



Cisco Videoscape Voyager Vantage Configuration Guide

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks.

MoCA is a trademark of the Multimedia over Coax Alliance.

Other third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Open Source GNU GPL Statement

Cisco® Videoscape Voyager Vantage (Vantage) contain(s), in part, certain free/open source software ("Free Software") under licenses which generally make the source code available for free copy, modification, and redistribution. Examples of such licenses include all the licenses sponsored by the Free Software Foundation (e.g. GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Berkeley Software Distribution (BSD), the MIT licenses and different versions of the Mozilla and Apache licenses). To find additional information regarding the Free Software, including a copy of the applicable license and related information, please go to: (i) for North America

http://www.cisco.com/web/consumer/support/open_source.html, or (ii) for outside North America

http://www.cisco.com/web/consumer/support/open_source.html#~international.

Once at the site, search for the product listing and click on the related items identified. If you have any questions or problems accessing any of the links, please contact: spvtg-external-opensource-requests@cisco.com.

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing or later issued patent.

Copyright

© 2012 Cisco Systems, Inc. All rights reserved. Printed in the United States of America.

Information in this publication is subject to change without notice. No part of this publication may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco Systems, Inc.

Contents

About This Guide	v
Chapter 1 Introducing the Vantage Client User Interface	1
What is the Vantage Client User Interface?.....	2
Chapter 2 Provision Authorization for Services	3
Create an Entitlement Package	4
Determine the EID (Decimal) Value.....	5
Create a SAM Service	6
Set Up Services on Set-Tops	8
What's Next?	9
Chapter 3 Installing and Authorizing Themes	11
Load Theme on BFS.....	12
Allow Subscribers to Select from Multiple Themes	13
Globally Use Default Theme	14
Troubleshooting Themes	15
Chapter 4 Multi-Room DVR	17
Process Overview.....	18
Support MoCA Devices	19
Optional Features.....	24
Chapter 5 Configuring the Vantage Client for VOD Entitlement and Poster Art	25
VOD Entitlement.....	26
Poster Art	28
Chapter 6 Defining Walled Gardens	33
Configuring and Authorizing Walled Gardens.....	34
Walled Garden SAM Service Settings.....	35
Create the Walled Garden Package.....	38
Assign the Walled Garden Package to the Set-Top.....	39

Chapter 7 Configuration Options	41
Downloadable Configuration Files	42
Configuration Variables	43

About This Guide

Introduction

This document provides instructions to provision authorization for services (downloadable objects, DVR, Walled Garden, or other services, such as MR-DVR and Remote DVR) on set-tops operating with the Cisco® Videoscape Voyager Vantage (Vantage) Client User Interface. Vantage is the on-screen interface of your set-top that you use to navigate, control, and interact with your cable TV (CATV) service.

The user interface and your set-top bring a rich, new set of interactive services directly to you.

Vantage is a browser-based application framework that leverages the latest W3C standards to enable a high degree of customization in User Interface (UI) design. Vantage also allows for personalization of the experience at the consumer level while maintaining key elements of the service provider branded experience.

As an example, the consumer can customize their individual experience to get access to the content and applications that matter most to them. This advanced next-generation client delivers a rich and industry-leading consumer navigation and applications experience.

Audience

This document is intended for operators of a Digital Network Control System (DNCS).

Document Version

This is the first formal release of this document.

1

Introducing the Vantage Client User Interface

Introduction

This chapter provides a brief description of the highlights available for systems implementing the Vantage Client User Interface.

In This Chapter

- What is the Vantage Client User Interface?..... 2

What is the Vantage Client User Interface?

The Cisco Vantage Client User Interface is the on-screen interface of a set-top that subscribers use to navigate, control, and interact with their cable television (CATV) service.

The user interface provides a rich, new set of interactive services directly to your subscribers.

Available set-top services may include some or all of the following features:

- **Digital Video Recorder (DVR)** – Allows subscribers to record favorite programs so that they can still go to a friend’s house for dinner and not miss a favorite TV show
- **Pause Live TV** – Allows subscribers to pay for the pizza and come back to the show where they left it
- **High-Definition (HD)** – Provides crystal-clear pictures and sound when compared to standard definition – subscribers won’t want to watch television any other way once they've experienced HD
- **Video-On-Demand (VOD)** – Gives subscribers access to an enormous library of movies and programs that they can watch – when they want to watch them
- **Interactive Services** – Provides access to interactive online content, including data such as news, weather, and online photos. No more leaving the comfort of the couch to access valuable online information
- **Multi-Room DVR (MR-DVR)** - Provides DVR-like functionality to diskless (non-DVR) devices within the home network, allowing users to view all content from any DVRs in the home on any client devices in the home. MR-DVR capability allows users to browse a unified list of all recordings on all devices within the home and stream a program from any DVR to any STB in the home.
- **Remote DVR (R-DVR)** - Provides an interface that is used by DVR Scheduling and DVR Management applications that are running on a remote device but wish to browse or modify DVR assets (recordings) on a DVR set-top device

Refer to the *Cisco Videoscape Voyager Vantage Client User Interface User Guide* (part number OL-26393-01) for additional details.

2

Provision Authorization for Services

Introduction

This chapter provides instructions to provision authorization for the following services on Cisco Vantage-compatible set-tops:

- Downloadable objects, such as applications, themes, logos, and language packages
- DVR
- MR-DVR
- R-DVR

Once the procedures in this section are complete, the authorization package can be added to the applicable set-tops via the DNCS or the Billing System.

For instructions to authorize a Walled Garden service, skip to *Defining Walled Gardens* (on page 33).

In This Chapter

- Create an Entitlement Package 4
- Determine the EID (Decimal) Value..... 5
- Create a SAM Service 6
- Set Up Services on Set-Tops 8
- What's Next? 9

Create an Entitlement Package

Complete the following steps to create a new package for the services or applications that you want to provision. If you have already created the package you want to use for the service, skip to the section *Determine the EID (Decimal) Value* (on page 5).

- 1 On the DNCS Administrative Console, click **Package** from the System Provisioning tab. The Package List window opens.
- 2 Select **File > New** to open the Set Up Package window.
- 3 Enter a unique name for the package.
- 4 Click **Save**. The package is created.

Determine the EID (Decimal) Value

Complete the steps below to determine the EID (decimal) value of the service you want to authorize.

- 1 Open the package you will use to authorize the service and record the EID (decimal) value: _____.

Set Up Package

Package Name: DVR_srv

EID: 11e (hex)

Duration: ☒ Unlimited ☐ Limited

Start Date: 12/31/1969

Start Time: 07:00:00 PM

Length: 1 days 1 hours 1 minutes

☒ Pay Per View

Right To Copy: ☒ Allowed

☒ Impulse Pay Per View

Preview Buy Window Purchase Modes

Start Date: MM/DD/YYYY

Start Time: HH:MM:SS AM

Duration: 0 hours 0 minutes

☒ Allow Event Extension

Save Cancel Help

- 2 Click **Cancel** to close the Set Up Package window.
- 3 In the Package List window, select **File > Close** to close the window.
- 4 Continue with Create a SAM Service.

Create a SAM Service

Complete the following steps to create a SAM service for the package you created.

Note: Multiple SAM services can be associated with one entitlement package.

- 1 From the DNCS Administrative Console, select the **Application Interface Modules** tab.
- 2 Click the **SAM Service** button. The SAM Service List window opens.
- 3 Click **File > New**. The Set Up SAM Service window opens.
- 4 Configure the SAM Service variables per the guidelines below.
 - **Service Name** (required) - This name is only available and shown to users of the DNCS who have access to the SAM Services List. Make this descriptive enough to understand which service is being offered. End users will not see this field.
 - **Short Description** (required) - The short description must match one of the values defined in this document; the Vantage UI will use these short description values to determine if those services are being provisioned.

The following short description names are reserved for provisioning services. Each of these short descriptions must only be used once per system and must be used **exactly** as shown.

Service Type	SAM Short Description
Brick package	_BASE
MR-DVR	_MRDV Note: Before you set up a SAM Service for MR-DVR, refer to the <i>Multi-Room DVR</i> (on page 17) chapter for an overview of the end-to-end process required to support the MR-DVR feature.
Remote DVR	_RDVR
DVR	_SADV
Switched Digital Video (SDV)	_SASD
Downloadable objects	_<downloadable package ID> Note: See the <i>Configuring Downloadable Objects for Cisco Videoscape Voyager Vantage</i> (part number OL-26414) document for details.
Walled Gardens	_<reserved walled garden ID> Note: See the <i>Defining Walled Gardens</i> (on page 33) chapter for details.

- **Long Description** - The long description may be used to clarify the short description.
- **Application URL** - The application URL provides additional information for how the service is authorized. Enter **DummyURL;eid=<EID decimal value>**; using the EID information you recorded in step 1 of the *Determine the EID (Decimal) Value* (on page 5) procedure.
Note: One package can support multiple services by reusing the EID information for each associated service.

- **Logo** - Enter 0 (zero).
- **Parameter** - Select the bullet next to **Number** and type 0 in the field.

Example: Set Up SAM Service Window

Service ID: 134

Service Name: DVR

Short Description: _SADV

Long Description: Enable DVR Service

Application URL: DummyURL;EID=8 Select...

Logo: 0

Parameter: Number 0 String

Save Cancel Help

- 5 Click **Save**.

Set Up Services on Set-Tops

Complete the following steps to set up service(s) on a set-top.

WARNING! Before you perform these steps for MR-DVR service, read the *Multi-Room DVR* (on page 17) chapter and complete the procedures applicable to your configuration.

- 1 From the DNCS Administrative Console, select the **Home Element Provisioning** tab.
- 2 Click the **DHCT** button. The DHCT Provisioning window opens.
- 3 Click the **Open** button and enter the MAC Address, IP address or serial number of the target DHCT.
- 4 Click the **Continue** button. The Set Up DHCT window opens.
- 5 Click the **Secure Services** tab.
- 6 Click the service package name in the Available window and click the **Add** button to move the package to the Selected window.
- 7 Click the **Save** button.

The screenshot shows the 'Set Up DHCT' window with the 'Secure Services' tab selected. The window contains the following elements:

- MAC Address:** 00:23:BE:64:68:CA
- Secure Element Serial Number:** 00:23:BE:64:68:CA
- Key Certificate:**
 - Powerkey name: C=US,O=Scientific-Atlanta,OU=Scientific-Atlanta,Mexico,CN=PK0002debffdfb
 - Buttons: Clear, Load from batch CD...
- Packages:**
 - Available:** VOD_PreEncrypt, Vod_svc, terFy_test, terry_test2
 - Selected:** Avail, Mcdvr_svc, Dvr_svc
 - Buttons: Add >>, << Remove
- Options:**
 - ☒ IPPV Enable
 - IPPV Credit Limit: 0
 - Max. IPPV Events: 0
 - ☒ DMS Enable, ☒ DIS Enable, ☐ Analog Enable
 - ☐ Fast Refresh Enable
 - Location X: 0, Y: 0
- Buttons:** DHCT Instant Hit, Poll DHCT for IPPV Data, Save, Cancel, Help

What's Next?

Repeat the procedures in this chapter for each service you want to authorize.

Some services require additional steps to complete implementation for the associated feature. Use the following table to determine next steps for the service you created.

Service Type	Refer to
MR-DVR	<i>Multi-Room DVR</i> (on page 17)
Downloadable Objects	<i>Configuring Downloadable Objects for Cisco Videoscape Voyager Vantage</i> (part number OL-26414)
Walled Gardens	<i>Defining Walled Gardens</i> (on page 33)

3

Installing and Authorizing Themes

Introduction

This chapter provides instructions to implement the Vantage themes feature.

In This Chapter

- Load Theme on BFS..... 12
- Allow Subscribers to Select from Multiple Themes..... 13
- Globally Use Default Theme 14
- Troubleshooting Themes 15

Load Theme on BFS

For instructions to create, load, and authorize a theme object, refer to *Configuring Downloadable Objects for Cisco Videoscape Voyager Vantage* (part number OL-26414).

Then, proceed with procedures below to modify the global configuration file and set up DNCS to support themes.

Allow Subscribers to Select from Multiple Themes

Modify Global Configuration File to Support Multiple Themes

Complete the following steps to modify the global configuration file to allow subscribers to select from multiple themes.

Note: Only codes that have been authorized will be made available to the end-user. Instructions to add and authorize themes are provided in *Configuring Downloadable Objects for Cisco Videoscape Voyager Vantage* (part number OL-26414).

- 1 Open an xterm window on the DNCS.
- 2 Open the **globalconfig.txt** file in a text editor from the following directory path:
`/dvs/dvsFiles/BFS/DNCS/msoconfig/rtn/<default hub ID>/`

Note: 0 is typically the default hub.

- 3 Ensure that the **ciscoSg/look/skinStyleList** parameter contains a comma-separated list of the 4-character IDs of themes you wish to offer.

Example:

```
ciscoSg/look/skinStyleList:cbhd,cbhd
```

- 4 **Note:** You need to have at least one 4-character ID assigned to this parameter to support themes. The first in the list will be the default when the set-top boots up. Type # at the beginning of any line where the parameter is **ciscoSg/look/skinStyle** to disable the parameter.

Example:

```
#ciscoSg/look/skinStyle:cbhd
```

Note: If you do not disable this parameter, it will override your settings from step 4.

- 5 Save the file and exit the text editor.

Add the Theme Package

Complete the steps below to enable multiple themes.

- 1 From the DNCS Administrative Console, select the **Home Element Provisioning** tab.
- 2 Click the **DHCT** button. The DHCT Provisioning window opens.
- 3 Click the **Secure Services** tab.
- 4 From the **Available** window, select the package names for the themes you want to use; then, click the **Add** button to move the packages to the **Selected** window.
- 5 If you need to remove a theme, select the theme package name from the **Selected** window; then, click the **Remove** button to move it to the **Available** window.
- 6 At the bottom of the window click **DHCT Instant Hit**.
- 7 Click the **Save** button.

Globally Use Default Theme

Modify Global Configuration File to Use Default Theme for All Set-Tops

Complete the following steps to modify the global configuration file to use the default theme for all set-tops.

Note: You will need to know the package name from the config.xml file for the theme you wish to use.

- 1 Open an xterm window on the DNCS.
- 2 Open the **globalconfig.txt** file in a text editor from the following directory path:
`/dvs/dvsFiles/BFS/DNCS/msoconfig/rtn/0/`

- 3 Ensure that the **ciscoSg/look/skinStyleList** parameter has the 4-digit ID of the theme you wish to use as the first value in the comma-separated list.

Example:

```
ciscoSg/look/skinStyleList:cbhd, cbsd
```

- 4 Ensure the following parameters are configured with the 4-digit ID you are using as the default:

- **ciscoSg/look/skinStyle**
- **com_antplc_tvlib.tvlib_config_global_theme**
- **com_antplc_tvlib.tvlib_config_global_default_theme**

Example:

```
ciscoSg/look/skinStyle:cbhd  
com_antplc_tvlib.tvlib_config_global_theme: cbhd  
com_antplc_tvlib.tvlib_config_global_default_theme: cbhd
```

- 5 Save the settings and exit the text editor.
- 6 Perform the steps in the *Add the Theme Package* (on page 13) section to complete theme set-up on the DNCS.

Troubleshooting Themes

Solution 1

Complete the following steps to troubleshoot the set-top you are using for verification.

Note: You will need to know the package name from the config.xml file for the theme you wish to use.

- 1 From the DNCS Administrative Console, select the **Home Element Provisioning** tab.
- 2 Click the **DHCT** button. The DHCT Provisioning window opens.
- 3 Click the **Open** button and enter one of the following criteria for the target set-top:
 - **MAC Address**
 - **IP Address**
 - **Serial number**
- 4 Click the **Continue** button. The Set Up DHCT window opens.
- 5 Click the **Secure Services** tab and verify the package name of the desired theme appears in the **Selected** window.
- 6 At the bottom of the window, click **DHCT Instant Hit**.
- 7 Click the **Save** button.
- 8 Reboot the set-top.
- 9 Select **Menu > Settings > Appearance** and confirm that the theme package name you selected appears.
- 10 Did the theme package name appear as expected?
 - If **yes**, you have successfully completed theme setup.
 - If **no**, perform the procedures provided in the *Solution 2* (on page 15) section.

Solution 2

Complete the following steps using the MAC Address for the set-top you are troubleshooting.

- 1 Open an xterm window on the DNCS.
- 2 Type `$ modDhctCfg -s <MAC Address>` and press **Enter**.
- 3 Reboot the set-top.

4

Multi-Room DVR

Introduction

This chapter provides instructions to authorize the MR-DVR service on Cisco Vantage-compatible set-tops.

In This Chapter

■ Process Overview	18
■ Support MoCA Devices	19
■ Optional Features.....	24

Process Overview

Vantage 3.0 features MR-DVR, which provides DVR-like functionality to diskless (non-DVR) devices within the home network, allowing users to view all content from any DVR in the home. MR-DVR capability allows users to browse a unified list of all recordings on all devices within the home and stream a program from any DVR to any STB in the home. Users can perform trick-plays (for example, Fast Forward, Rewind, Skip, Back), pause or stop a program in one room and resume it in another, and manage and schedule recordings just as if they were sitting at one of the home DVRs.

The following table lists the procedures you need to complete to fully implement the MR-DVR feature, where to find instructions, and where to perform the procedures:

Procedure (What do I need to do?)	Reference Chapter or Document (Where are the instructions?)	Interface (Where do I perform the procedures?)
Update system configuration file (config.ini) for MR-DVR service on BFS (global option)	<i>Configure MoCA using the config.ini File</i> (on page 19)	Perform once on DNCS or perform next procedure every time you want to enable the MoCA if on a set-top
Enable the MoCA Interface MIB Object (set-top specific option)	<i>Enable the MoCA Interface MIB Object</i> (on page 20)	DNCS
Install Point of Entry (POE) Filter	<i>MoCA Installation and Troubleshooting Reference Guide</i> (part number 4031235)	Subscriber's home
Provision Authorization for MR-DVR Service	<i>Provision Authorization for Services</i> (on page 3)	DNCS or Billing System WARNING! Before you perform these steps for MR-DVR service, make sure that the POE filter for this home is installed.
Confirm the MIB objects for MoCA	<i>Confirm the MIB objects for MoCA</i> (on page 21)	DNCS
Confirm MoCA settings on diagnostic screens	<i>Understanding Diagnostic Screens for Cisco Videoscape Voyager Vantage Implementation Design Guide</i> (part number OL-26413-01)	Subscriber's home
Verify MR-DVR Service on Set-Top	<i>Cisco Videoscape Voyager Vantage Client User Interface User Guide</i> (part number OL-26393-01)	Subscriber's home
Set Friendly Name (Optional)	<i>Cisco Videoscape Voyager Vantage Client User Interface User Guide</i> (part number OL-26393-01)	Subscriber's home

Support MoCA Devices

To properly implement the MR-DVR service, refer to the *MoCA Installation and Troubleshooting Reference Guide* (part number 4031235), which contains installation guidelines, performance verification steps, and troubleshooting measures for devices that support a multi-room network over Multimedia over Coax Alliance (MoCA™). Multi-room networks allow client devices (non-DVR set-tops) to stream content from a server device (DVR set-top) that has recorded linear content.

Use the *MoCA Installation and Troubleshooting Reference Guide* (part number 4031235) to understand where to install the MoCA POE filter and MoCA set-tops with respect to cable splitters and amplifiers. The document is also helpful to verify links between MoCA set-tops and troubleshoot faulty installations.

Configure MoCA using the config.ini File

You can enable or disable MoCA using a file on BFS. This file is named config.ini. This file specifies whether MoCA should be enabled automatically on assignment of the _MRDV package.

You may not need to perform the following procedure. By default, the config.ini file built in to the the set-top image has a default setting such that the set-top will be enabled for MoCA service whenever the MR-DVR service (_MRDV) is authorized.

If you prefer to enable the MoCA radio MIB Object manually using a SNMP set command instead of automatically when the _MRDV package is assigned to the set-top, you will need to follow the instructions below and then refer to *Enable the MoCA Interface MIB Object* (on page 20).

- 1 On the DNCS, edit the config.ini file. The following are the lines for the default setting.

```
[moca]
enable_moca_by_service = 1
```
- 2 If you do NOT want to enable MoCA with config.ini, change the lines to:

```
[moca]
enable_moca_by_service = 0
```
- 3 Modify or put the file on BFS, typically in /bfs/msoconfig/rtn/0/config.ini which updates settings on all set-tops.
- 4 If necessary, send the service package to set-top(s) for the _MRDV service.

Enable the MoCA Interface MIB Object

Complete the following steps to verify and manually set the MoCA interface MIB Object to enabled using SNMP commands. This is only needed if you do not choose to have the MoCA interface automatically enabled on assignment of the _MRDV package.

- 1 From the DNCS, open an xterm and log in as root user.
- 2 From the DNCS \$ prompt, type the following command and then press **Enter** to determine if the MoCA Interface MIB object is already enabled:

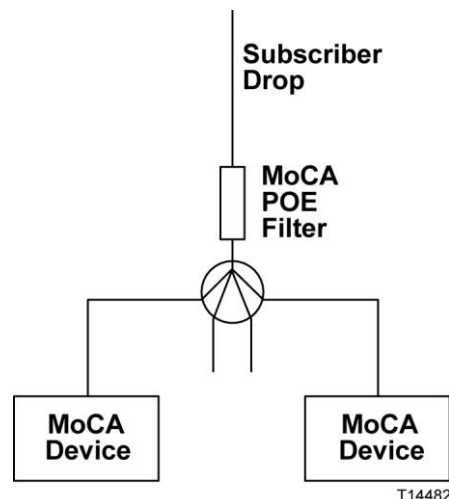
```
snmpget -v2c - cpublic [set-top IP address].1.3.6.1.4.1.31621.1.1.1.1.1.3
```
- 3 Is the object set to **true**?
Example: MOCA11-MIB::mocalfEnable.3 true
 - If **yes**, then the MoCA Interface MIB object is already enabled.
 - If **no**, type the following command and then press **Enter** to enable the object:

```
snmpset -v2c - cpublic [set-top IP address].1.3.6.1.4.1.31621.1.1.1.1.1.3 i 1
```
- 4 Repeat step 1 to verify the object is enabled.
- 5 If you want to confirm other MIB objects, continue with the next section. Otherwise, type **exit** and press **Enter** to close the window; then, proceed to the *Optional Features* (on page 24) section.

Install POE Filter

The POE filter (see *MoCA Point of Entry Filter Data Sheet*, part number 7016817) is a 1002 MHz low-pass filter which is installed at the subscriber drop. It prevents interference between MoCA devices in homes connected to the same tap. As shown in the Basic Installation Wiring Example below, the POE filter should be connected between the ground block and the splitter.

Basic Installation Wiring Example



Confirm the MIB objects for MoCA

Complete the following steps to view the current MIB Object settings for MoCA on a specific set-top.

- 1 From the DNCS, open an xterm window and log in as root user.
- 2 From the DNCS \$ prompt, type the following command and then press **Enter**:

```
% snmptable -v 2c -c public -Os [set-top IP address]
.1.3.6.1.4.1.31621.1.1.1.1
```

Example command line: % snmptable -v 2c -c public -Os 10.10.1.21
 .1.3.6.1.4.1.31621.1.1.1.1

Example Output:

```
# find the moce index
```

```
$snmpwalk -Oq -v2c -cpublic 10.10.1.21 IF-MIB::ifType
```

```
IF-MIB::ifType.1 ethernetCsmacd
```

```
IF-MIB::ifType.3 mocaVersion1
```

```
IF-MIB::ifType.5 ethernetCsmacd
```

```
IF-MIB::ifType.6 other
```

```
IF-MIB::ifType.7 ethernetCsmacd
```

```
#view the netstats of the moca interface
```

```
$snmpwalk -Oq -v2c -cpublic 10.10.1.21 IF-MIB::ifTable |grep
"\.3"
```

```
IF-MIB::ifIndex.3 3
```

```
IF-MIB::ifDescr.3 eth1
```

```
IF-MIB::ifType.3 mocaVersion1
```

```
IF-MIB::ifMtu.3 1500
```

```
IF-MIB::ifSpeed.3 10000000
```

```
IF-MIB::ifPhysAddress.3 2:23:be:bd:d2:86
```

```
IF-MIB::ifAdminStatus.3 down
```

```
IF-MIB::ifOperStatus.3 down
```

```
IF-MIB::ifLastChange.3 0:0:00:00.00
```

```
IF-MIB::ifInOctets.3 0
```

```
IF-MIB::ifInUcastPkts.3 0
```

```
IF-MIB::ifInNUcastPkts.3 0
```

```
IF-MIB::ifInDiscards.3 0
```

```
IF-MIB::ifInErrors.3 0
```

```
IF-MIB::ifInUnknownProtos.3 0
```

```
IF-MIB::ifOutOctets.3 0
```

```
IF-MIB::ifOutUcastPkts.3 0
```

```
IF-MIB::ifOutNUcastPkts.3 0
```

Chapter 4 Multi-Room DVR

```
IF-MIB::ifOutDiscards.3 0
IF-MIB::ifOutErrors.3 0
IF-MIB::ifOutQLen.3 0
IF-MIB::ifSpecific.3 SNMPv2-SMI::zeroDotZero
####
# Steps to enable
####
## 1) get the current state
$snmpget -Oq -v2c -cpublic 10.10.1.21
.1.3.6.1.4.1.31621.1.1.1.1.1.3
MOCA11-MIB::mocaIfEnable.3 false
## 2) Set to true (1= true & 2= false)
$snmpset -Oq -v2c -cpublic 10.10.1.21
.1.3.6.1.4.1.31621.1.1.1.1.1.3 i 1
MOCA11-MIB::mocaIfEnable.3 true
## 3) verify the set
$snmpget -Oq -v2c -cpublic 10.10.1.21
.1.3.6.1.4.1.31621.1.1.1.1.1.3
MOCA11-MIB::mocaIfEnable.3 true

#View all moca configuration and stats
$snmpwalk -Oq -v2c -cpublic 10.10.1.21 .1.3.6.1.4.1.31621
MOCA11-MIB::mocaIfEnable.3 true
MOCA11-MIB::mocaIfChannelMask.3 16384
MOCA11-MIB::mocaIfPowerControl.3 true
MOCA11-MIB::mocaIfTxPowerLimit.3 0
MOCA11-MIB::mocaIfBeaconPowerLimit.3 0
MOCA11-MIB::mocaIfPowerControlTargetRate.3 235
MOCA11-MIB::mocaIfPrivacyEnable.3 true
MOCA11-MIB::mocaIfPreferredNC.3 false
MOCA11-MIB::mocaIfAccessEnable.3 false
MOCA11-MIB::mocaIfPhyThreshold.3 95
MOCA11-MIB::mocaIfPhyThresholdEnable.3 false
MOCA11-MIB::mocaIfStatus.3 noLink
MOCA11-MIB::mocaIfLinkUpTime.3 0
MOCA11-MIB::mocaIfSoftwareVersion.3 1.35.117
MOCA11-MIB::mocaIfMocaVersion.3 moca10
MOCA11-MIB::mocaIfBeaconVersion.3 moca10
MOCA11-MIB::mocaIfMacAddress.3 2:23:be:bd:d2:86
MOCA11-MIB::mocaIfNodeID.3 0
MOCA11-MIB::mocaIfName.3 eth1
```



```

MOCA11-MIB::mocaIfNumNodes.3 0
MOCA11-MIB::mocaIfNC.3 0
MOCA11-MIB::mocaIfBackupNC.3 0
MOCA11-MIB::mocaIfRFChannel.3 d1
MOCA11-MIB::mocaIfLOF.3 d1
MOCA11-MIB::mocaIfTabooChannelMask.3 243712
MOCA11-MIB::mocaIfNodeTabooChannelMask.3 243712
MOCA11-MIB::mocaIfCapabilityMask.3 357908984
MOCA11-MIB::mocaIfQAM256Capable.3 false
MOCA11-MIB::mocaIfTenPacketsAggrCapable.3 false
MOCA11-MIB::mocaIfStatusEntry.23.3 "53ce"
MOCA11-MIB::mocaIfTxPackets.3 Wrong Type (should be Counter32): 0
MOCA11-MIB::mocaIfTxDrops.3 Wrong Type (should be Counter32): 0
MOCA11-MIB::mocaIfRxPackets.3 Wrong Type (should be Counter32): 0
MOCA11-MIB::mocaIfRxCorrectedErrors.3 Wrong Type (should be Counter32): 0
MOCA11-MIB::mocaIfRxDrops.3 Wrong Type (should be Counter32): 0
MOCA11-MIB::mocaIfEgressNodeNumFlows.3 0
MOCA11-MIB::mocaIfIngressNodeNumFlows.3 0
MOCA11-MIB::mocaIfIngressNodeNumFlows.3 No more variables left
in this MIB View (It is past the end of the MIB tree)

```

- 3 Edit the MoCA parameters as needed.
- 4 Save the settings.
- 5 Type **exit** and press **Enter** to close the window.

Verify MoCA

Complete the steps below to verify that the MoCA support is enabled.

- 1 Is the MoCA LED (home icon) on the front panel of the set-top lit?
 - If **yes**, MoCA support is properly enabled.
 - If **no**, continue with step 2.
- 2 From the **Home Networking** category of the On-Screen Diagnostic home page, browse to the second page of the **MoCA Summary**.
- 3 From the MoCA Interface details, set the **Interface/Beacon** status to **Enabled**.
- 4 From an SNMP browser or client, set the value of the MIB parameter **MocaIfStatus** in the **mocaIfStatusTable** to **3 (linkUp)**.

Optional Features

Use the Vantage on-screen interface for configuring optional features, such as naming each DVR set-top on the home network (if desired), and services on your set-top. For more information, see the *Cisco Videoscape Voyager Vantage Client User Interface User Guide* (part number OL-26393-01).

5

Configuring the Vantage Client for VOD Entitlement and Poster Art

Introduction

This chapter provides instructions to configure the Vantage Client to support VOD Entitlement and Poster Art.

In This Chapter

- VOD Entitlement 26
- Poster Art 28

VOD Entitlement

Configuring the Vantage VOD Client Platform

The Vantage software includes a default config.ini file that you need to customize with system-specific information to support your specific VOD catalogs. This section provides guidelines to edit the config.ini file and place it on the BFS server. Once the customized file is on BFS, it will override the default version.

Gather Data for the VOD Section of the config.ini File

You will need to provide values for the following VOD-related fields included in the default config.ini file:

- **uids:** Enter the hexadecimal value for the unique ID used by your VOD server to identify a catalog. In the example provided in the table below, the UID for On-Demand is 25601.
Note: You can precede the value with 0x, if desired.
- **types:** Enter the catalog type, either **vod** (Video-On-Demand) or **svod** (Subscription-Video-On-Demand), as appropriate.
Note: The entry is not case sensitive.
- **samIds:** From the DNCS, find the SAM Service ID associated with the specific catalog.
Note: For SVOD, the Sam Service's application URL must contain an EID value. Otherwise, the associations in this file will not be set up properly.

Create a table similar to the example below to gather the catalog information you need to edit the config.ini file.

Field	Catalog 1	Catalog 2	Catalog 3
uids (hexidecimal)	25601	11a8006a	0x25625
types	VOD	SVOD	SVOD
samIds (decimal)	345	329	367

Edit the VOD Section of the config.ini File

Follow the steps below to create a customized config.ini file on the BFS server.

Note: Refer to the data you collected for the *Gather Data for the VOD Section of the config.ini File* (on page 26) section. The examples provided correspond to the table in that section.

- 1 Open an xterm window on the DNCS.
- 2 Copy the default config.ini file that is currently on the BFS server to a separate directory.
- 3 Record the directory path where you stored the copied file:
_____.
- 4 Open a text editor and navigate to the copied config.ini file.
- 5 Navigate to the VOD section and add the uids.
Note: Entries are separated by commas.
Example: uids=25601,11a8006a,0x25625
- 6 Add the samids in the order corresponding to the uids. For example, if 0x25625 is third in the list of uids, then the values for that catalog should be third for every field.
- 7 Add the types in the order corresponding to the uids.
Examples:
uids=25601,11a8006a,0x25625
samids=345,329,367
types=vod,svod,svod
- 8 Save the settings and exit the text editor.
- 9 Close the xterm window.

Poster Art

If your site does not have a high bandwidth interactive WAN connection, place poster art images on an inband transport that are to be downloaded by the set-top.

The poster art images will be transported as a single .tar archive file; this file is the Poster Art TAR File.

The Poster Art TAR file (posterart.tar) will be placed on an in-band BFS data carousel (/rtnclient/posterart). Given the size of the file and the limited number of tuners, downloading the file will take several minutes even when a tuner is idle. The Cisco VOD Client Platform will download the Poster Art TAR File as a background task, expand archive and then place in a local file directory (/tmp/VodArt). The background task should be initiated at night when tuners are likely to be available.

Similar to EPG program guide downloads, Poster Art TAR File downloads may pre-empt video rendering services but will not pre-empt a recording.

A single default image (default.jpg) can be placed on the in-band BFS data carousel (/rtnclient/posterart); this image is the Service Provider Defined Default Poster Art Image. This default image is to be displayed when the tar file has not been downloaded or an image is not found in the tar file. This small file will be downloaded at a high priority when the Cisco VOD Client Platform is initialized. If defined, the Service Provider Defined Default Poster Art Image will take precedence over the Platform Default Poster Art Image.

Before You Begin

Associate Images with Assets

Follow the instructions for your VOD server software to associate poster art images with assets.

Create TAR File for Poster Art

Create a TAR file named **posterart.tar** that includes the images you have associated with assets. The images must be in jpg format that are 216 pixels wide by 275 pixels high. The TAR file must not exceed 15 MB.

Copy or move the TAR file to a directory in the DNCS. Record the directory where you placed the file for use in the procedures that follow:

Store Default Poster Art Image

The default poster art image must be in jpg format that is 216 pixels wide by 275 pixels high.

Save the default poster art image to a directory in the DNCS as **default.jpg**. Record the directory where you placed the image for use in the procedures that follow:

What's Next?

When you have completed storing the posterart.tar and default.jpg files on the DNCS, proceed with the instructions in the *Create BFS Directories for Poster Art* (on page 29) section.

Create BFS Directories for Poster Art

Complete the steps below to create a BFS directory on the DNCS for poster art images.

Notes:

- The instructions include steps to set up both a default image and asset-associated images. The default image will appear for assets that do not have an associated image.
 - These instructions assume that you have already installed the Vantage software and set up the **rtnclient** server on the BFS server. The steps below use an example directory of rtnclient/posterart. You do not have to use the rtnclient/posterart directory that is used in our example. If you use a different directory, note the new location as you will need it in subsequent procedures.
- 1 From the DNCS Administrative Console, click the **Application Interface Modules** tab.
 - 2 Click the **BFS Client** button.
 - 3 Select the **rtnclient** cabinet.
 - 4 Click **File**; then select **New Directory** from the file menu bar.
 - 5 In the **Directory Name** field, type `posterart`.
Note: The name must be one word in lowercase.
 - 6 Click **Save**.
 - 7 Continue with the instructions in the *Add Links for Poster Art* (on page 30) section.

Add Links for Poster Art

Complete the following steps to add links to the BFS directory for image files.

Note: Perform this procedure twice to add links for both the default image and the asset-associated image files.

- 1 From the BFS Server list, click **rtncclient**, then select **posterart** from the list of available directories.
- 2 Click **File**; then select **New Link** from the file menu bar.
- 3 In the **Link Name** field, enter one of the following terms:
 - If you are setting up the default image, type `default.jpg`.
 - If you are setting up the asset-associated image files, type `posterart.tar`.
- 4 Ignore the **Source Name** field.
- 5 Click the **Select** button associated with the Linked Path field.
- 6 Navigate to the file you are linking:
 - If you are setting up the default image, select the **default.jpg** file you saved to the DNCS. Refer to the directory path you recorded in the *Before You Begin* (on page 28) section.
 - If you are setting up the asset-associated image files, select the **posterart.tar** file you saved to the DNCS and select it. Refer to the directory path you recorded in the *Before You Begin* (on page 28) section.
- 7 Click **OK** to set up the link.
- 8 Click **Save**.
- 9 Close the BFS window.
- 10 Continue with the instructions in the *Edit the config.ini File* (on page 31) section.

Edit the config.ini File

Complete the following steps to associate the BFS location where you have placed your posterart.tar and default.jpg files with the posterartpath parameter.

- 1 Open an xterm window on the DNCS.
- 2 Open the **config.ini** file in a text editor.
- 3 Locate the parameter named **posterartpath**?
- 4 If necessary, add or edit the parameter as follows:
`posterartpath=<BFS server>/<directory>/<link>`
Example: If you used the recommended naming convention from the previous procedures, you will add a line or edit the settings to match the following string:
`posterartpath=/bfs/rtnclient/posterart`
- 5 Save the settings and exit the text editor.
- 6 Close the xterm window.

After you complete this procedure, the poster art images will load during the next maintenance window.

Verify Poster Art Setup

Complete the following steps to verify that the poster art image files are set up properly.

- 1 Power off a set-top for two minutes to initiate a maintenance window.
- 2 Power the set-top on.
- 3 Launch the VOD application.
- 4 Select an asset that does not have poster art associated with it to verify that the default image appears.
- 5 Select an asset that does have an associate poster art image to verify the correct image appears.

6

Defining Walled Gardens

Introduction

This chapter provides instructions to define Walled Gardens on Cisco Vantage set-tops.

In This Chapter

- Configuring and Authorizing Walled Gardens 34
- Walled Garden SAM Service Settings..... 35
- Create the Walled Garden Package..... 38
- Assign the Walled Garden Package to the Set-Top 39

Configuring and Authorizing Walled Gardens

The signaling from the DNCS to provision Walled Garden services is accomplished by defining Walled Garden SAM service definitions on the DNCS, one for each Walled Garden service that is to be provisioned.

You can define up to 10 generic Walled Garden services for use on Vantage. Additionally, two special Walled Garden services for "My Account" and "App Store" can be defined.

Walled Garden SAM Service Settings

Use the following fields when you create and manage Walled Garden services on the DNCS.

Field	Description
Service Name (required)	The name of the service is only available and shown to users of the DNCS who have access to the SAM Services List. Make this descriptive enough to understand what Walled Garden service is being offered. Subscribers will not see this field. Example: Walled Garden – App Store
Short Description (required)	The Short Description is from a set of well-known values defined in the following list. The set-top uses these short description values to determine whether those services should be displayed on the Vantage UI. If you are configuring the Walled Garden service to appear in the EPG, this field is used as the channel indicator. Example: _WG00 The following short description names are reserved for provisioning Walled Garden services. Each of these short descriptions must only be used once per system and must be used <i>exactly</i> as shown. ■ _WG00 - Main service for Walled Garden ■ _WG01 - Service for Walled Garden 01 ■ _WG02 - Service for Walled Garden 02 ■ _WG03 - Service for Walled Garden 03 ■ _WG04 - Service for Walled Garden 04 ■ _WG05 - Service for Walled Garden 05 ■ _WG06 - Service for Walled Garden 06 ■ _WG07 - Service for Walled Garden 07 ■ _WG08 - Service for Walled Garden 08 ■ _WG09 - Service for Walled Garden 09 ■ _WGMA - Service for Walled Garden "My Account" ■ _WGAP - Service for Walled Garden "App Store"
Long Description	The Long Description is for meaningful display to the subscriber. This field appears in the menu and/or in the grid cell of the EPG, as indicated by the options in the Application URL field, and is up to you. Example: Add Applications

Field	Description
Application URL	The Application URL provides additional information for how the Walled Garden service can be accessed. It contains the application name and additional attributes, separated by semicolons.

■ **inEPG**

- **0** (zero) – Service is not displayed in the EPG
- **1** (or name) – Service is displayed in the EPG (default)

Note: The inEPG flag is independent of whether the service is channel-mapped or not.

Channel Mapped	inEPG Flag	Result
No	X	Not listed in EPG
Yes	0	Not listed in EPG; Direct tune brings up the service
Yes	1	Listed in EPG; Direct tune brings up the service

inMenu

- **0** (or name not present) – Service is not displayed in the Applications Menu (default)
- **1** (or name is present) – Service is displayed in the Applications Menu

■ **eid** – The authorization EID (decimal) of the service. This is to ensure that you can authorize this Walled Garden service to individual STBs. See *Create the Walled Garden Package* (on page 38) for details on creating a Walled Garden package and authorizing a set-top for the package.

■ **url** – The URL to access the service. This must be the last attribute of the Application URL so that it is not required to be escaped

Format:

```
wgarden://wgarden;inEPG=0;inMenu=1;eid=[xx];url=http://[server]/[location]
```

Notes:

- Replace [xx] with the EID (decimal) value associated with the Walled Garden package. See *Create the Walled Garden Package* (on page 38).
- Replace [server] with the name or IP address of the server.
- Replace [location] with the location of the web page/application.
- The syntax requires the EID to be placed before the URL.

Field	Description
Logo	The channel or application logo number associated with this walled garden application Note: The logo functions in the EPG in the same way as current channel logos.
Parameter	Select the Number option
Number	Enter 0 (zero)

Complete these steps to add a new Walled Garden service.

- 1 From the DNCS Administrative Console, select the **Application Interface Modules** tab.
- 2 Click **SAM Service**. The SAM Service List window opens.
- 3 Click **File** and then select **New**. The Set Up SAM Service window opens.
- 4 Complete the fields on the Set Up SAM Service window, as described in *Walled Garden SAM Service Settings* (on page 35).
- 5 Save the Set Up SAM Service window when you are finished.

Complete these steps to modify an existing Walled Garden service.

- 1 From the DNCS Administrative Console, select the **Application Interface Modules** tab.
- 2 Click **SAM Service**. The SAM Service List window opens.
- 3 Locate and highlight the service you want to modify.
- 4 Click **File** and then select **Open**. The configuration window for the service selected opens.
- 5 Edit the fields as described in *Walled Garden SAM Service Settings* (on page 35).
- 6 Click **Save**.
- 7 If prompted, confirm the changes.

Create the Walled Garden Package

Complete these steps to create a Walled Garden authorization package.

- 1 From the DNCS Administrative Console, click the **System Provisioning** tab.
- 2 Click **Package**. The Package List window opens.
- 3 Click **File** and then select **New**. The Set Up Package window opens.
- 4 In the **Package Name** field of the Set Up Package window, type the following:
Walled Gardens (or Walled Garden 00 if you want to assign a package for each Walled Garden service)
- 5 Be sure the **Duration** field is set to **Unlimited**.
- 6 Click **Save**. The Set Up Package window closes.
- 7 From the Package List window, scroll down to find the **Walled Gardens** package you just created.
- 8 Highlight the **Walled Gardens** package.
- 9 Click **File** and then select **Open**. The Set Up Package window opens showing the just-created Walled Gardens package.
- 10 Take note of the Entitlement ID (**EID**) (in both hexadecimal and decimal form) and record those values.
hex: _____ decimal: _____
- 11 Click **Cancel** to close the Set Up Package window.
- 12 Click **File** and then select **Close** to close the Package List window.

Assign the Walled Garden Package to the Set-Top

In this procedure, you will assign the Walled Garden package to a set-top box.

- 1 From the DNCS Administrative Console, click the **Home Element Provisioning** tab.
- 2 Click **DHCT**. The DHCT Provisioning window opens.
- 3 Click **By MAC Address** and type the MAC address of a DHCT you wish to authorize, and then click **Continue**. The Set Up DHCT window opens.
- 4 Click the **Secure Services** tab. The window updates to allow you to assign a package or packages to the DHCT.
- 5 Locate and then highlight the **Walled Garden** package in the **Available** column of the **Packages** section of the window.
- 6 Click **Add**. The Walled Garden package moves from the **Available** column to the **Selected** Column.
- 7 Click **Save**.
- 8 Click **Close** to close the Set Up DHCT window.
- 9 Click **Cancel** to close the DHCT Provisioning window.
- 10 Reboot the set-top box to see the object immediately.

7

Configuration Options

Introduction

The configuration options enable the service provider to customize the web browser and the Vantage user interface (UI).

In This Chapter

- Downloadable Configuration Files 42
- Configuration Variables..... 43

Downloadable Configuration Files

Complete the steps below to implement the downloadable configuration file feature.

Note: This feature allows you to set configurations for Vantage properties that cannot be configured using the SARA configurable options.

Important: We recommend that modifications to configuration variables be performed only by operators with full understanding of the impacts to the system.

- 1 Create a customized configuration file using the known configuration variables listed in the section Configuration Variables.

Example:

```
# Set the Media Object Model (MOM) to insecure mode
# (allow non-wafer applications, e.g. Walled Gardens, access to
"sensitive" APIs)
mom.insecure: 1

# Set the default theme, over-riding the user's selection every time
com_antplc_tvlib.tvlib_config_global_theme: darkblue
```

- 2 Create the customized file as follows:

Note: Replace <hub_id> with zero (0) if you want all set-tops to use this file. Otherwise, specify the hub that supports the set-tops you want to use this file.

- Configurations to be applied during staging:
bfs:///msoconfig/rtn/<hub_id>/stagingdefaults.txt (if present)
- Configurations to be applied globally every time the set-top boots:
bfs:///msoconfig/rtn/<hub_id>/globalconfig.txt (if present)

- 3 Save the file onto the DNCS in the export/home/dncs/SiteFiles directory.
- 4 Use the BFS client DNCS UI to add the file(s) at the following location:

msoconfig/rtn/<hub_id>

Note: Replace <hub_id> with zero (0) if you want all set-tops to use this file. Otherwise, specify the hub that supports the set-tops you want to use this file.

Configuration Variables

Variable	Options (default first)	Description
ciscoSg/acc/accAllowMom	true false	If true, enable non-wafer applications access to Media Object Model (MOM) APIs (needed for Walled Gardens which need access to MAC, screen size, etc.). Allows access to sensitive MOM APIs. This should only be used on sites wishing to support Walled Garden applications.
ciscoSg/audio/fixedVolumeLevel	100 - 0	The level of the fixed audio volume, expressed as a percentage. It indicates which volume to use when in fixed (not variable) volume mode. Any value between 0 and 100 can be used with 0 indicating zero volume and 100 indicating full volume.
ciscoSg/audio/variableVolumeControl	true false	Whether volume is variable, i.e, not fixed. Fixed volume is used to set the audio output to optimum stereo level and disable remote volume control of the set-top.
ciscoSg/chan/chanPowerOn	Blank (last viewed), or any channel in the channel list	The power-on channel or service. The structure of the value string is a channel unique ID (UID) as defined in the channel list manager API. If blank, the last viewed channel is used.
ciscoSg/chan/markUnauthChanInGuide	false true	When true, this enables the feature for graying out unauthorized channels in the program guide.
ciscoSg/look/mainMenuHasLiveTv	true false	Whether to display the Live TV element in the Menu Portal. A value of false will hide the Live TV entry in the menu. A value of true will show the Live TV entry in the menu.
ciscoSg/look/pipSuppt	true false	Indicates whether PIP (picture in picture) is a supported feature. If false, the app will ignore all PIP user input (such as key presses.)
ciscoSg/look/popSuppt	true false	Indicates whether POP (picture outside picture) is a supported feature. If false, the app will not allow the POP type of positioning when the MOVE key is used to move the PIP screen around the screen.
ciscoSg/look/skinStyle	Any theme ID (e.g. cbsd, or other operator-downloaded theme)	Style of the skin, or global theme to be used by default, such as kubrickblack, cbsd, etc.

Variable	Options (default first)	Description
ciscoSg/look/skinStyleList	A comma separated list of theme IDs (including operator-downloaded themes) that should be made available to the user (e.g. kubrickblack, cbsd)	The list of available styles of the skin expressed as a comma-separated list of skin IDs.
ciscoSg/look/buttonListFunction	recordedTV rpl	Describes the user interface function to be performed when the LIST button on the remote control is pressed (launch the "Recorded TV" sub-menu or the "RPL" Recorded Program List directly).
ciscoSg/sys/powerOnAfterBoot	false true	If true, then automatically power on (go to non-standby) at booting time. If absent or false, then user must press Power button after a boot. True indicates that the set-top should present the UI and video when powered-on or rebooted. False indicates that the set-top should wait for the user to press the Power button to leave the standby state and present the UI and video.
ciscoSg/sys/screenLang	Any language pack ID (e.g. eng_us, fr_ca, or other operator-downloaded language pack)	The screen language, also known as the global language, used in the UI.
ciscoSg/sys/showTunedChanBanner	true false	Whether to show the channel change banner.
ciscoSg/sys/startupAppName	Any application ID (e.g. setup, ipg, etc.)	Application that is in focus on startup. Default is to not open the main menu on startup.



Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

This document includes various trademarks of Cisco Systems, Inc. Please see the Notices section of this document for a list of the Cisco Systems, Inc. trademarks used in this document.

Product and service availability are subject to change without notice.

© 2012 Cisco and/or its affiliates. All rights reserved.

March 2012 Printed in USA

Part Number OL-26411-01