active Directory for remote administration
    - access 261
    - administering 184
    - administering one vs. multiple 196
    - administration port 259
    - anonymization 295
  - background information 293
  - changes requiring disconnecting Tuner Administration 190
  - changing the administration port 259
  - channel directories 182
  - channels required for Tuner Administration 188
  - checking for workspace corruption 182
  - command-line interface 185
  - configuring to use proxies 265
  - connecting to 197
  - creating diagnostic reports 282
  - defining a query in Report Center 203
  - deleting custom properties 254
  - disabling network detection 298
  - features 178
  - flash storage and 294
  - garbage collection 300
  - general process for administering 189
  - icon of 192
  - IDs 295
  - installation directory 179
  - log files 286, 288, 289
  - machine IDs and 293
  - managing bandwidth 270
  - manually entering a list in Tuner Administration 197
  - minimal mode 299, 300
  - missed events and network detection 299
  - network detection 296, 299
    - overview 178
    - prefs.txt file 180
  - prerequisites for administering 188
  - previewing and applying settings 190
  - properties.txt file 181
  - querying for a list 202
  - restarting 212
  - resuming actions 209
  - retrying actions 209
  - scanning machines 215
  - security policies and 43
  - security settings 45, 255
  - selecting from list of recently used tuners in Tuner Administration 198
  - setting custom properties 252

- setting remote administration access 258, 260
- setting the user interaction mode 243
- specifying JVM arguments 271
- specifying trusted transmitters 256
- starting and stopping 192
- starting console window 220
- stopping actions on 209
- stopping jobs on 209
- updates to binaries 214
- updating 213
  - updating Patch Service 218
  - updating policies 216
  - user interaction modes 242
  - user name and password for endpoints 83
  - using a query from Report Center 205
  - using client-side certificates 47, 264
  - using directory service for remote administration access 260
  - using multicast for network detection 298
  - using ping for network detection 296
  - using profiles to change configuration 184
  - using SSL for connections 45, 262
  - viewing channels and packages using Tuner Administration 224
  - viewing information about 211
  - viewing JVM properties 271
  - viewing the date and time when the JRE started 211
  - viewing the date and time when the tuner started 211
  - viewing the JRE version 211
  - viewing the version 211
  - workspace directory 180
- tuners, multiple
  - monitoring actions 206
  - viewing action details 206
- U**
  - unsubscribing from packages and channels 232
  - up since information
    - for tuners 211
  - update from (command) 231
  - update URL, changing for channels and packages 231
  - updates
- Daylight Savings Time and 238
- restricting schedules for channels 245
- scheduling for channels 236
- setting restrictions for channels 245
  - to profiles 214
  - to tuner binaries 214
- updating
  - applications on console 67
  - channels and packages 230
  - console 82
  - policies using Tuner Administration 216, 218
  - profiles 32
  - proxies 217
  - transmitters 217
  - tuners 213
- URLs
  - changing for channels 231
  - specifying for applications 69
  - viewing for applications 67
- user accounts
  - adding to local user database 90
  - changing passwords in local user database 91
  - changing roles in local user database 92
  - creating in local user database 90
  - removing from local user database 92
  - searching in local user database 90
  - viewing logged in users in local user database 93
- user authentication
  - selecting the type 87
  - settings 56, 86
- user database. *See* local user database
- user identification 107
- user interaction modes
  - setting for tuners 243
  - tuner properties 243
  - types for tuners 242
- user names
  - admin 60
  - AR database 144
  - endpoint tuners 83
- user roles
  - administrator 86
  - changing in local user database 92
  - defined 86

- distinguished names 97
- mapping to directory service users and groups 96
- operator 87
- primary administrator 86
- Tuner Administration 193, 194
- using common names 97

user status 62

user timeout 71

- troubleshooting 152

users

- deleting from ACLs 136
- setting permissions for 126

## V

verifying

- channels 43
- packages 233

version information, viewing for

- applications 66
- JRE 211
- tuners 211

viewing action details

- multiple tuners 206
- tuners' status 206

viewing information for

- tuners 206

## W

web services

- changing status of 146
- viewing 146

wildcard certificates 41

Windows

- files in tuner workspace directory 181

Windows NT service 192

Windows registry, preparing for imaging 295

WINS resolution 189

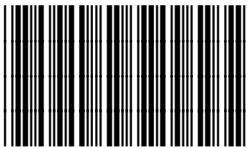
workspace directory

- tuners 180
- using profile name 180
- using tuner keyword 180

workspace, tuner

- checking for corruption 182

write timeout for CMS connections 76



\*\*