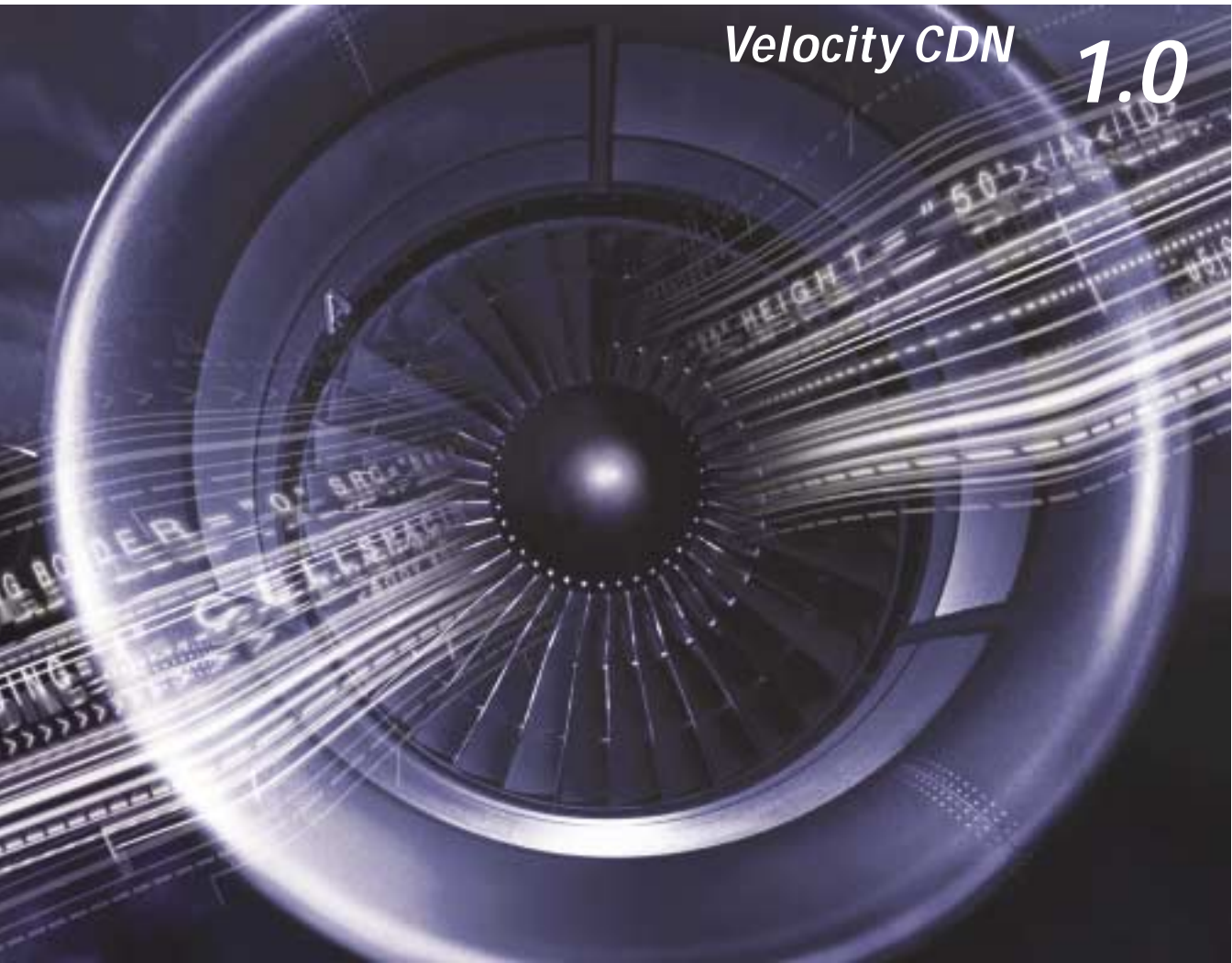




Velocity CDN **1.0**



***Creating and Managing Content
with Content Controller***

Legal Notices

Volera, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Volera, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Volera, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Volera, Inc. reserves the right to make changes to any and all parts of Volera software, at any time, without any obligation to notify any person or entity of such changes.

This product may require export authorization from the U.S. Department of Commerce prior to exporting from the U.S. or Canada.

Copyright © 1997-2001 Volera, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

U.S. Patent Nos. 5,870,739; 5,873,079; 5,884,304. Patents pending.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Volera, Inc.
2211 North First Street
San Jose, CA 95131-2021
U.S.A.

www.volera.com

Creating and Managing Your CDN Using Velocity CDN
August 2001

Online Documentation: To access the online documentation for this and other Volera products, and to get updates, see www.volera.com.

Volera Trademarks

Volera is a trademark of Volera, Inc. in the United States and other countries.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

Contents

About this Manual	7
Part I Preparing Your CDN for Management	
1 Preparing VCDN Management Servers	11
Installing the First Management Servers	11
Installing Additional Management Servers	12
Providing for Communication Between VCDN Components.	12
2 Using the VCDN Management Tool	13
Starting the Browser-Based Management Tool	13
Using the VCDN Search Feature	13
3 How the VCDN Scheduler Works	15
All Configuration Changes Are Scheduled	15
All Administrative Users Can Schedule and Modify Configuration Changes.	15
Tracking Scheduled Changes	15
4 Preparing Cache Devices for VCDN Management	17
Initial Setup.	17
Configuring New Cache Devices	17
Setting a VCDN Management Address on Each Device	17
Adding New Cache Devices in System Controller	18
5 Managing and Configuring Cache Devices	19
6 Managing and Configuring Device Groups	21
The Purposes of VCDN Device Groups	21
How Group Configuration Works.	22
VCDN Assumptions about Group Member Configuration Settings.	22
Group Configuration Settings Are Stored in Data Objects	23
Group Configuration Settings Are Initially Empty.	24
Cautions for Applying Configuration Settings at a Group Level	25
Scheduling Group Changes	32
Creating Device Groups	33
Removing Device Groups	34
Adding a Cache Device to a Group	35
Removing Devices from Groups	35

7	Creating CDN Administrators	37
	Creating VCDN Administrators	37
	Restricting Administrative Access	37
Part II Creating Caches on Your CDN		
8	Creating HTTP Caches	41
9	Creating Streaming Media Caches	43
	Using Media Exceleator for Windows Media on Your CDN	43
	Including Microsoft Media Server (MMS) Objects in Collections	43
Part III Providing Access to Caches		
10	Configuring Browsers and Players to Use the CDN	47
11	Web Proxy Auto-Discovery (WPAD) Setup	49
12	Limiting Access to Caches	51
Part IV Monitoring and Maintaining Your CDN		
13	Monitoring CDN Health and Performance	55
14	Handling System Alerts and Warnings	57
15	Installing Patches and Upgrades	59
	Uninstall Required Before Each Upgrade	59
	Uninstalling Content Accountant	59
	Uninstalling Content Controller	59
	Uninstalling System Controller	60

About this Manual

This manual contains an overview of content distribution networks and how Velocity CDN™ helps you create and manage them.

To	See
Prepare your CDN components for management	“Preparing Your CDN for Management” on page 9.
Create content caches on your CDN	“Creating Caches on Your CDN” on page 39.
Provide access to CDN caches	“Providing Access to Caches” on page 45.
Monitor and maintain the CDN after it is installed and delivering content	“Monitoring and Maintaining Your CDN” on page 53.

Preparing Your CDN for Management

The following table summarizes the tasks discussed in this section.

To	See
Prepare one or more Velocity CDN™ management servers to manage your CDN	“Preparing VCDN Management Servers” on page 11.
Prepare Excelerator 2.1 devices for management	“Preparing Cache Devices for VCDN Management” on page 17
Configure basic settings on Excelerator 2.1 devices and groups of devices	“Managing and Configuring Cache Devices” on page 19
Create CDN administrators and restrict administrative access to VCDN components	“Creating CDN Administrators” on page 37

1

Preparing VCDN Management Servers

Getting Started with System Controller describes basic VCDN management server setup. This chapter provides additional setup information, including the topics summarized in the following table:

To	See
Set up the first VCDN management server	“Installing the First Management Servers” on page 11
Set up additional VCDN management servers	“Installing Additional Management Servers” on page 12

Installing the First Management Servers

When installing the first VCDN management server, you are asked to specify a name for the VCDN datastore. This same datastore name must be specified for each additional VCDN management server that will share and jointly manage the objects in the datastore.

If you plan to have multiple, independent CDN implementations for evaluation or testing purposes, you must ensure that you give each VCDN datastore a unique name.

For example, if you install two CDNs for independent testing of HTML and multimedia functionality, you might name the first datastore of the HTML CDN TEST_HTM and the first datastore of the multimedia CDN TEST_MM. You would then name subsequent datastores either TEST_HTM or TEST_MM, depending on which VCDN datastore the server will help manage.

WARNING: This is especially critical if the CDNs are on independent networks that do not initially communicate with each other but might have communication on the network at sometime in the future. Failure to follow this rule will cause corruption and data loss when network communication is enabled.

Installing Additional Management Servers

Velocity CDN provides for automatic datastore synchronization between VCDN datastores on all management servers managing the same CDN. There are two requirements for this feature:

- ◆ The VCDN management servers must be able to communicate with each other using port on the same network.
- ◆ During System Controller installation of each additional management server, you must specify that each is a secondary server that shares an existing datastore.

Providing for Communication Between VCDN Components

You must ensure that the following communication is possible on your CDN:

- ◆ **VCDN Servers:** must be able to communicate with each other.
Servers containing System Controller must be able to communicate with each other to keep their datastores synchronized
- ◆ **VCDN Servers and Cache Devices:** If these are on a secure network, they can communicate using a non-secure data port. If they must communicate through firewalls, you must enable communication through SSL. This requires that you provide for communication on the chosen SSL port through any firewalls that are between the servers and devices. Additionally, if you are using Secure Excelsator on any managed cache devices, you must provide for separate IP address/port combinations for VCDN communication and Secure Excelsator-based traffic.
- ◆ **VCDN Servers and Managing Browsers:** If browsers and servers are on the same network, they can communicate using the network's standard HTTP protocol. If they are separated by one or more firewalls, you will need to install SSL certificates on the servers and enable a port for communication through the firewalls.

2

Using the VCDN Management Tool

You manage Velocity CDN™ using a browser to access one of the VCDN management servers you have installed.

This chapter provides information regarding the following topics:

Starting the Browser-Based Management Tool

Using the VCDN Search Feature

If you need to find multiple groups, devices, collections or jobs, you can use the search window. If partial names are used, you must include an asterisk for the characters that follow. Only the names matching the search field value are displayed. Use an asterisk or null search field value to redisplay the entire list of groups.

Also, when selecting named objects for applying some action, keep in mind that selected objects are cleared each time the search feature is used.

Boolean searching is not supported in Velocity CDN 1.0. To select multiple objects that cannot be easily returned by a single search operation, you must check the objects from their complete listing.

3

How the VCDN Scheduler Works

It is important that you understand the process the VCDN management suite follows when applying configuration changes to managed cache devices and groups. This will prevent your thinking that a configuration operation has failed when in fact the change is merely in the process of being applied.

All Configuration Changes Are Scheduled

All configuration changes made with the VCDN management suite are managed by the VCDN event scheduler.

If you direct that changes should be applied immediately, the scheduler will begin processing them as soon as possible. If you schedule the changes for later, the scheduler will apply them at the scheduled time.

All Administrative Users Can Schedule and Modify Configuration Changes

Administrative users with group management privileges can create and modify scheduled changes for the groups they manage.

Administrators can change and modify any scheduled changes for their managed groups, including the time at which scheduled changes will be applied. In other words, administrative users can overwrite the events scheduled by other administrative users.

The datastore keeps only the last configuration setting entered for any given parameter. All parameter settings currently in the configuration data object are applied when the scheduled time arrives.

Tracking Scheduled Changes

The management interface provides general schedule tracking messages in its higher-level tabs, such as the Device Configuration and Group Configuration tabs. A Finished status indicates that the scheduled event has been sent to the affected cache devices. When the status changes to Succeeded, you should go

to the configuration page for each device to verify that the configuration changes were actually successful.

When making group configuration changes, try to group the changes together. Not all devices respond at the same speed. If there are multiple group configuration changes pending, there could be problems between boxes because the device changes are not in sync.

As a general rule, make sure the changes you last applied have been applied on each box before making another configuration change.

4

Preparing Cache Devices for VCDN Management

This section contains instructions for preparing your cache devices for VCDN management.

Initial Setup

Each Excelerator 2.1 cache device has the following default setting:

```
vcdn managementaddress=10.1.1.1
```

For System Controller to recognize the device on the network, you must set the `vcdn managementaddress` value to an IP address that is bound to a network card.

Configuring New Cache Devices

Initial configuration of Excelerator 2.1 cache devices for communication on the network is documented in the Excelerator 2.1 Initial Installation Guide and involves either a crossover cable connection with the device or using an attached keyboard and monitor to access the device's command line.

Setting a VCDN Management Address on Each Device

After you have configured the device for communication on your network, you must complete the following steps for each cache device:

- 1 Access the device's command line using a Telnet connection or an attached keyboard and monitor as described in the Excelerator 2.1 documentation.

NOTE: Setting the `vcdn managementaddress` is not supported in the browser-based management tools.

- 2 Enter the following command:

```
set vcdn managementaddress=iii.iii.iii.iii
```

where *i* is the IP address through which System Controller will manage the device.

Adding New Cache Devices in System Controller

To add a cache device in System Controller, complete the following steps:

- 1 Start the VCDN browser-based management tool.
For more information on using the VCDN management tool, see [Chapter 2, “Using the VCDN Management Tool,”](#) on page 13.
- 2 Click System > Device List > Add New Device
- 3 Type a Device Name.
This is the name System Controller displays in various lists.
- 4 Type the VCDN Management Address for the device you set in [“Setting a VCDN Management Address on Each Device”](#) on page 17.
- 5 If you have set a password for the Config user on the device, type the password in the Management Password field.
- 6 Click Continue to Step 2.
- 7 If you have created administrative users, you can assign one or more of them device management privileges by selecting them from the list before proceeding to the next step.

NOTE: The VCDN Administrator (admin) has all management rights to all system objects and therefore doesn't appear in lists of administrative users.
- 8 Click Continue to Step 3.
- 9 Review the Device Summary > click Edit to make changes > click Add Device Now.

5

Managing and Configuring Cache Devices

WARNING: After an Excelerator has been created as a cache device in VCDN, you should not use the Excelerator management tools to make configuration changes. Configuration changes you make to VCDN-managed features will be overwritten by the configuration data stored for the device in the VCDN datastore. For more information, see [How Velocity CDN 1.0 Affects Excelerator 2.1 Management Features](#) in *Planning Your Content Distribution Network (CDN)*.

To manage a device using System Controller, you must first add the device to the VCDN datastore. For more information, see [Chapter 4, “Preparing Cache Devices for VCDN Management,”](#) on page 17.

To select a device for management, complete the following steps:

- 1 Start the VCDN browser-based management tool.
For more information on using the VCDN management tool, see [Chapter 2, “Using the VCDN Management Tool,”](#) on page 13.
- 2 Click System > Device List > a device name
- 3 For more information regarding the options available in the Device Detail panel, see [Management Interface Help](#).

6

Managing and Configuring Device Groups

Velocity CDN™ lets you group Excelerator 2.1 cache devices to meet your CDN management needs. For example, you might want to group cache devices in various groups according to some or all of the following criteria:

- ♦ The geographical structure of your CDN
- ♦ Who is responsible to manage which devices
- ♦ The different types of services hosted on specific devices
- ♦ The customers that devices provide services to
- ♦ The types of content you store on devices

There is no limit to the number of groups you can create, and no limit to the number of groups that a cache device can belong to.

However, before you begin creating and managing cache device groups, it is vital that you understand how group configuration changes affect individual cache devices as explained in this chapter.

The following table summarizes the various device group topics discussed in this chapter.

To	See
Learn about device groups	“The Purposes of VCDN Device Groups” on page 21
Create device groups for management	“Creating Device Groups” on page 33
Make configuration changes to device groups	“How Group Configuration Works” on page 22

The Purposes of VCDN Device Groups

VCDN device groups are a powerful CDN management tool. To use them effectively, however, you must fully understand their purposes and how the VCDN management suite interacts with them.

Device groups are required for the following tasks:

- ♦ **Monitoring:** Using Velocity CDN to monitor cache devices requires that the devices are members of at least one group.
- ♦ **Administration:** Assigning administrative rights to users you want to manage only specific cache devices requires that you create a group containing the devices to be managed.
- ♦ **Global Configuration Changes:** Applying configuration changes to multiple cache devices requires that they are members of a group.

IMPORTANT: Be sure to read [How Group Configuration Works](#) before attempting to use the global configuration feature.

Additionally, you can assign administrative rights to users you want to manage specific cache devices by making devices members of a group and then giving the user administrative rights to that group.

How Group Configuration Works

To avoid causing problems with the configuration of Excelerators in a group operation, it is vital that you understand how group configuration works in VCDN 1.0.

VCDN Assumptions about Group Member Configuration Settings

The VCDN management suite makes certain assumptions regarding the configuration of grouped devices as explained in the following sections.

Initially Device Individuality Is Expected

Since cache devices are grouped together for different purposes, VCDN 1.0 expects each device in a group to have initial configuration differences.

The most obvious example of configuration differences is that each device must have one or more unique IP addresses to communicate on the network. And since IP address settings must remain unique, they are not configurable at the group level.

Another obvious example of settings that might not be shared is the device gateway configuration. On the other hand, devices on the same network subnet could very easily require the same exact gateway configuration.

Other configuration differences are more subtle. For example, you might have a group of devices from different geographical areas that have identical

forward proxy configurations except that they send their log files to different locations.

System Controller is designed to accommodate device differences, but it is also designed to enable conformity when desirable.

Applying a Configuration Resets Expectations

As explained in “[Group Configuration Settings Are Stored in Data Objects](#)” on [page 23](#), there are 18 different areas of configuration or *configuration data objects* that can be applied to devices at the group level.

None of these configurations objects are active until they are applied. Once applied, however, the VCDN management suite is designed to assume that the configuration of each device in the group looks exactly like the settings stored in the configuration object.

NOTE: After applying a group configuration, you can change individual devices to have individualized settings if desired. However, changes made in this manner remain in effect only until the service is configured again at the group level. Once this occurs, individual device settings will again be overwritten.

Group Configuration Settings Are Stored in Data Objects

Device group configurations are stored in the datastore in 18 different data objects (starting with Forward Proxy settings) that appear as links in the left hand column of Group Configuration tab as shown in [Figure 1](#).

Figure 1

Group Configuration Manager: Test2				
Details	Device List	Monitoring	Schedule	Configuration
[Activity View]				
Service Settings	Enabled	Changes	Admin	
Forward Proxy		Aug 25, 2001 7:52 PM	admin	
Transparent Forward Proxy				
Reverse Proxy				
Mini FTP Server				
FTP Forward Proxy				
FTP Reverse Proxy				
Media Exceleator				
Cache Settings	Enabled	Changes	Admin	
Authentication	n/a	n/a	n/a	
Tuning	n/a			
Cache Freshness	n/a			
System/Network Settings	Enabled	Changes	Admin	
DNS		Aug 25, 2001 6:13 PM	admin	
Gateway/Firewall		Aug 25, 2001 6:13 PM	admin	
Date & Time		Aug 25, 2001 6:13 PM	admin	
SNMP		Aug 25, 2001 6:13 PM	admin	
IPQoS	n/a	Aug 25, 2001 6:13 PM	admin	
IP Access Control		Aug 25, 2001 6:13 PM	admin	
Content Settings	Enabled	Changes	Admin	
Dynamic Bypass		Aug 25, 2001 6:13 PM	admin	
Purging				

Group Configuration Settings Are Initially Empty

As explained in “Initially Device Individuality Is Expected” on page 22, System Controller expects and accommodates the configuration differences in

individual cache device configurations by not attempting to set them when the device is initially created.

System Controller therefore stores empty values for all fields in the 18 group configuration data objects shown in [Figure 1 on page 24](#).

These empty configuration values are reflected by the fact that the Enabled column in the Group Configuration tab is mostly blank. This can be misinterpreted by administrators to mean that services are not enabled. However, all it really indicates is that the services have never been set *at the group level*. After they are set for the first time, the group settings will remain, even though some of the individual group members might have changed.

For example, the Enabled column is initially blank for Forward Proxy because a single value does not logically reflect the initial Forward Proxy status of individual devices in the group.

In other words, services that are individually configured cannot be reflected in a group configuration object that has not been activated or applied to the group as a whole.

Cautions for Applying Configuration Settings at a Group Level

There are three points to consider before applying a group configuration data object to a group of devices:

All Configuration Settings Are Applied to All Group Members

When you apply one of the 18 group configuration data objects to a group, all devices in that group will have identical settings for all the fields defined in the group configuration data object.

For example, if you define and apply forward proxy settings to a group, every member of the group will have identical settings. For more information regarding the implications of applying configuration settings to group members, see [“How Group-Level Configuration Affects Grouped Devices” on page 26](#).

Null Values Will Be Applied to Any Fields Left Empty

When applying settings to a group of devices, the VCDN management tools cannot determine whether empty field values were intentionally set or simply reflect the initial empty values from when the group object was created.

If you apply a group configuration object that has empty field values to a group of devices, VCDN will send all configuration settings, including the empty values, to each device. This can result in one of two conditions:

- ◆ Fields are set to empty values on all grouped devices

or

- ◆ Configuration errors are generated for values that cannot be empty

Implications of empty settings in each group configuration object are discussed in [“How Group-Level Configuration Affects Grouped Devices” on page 26](#).

All Network Card IP Addresses Are Set

Some group configuration objects require that you select a network card (eth0, eth1, etc.) for the configuration. When the group configuration object is applied, all IP addresses that are bound to the card at the time the configuration change occurs are assigned to provide the service being configured.

For example, if you apply a Forward Proxy configuration to a group of devices with eth0 selected as the network card, all the IP addresses assigned to et0 will be configured to provide forward proxy services.

A Tip for Grouping Devices

Make separate groups for each type of group configuration.

For example, you might have a group for devices that share forward service settings but do not have the same DNS settings. In such a case, you would not attempt to use the forward service group to manage device DNS settings. Rather you would create other groups of devices that share DNS settings for the express purpose of managing only DNS settings.

How Group-Level Configuration Affects Grouped Devices

The following table discusses each of the 18 group configuration data objects and the implications for configuring the settings at the group level.

Table 1

Group Configuration Area	Implications to Consider
Forward Proxy	<p data-bbox="427 203 1231 258">Configure forward proxy settings for a group only if the following settings are the same for each device in the group:</p> <ul data-bbox="427 279 1231 644" style="list-style-type: none"><li data-bbox="427 279 1231 390">◆ IP Address Settings: The same settings for network card (eth0, eth1, etc.), port, and WPAD apply to each group device, including activation of forward proxy services for each IP address bound to each selected network card.<li data-bbox="427 411 1085 435">◆ Logging: The Logging options apply to each group device.<li data-bbox="427 456 1231 539">◆ Authentication: Each device has the same authentication settings—authentication is either disabled or the same profile is used to access all group devices.<li data-bbox="427 560 1231 644">◆ Cache Control: The same cache control settings (x-forward for, custom cache control header, and HTTP connect method) are appropriate for each group device. <p data-bbox="427 673 1231 812">Configuring forward proxy services for the group will overwrite all forward proxy services set on individual cache devices. You can then configure each device with individualized settings if desired. However, you must make sure that the individual device configuration changes occur after the group configuration changes are completed.</p> <p data-bbox="427 841 1231 925">Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual device settings will again be overwritten.</p>

Group Configuration Area Implications to Consider

Transparent Forward Proxy

Configure transparent forward proxy services at the group level only if the following settings are the same for each device in the group:

- ◆ **Transparent Forward Proxy:** Each IP address bound to the selected network card on each group device is activated for transparent forward proxy services.
- ◆ **Proxy Ports:** The same port settings apply to the transparent service on each group device.
- ◆ **Exception IP Address:** The same settings for bypassing the transparent service for requests to listed Web servers apply to all group devices.
- ◆ **Routing:** The same gateway settings apply to each group device (minimally, all devices are on the same subnet).
- ◆ **Logging:** The Logging options you specify apply to each group device.
- ◆ **Authentication:** Each device has the same authentication settings—authentication is either disabled or the same profile is used to access all group devices.
- ◆ **Options:** The same cache control settings (error handling method, x-forward for, custom cache control header, and HTTP connect method) are appropriate for each group device.
- ◆ **WCCP:** The same cache control settings (error handling method, x-forward for, custom cache control header, and HTTP connect method) are appropriate for each group device.

Configuring transparent forward proxy services for the group will overwrite all transparent handling services set on individual cache devices. You can then configure each device with individualized settings if desired. However, you must make sure that the individual device configuration changes occur after the group configuration changes are completed.

Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual device settings will again be overwritten.

Group Configuration Area	Implications to Consider
Reverse Proxy	<p data-bbox="427 163 1233 218">Configure reverse proxy services for a group only if the same reverse proxy services and load balancing options apply to each group member.</p> <p data-bbox="427 244 1233 387">Configuring forward proxy services for the group will overwrite all reverse services defined on individual cache devices. You can then configure each device with individualized settings if desired. However, you must make sure that the individual device configuration changes occur after the group configuration changes are completed.</p> <p data-bbox="427 413 1233 493">Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual device settings will again be overwritten.</p>
Mini FTP Server	<p data-bbox="427 527 1233 607">Configure the Mini FTP Server area for a group only if each IP address bound to the selected network card on each group device should be activated for mini FTP server services.</p> <p data-bbox="427 633 1233 775">Configuring this for the group will overwrite Mini FTP Server settings on individual cache devices. You can then configure each device with individualized settings if desired. However, you must make sure that the individual device configuration changes occur after the group configuration changes are completed.</p> <p data-bbox="427 802 1233 881">Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual settings are again overwritten.</p> <p data-bbox="427 907 1163 939">This option is also available from the FTP Forward Proxy service link.</p>
FTP Forward Proxy	<p data-bbox="427 973 1233 1053">Configure the FTP Forward Proxy area for a group only if each IP address bound to the selected network card on each group device should be activated for FTP forward proxy services.</p> <p data-bbox="427 1079 1233 1222">Configuring this for the group will overwrite FTP Forward Proxy settings on individual cache devices. You can then configure each device with individualized settings if desired. However, you must make sure that the individual device configuration changes occur after the group configuration changes are completed.</p> <p data-bbox="427 1248 1233 1328">Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual settings are again overwritten.</p> <p data-bbox="427 1354 1045 1385">This option is also available from the Mini FTP Server link.</p>

Group Configuration Area	Implications to Consider
FTP Reverse Proxy	<p>Configure the FTP Reverse Proxy area for a group only if each IP address bound to the same FTP servers should be accelerated by each group device.</p> <p>Configuring this for the group will overwrite FTP Reverse Proxy services configured on individual cache devices. You can then configure each device with individualized settings if desired. However, you must make sure that the individual device configuration changes occur after the group configuration changes are completed.</p> <p>Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual settings are again overwritten.</p>
Media Excelerator	<p>Configure the Media Excelerator area for a group only if the same media services apply to each group device.</p> <p>Configuring this for the group will overwrite Media Excelerator services configured on individual cache devices. You can then configure each device with individualized settings if desired. However, you must make sure that the individual device configuration changes occur after the group configuration changes are completed.</p> <p>Changes made in this manner remain in effect until the service is configured again at the group level, at which time, individual settings are again overwritten.</p>
Authentication	<p>Authentication profiles are global. Any profiles you define using this option are available to all managed devices and groups.</p>
Tuning	<p>The tuning parameters you specify apply to all devices in the group.</p> <p>After applying tuning parameters to grouped devices, you can change the tuning parameters on each device if desired. Changes made in this manner remain in effect until the service is accessed again at the group level, at which time, individual settings are again overwritten.</p>
Cache Freshness	<p>The cache freshness settings you specify apply to all devices in the group.</p> <p>After applying cache freshness settings to grouped devices, you can change the settings on each device if desired. Changes made in this manner remain in effect until the service is accessed again at the group level, at which time, individual settings are again overwritten.</p>

Group Configuration Area	Implications to Consider
DNS	Use caution when changing the DNS settings for a group. Keep in mind that the same settings will be applied to each device in the group. Unless all devices can function with the same DNS settings, applying them to a group might make some devices unavailable on the network. If this happens, someone must manually restore the correct DNS settings for the device to communicate on the network.
Gateway/Firewall	Use caution when changing the Gateway/Firewall settings for a group. Keep in mind that the same settings will be applied to each device in the group. Unless all devices can function with the same settings, applying them to a group might make some devices unavailable on the network. If this happens, someone must manually restore the correct gateway/firewall settings for the device to communicate on the network.
Date & Time	Configure the Date & Time settings for a group only if the same settings apply to each device in the group. Incorrect settings will cause log entries and accounting statistics to be incorrect and can disrupt other system functions, such as the importing of SSL certificates.
SNMP	<p>The SNMP settings you specify will apply to each group member. While some SNMP settings might be the same for each device in a group, the node name for each device must be unique. Otherwise, the origin of SNMP messages can't be determined.</p> <p>The node name will be changed if these settings are applied to the group. For example, a null node name will set a null node name on each device.</p> <p>If you use this option to set SNMP parameters for grouped devices, you will then want to access the devices individually to change the node name and possibly other settings. The changes you make will remain in effect until you access the SNMP settings at the group level again, at which time each device will again be assigned the same SNMP settings.</p>
IPQoS	<p>IP QoS settings specify how devices set Quality of Service (QoS) parameters in requests to servers, replies to clients, and device error pages. The same IP QoS settings will be applied to all group members.</p> <p>Having the same settings is a likely requirement in most CDN settings.</p>
IP Access Control	<p>IP Access Control lets you allow or block browser access to cache devices using the Source IP list. It also lets you allow or block IP addresses from which devices will fill cache using the Destination IP list.</p> <p>It is very likely that the same lists might apply to multiple devices on a CDN.</p>

Group Configuration Area	Implications to Consider
Dynamic Bypass	<p>The Dynamic Bypass feature lets you configure devices so that specific errors from Web sites are explicitly not cached and subsequent requests to the Web sites are simply passed through for a specific time period.</p> <p>It is likely that administrators would want devices on a CDN to have the same dynamic bypass settings.</p>
Purging	<p>This option removes all cached objects from all grouped devices. Since filling cache is sometimes a time consuming and costly process, many administrators will rarely use this option.</p>

Scheduling Group Changes

All changes to group configurations are scheduled

When you have applied a configuration change to the group, you can see the status of the change on the Schedule screen—one entry for the group and entries for each device in the group.

Status messages show only that the device has received and or is processing the change. They do not indicate that changes have been applied successfully. This means that you should always verify at the device level that changes have actually been applied. To do this, access the schedule for each device.

NOTE: Only 40 scheduled changes can be handled at one time on a VCDN server. The process of changing one device counts as one scheduled change.

Therefore, if you have more than 40 devices in a group, the completion time for scheduled changes will extend until each device is scheduled and configured. The same logic applies if you have scheduled changes to multiple groups that will result in more than 40 scheduled changes.

Scheduled group changes are applied to the devices that are members of the group when the scheduled event occurs. For example, if you add devices to a group after scheduling a configuration event and before the scheduled time arrives, the changes will be applied to all group devices, including those you have added to the group. The same logic applies to device resources, such as IP addresses bound to network cards, etc. Configuration changes are applied to the resources that are current when the changes actually occur.

Also, if changes to a device occur during the execution of a group schedule, there is not guarantee that the changes will be made.

For more information on VCDN management suite event scheduling functionality, see [Chapter 3, “How the VCDN Scheduler Works,”](#) on page 15.

Creating Device Groups

NOTE: Cache devices must first be added as devices in the VCDN datastore before they can be made members of a group.

If you used the worksheets mentioned in [Planning for Cache Device Management](#) in *Planning Your Content Distribution Network (CDN)*, you can use them in the following procedure.

To create a group of cache devices, complete the following steps:

- 1 Start the VCDN browser-based management tool.

For more information, see [“Starting the Browser-Based Management Tool”](#) on page 13.

- 2 Click System > Group List > Create New Group.

- 3 Type a group name.

The name might indicate the purpose for which the group is being created. It can contain up to 16 alphanumeric characters.

- 4 Type the IP address or DNS name of the VCDN management server that will receive all alerts and monitoring data from group members.

Administrators of large installations with multiple management servers might want to designate one or more management servers for collecting alerts and monitoring data from all device groups on the CDN.

- 5 If desired, type a brief description of the group for management reference.

- 6 Click Continue to Step 2.

- 7 Click Continue to Step 3.

- 8 In the Available Devices list, check the devices you are adding to the group.

For information about using the search feature to filter the list of available devices, see [“Using the VCDN Search Feature”](#) on page 13.

- 9 If you have created administrative users to help manage this group and its devices, check their names in the Available Admins list.

NOTE: Users assigned as device administrators have full access to the group and the devices it contains.

Super administrators do not appear in the Available Admins list because they have non-restrictable rights to all VCDN systems. Also, the group creator user ID will not be displayed even though that user ID will be included in the list of admins having access.

- 10 Click Continue to Step 4.
- 11 Review the group definition.
- 12 You can use an Edit button to make changes, or you can click a step link beneath the top banner to go directly to a section of the group definition.
- 13 When the group definition is correct, click Create Group Now.

Removing Device Groups

NOTE: Cache device objects are not deleted with this function, only the logical grouping of the devices is removed from the datastore.

To remove a group of cache devices, complete the following steps:

- 1 Start the VCDN browser-based management tool.
For more information, see [“Starting the Browser-Based Management Tool” on page 13](#).
- 2 Click System > Group List.
- 3 In the Available Groups list under Select, check the group or groups you want to remove.
- 4 Below the Available Groups list, click Remove Selected Group(s).

Removing a group causes the following to occur:

- ◆ The group name no longer appears in the Available Groups list.
- ◆ Administrative users lose access to group devices unless they have device access through another group or direct assignment.
- ◆ Scheduled group actions that are still pending are removed from the list of scheduled events. Any actions currently in process are not affected.
- ◆ Cache devices stop reporting monitoring data to the group’s designated monitoring server unless membership in another group causes them to continue reporting.

Adding a Cache Device to a Group

To add a cache device to an existing group of cache devices, complete the following steps:

- 1 Start the VCDN browser-based management tool.
For more information, see [“Starting the Browser-Based Management Tool” on page 13](#).
- 2 Click System > Group List > the target Group name > Device List.
- 3 Below the Device List, click Add Devices to this Group.
- 4 In Devices Not in This List, check the devices you want to add to the group.

The group is updated to show your additions

Adding devices to a group is a scheduled event and might take several minutes to complete. When it completes, it causes the following to occur:

- ◆ The device starts reporting monitoring data to the monitoring server.
- ◆ Scheduled group actions that are still pending will affect the newly added device along with all other group members.
- ◆ The Alert status for the group (enabled or disabled) is applied to the device.
- ◆ Admins with access rights to the group now have full access rights to the device.

Removing Devices from Groups

NOTE: Cache device objects are not deleted with this function, only their inclusion in the logical grouping of devices.

To remove a device from a group, complete the following steps:

- 1 Start the VCDN browser-based management tool.
For more information, see [“Starting the Browser-Based Management Tool” on page 13](#).
- 2 Click System > Group List > the target Group name > Device List.
- 3 In the Devices in this Group list under Select, check the group or groups you want to remove.

4 Below the Available Groups list, click Remove Selected Device(s).

Removing a device from a group causes the following to occur:

- ◆ The device name no longer appears in the Group's Device List.
- ◆ Administrative users lose access to the device unless they have access through another group or direct assignment.
- ◆ Scheduled group actions that are still pending will not affect the device. Any actions currently in process are not affected.
- ◆ The device stops reporting monitoring data to the group's designated monitoring server unless membership in another group causes it to continue reporting.

7

Creating CDN Administrators

Administrative users can only see the devices and groups they have been assigned to manage.

You can create up to 20 active administrator accounts

The Super Administrator, who is created during System Controller installation, has rights to all objects on the system.

Only the Super administrator can add and remove Administrators in the datastore. Once an administrative user is added to a cache device or group, that user will have the necessary rights to remove other administrators from managing the device or group. However, administrative users cannot remove other users from the datastore.

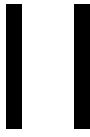
To	See
Create VCDN administrators in the datastore to help manage the CDN	“Creating VCDN Administrators” on page 37
Restrict administrative access to VCDN objects in the datastore	“Restricting Administrative Access” on page 37

Creating VCDN Administrators

You can create administrative users by running the VCDN browser-based management tool and clicking Users.

Restricting Administrative Access

Administrative users are automatically restricted to managing only those devices and groups to which you have granted them access.



Creating Caches on Your CDN

To	See
Create HTTP caches on your CDN	Chapter 8, “Creating HTTP Caches,” on page 41
Create streaming caches on your CDN	Chapter 9, “Creating Streaming Media Caches,” on page 43

8

Creating HTTP Caches

You can create HTTP caches on your CDN by configuring any of the caching service types described in the Excelsator 2.1 documentation. These services can be assigned to individual cache devices or to groups of cache devices as described in [Chapter 5, “Managing and Configuring Cache Devices,”](#) on page 19 and [Chapter 6, “Managing and Configuring Device Groups,”](#) on page 21.

After you create the proxy services on your network, you can define collections and jobs for managing specific content objects. For more information, see [Content Caching and Distribution Planning](#) in *Planning Your Content Distribution Network (CDN)*.

To learn more about creating collections and jobs, see [Managing Content with Content Controller](#).

To learn more about identifying content objects using URL masks, see [Ensuring Cache Freshness and Prepopulating, Retaining, and Removing Cache Objects](#) in *Managing Content with Content Controller*.

9

Creating Streaming Media Caches

Excellerator 2.1 cache devices support HTTP streaming wherein a streaming file is delivered through HTTP and played in a browser plug-in.

They also include support for non-proprietary RTSP/RTP streaming media content and tunneling of an RTSP/RTP session inside an HTTP connection as implemented in the QuickTime* and Darwin* products from Apple Computer, Inc.

Using Media Excelerator for Windows Media on Your CDN

Each installation of Volera's Media Excelerator for Windows Media requires a valid license to be installed on the target cache device.

System Controller lets you specify the creation of Windows Media acceleration services for cache devices or device groups without checking for valid Media Excelerator for Windows Media licenses on the target devices.

You must ensure that each target cache device contains a valid Media Excelerator license. Otherwise, the service creation operation will fail on unlicensed devices, causing errors and alerts to be generated.

Including Microsoft Media Server (MMS) Objects in Collections

To include MMS objects in collections, if the job action associated with the collection is Prepopulate or Prepopulate and Pin, the URL mask entered for the object must specify the MMS protocol moniker.

For example, the URL mask for prepopulating the object *film.asf* into cache from a media server located at *www.media.com* would be:

```
mms://www.media.com/film.asf
```




Providing Access to Caches

To	See
Configure browsers and media players to use CDN caches	Chapter 10, "Configuring Browsers and Players to Use the CDN," on page 47
Use Web Proxy Auto-Discovery (WPAD) to configure network browsers to use CDN caches	Chapter 11, "Web Proxy Auto-Discovery (WPAD) Setup," on page 49
Limit browser and player access to CDN caches	Chapter 12, "Limiting Access to Caches," on page 51

10

Configuring Browsers and Players to Use the CDN

The Excelerator 2.1 documentation contains instructions for configuring browsers and players to access caching services. The instructions also apply to CDN installations.

11

Web Proxy Auto-Discovery (WPAD) Setup

When properly configured for the browsers used on your network, the Web Proxy Auto-Discovery (WPAD) feature lets network users automatically access the cache device's forward proxy services without having to individually configure their browsers.

Instructions for configuring the cache devices on your CDN to work with Web Proxy Auto-Discovery are found in the Excelerator 2.1 documentation.

12 Limiting Access to Caches

Excelerator 2.1 cache devices let you specify various ways of requiring that users authenticate before using the device's caching services. They also let you restrict access based on the requesting IP address.

Both of these services can be configured in Velocity CDN 1.0.

Detailed feature descriptions are provided in the Excelerator 2.1 documentation.

IV

Monitoring and Maintaining Your CDN

This chapter will contain

To	See
Learn about and use VCDN's general health monitoring features	Chapter 13, "Monitoring CDN Health and Performance," on page 55
Learn about VCDNs various system alerts and how to handle them	Chapter 14, "Handling System Alerts and Warnings," on page 57
Install patches and upgrades to VCDN components	Chapter 15, "Installing Patches and Upgrades," on page 59

13

Monitoring CDN Health and Performance

Velocity CDN™ includes various tools for monitoring health and performance.

14 Handling System Alerts and Warnings

Velocity CDN™ provides the ability to manage Exceleator 2.1 alert and warning functionality on multiple cache devices.

15 Installing Patches and Upgrades

Velocity CDN™ provides the ability to apply over-the-wire upgrades to multiple cache devices.

Uninstall Required Before Each Upgrade

Before upgrading to a new version of System Controller, Content Controller, or Content Accountant, you must first uninstall the older version of each product in the reverse order of product installation, as explained in the following sections.

Uninstalling Content Accountant

From a GUI Interface

To uninstall Content Account using a GUI interface on the VCDN management server, run the following executable:

```
/opt/volera/roma/_ca_uninst/ca_uninstall
```

At the Server's Command Line

To uninstall Content Account from the command line on the VCDN management server, enter the following command:

```
./ca_uninstall -is:javaconsole -console
```

Uninstalling Content Controller

From a GUI Interface

To uninstall Content Account using a GUI interface on the VCDN management server, run the following executable:

```
/opt/volera/roma/_cc_uninst/cc_uninstall
```

At the Server's Command Line

To uninstall Content Account from the command line on the VCDN management server, enter the following command:

```
./cc_uninstall -is:javaconsole -console
```

Uninstalling System Controller

From a GUI Interface

To uninstall System Controller using a GUI interface on the VCDN management server, run the following executable:

```
/opt/volera/roma/_sc_uninst/sc_uninstall
```

You will need to provide the datastore name and administrator password specified during installation to uninstall System Controller.

At the Server's Command Line

To uninstall System Controller from the command line on the VCDN management server, enter the following command:

```
./sc_uninstall -is:javaconsole -console
```

WARNING: Uninstalling the last System Controller on your CDN from the command line removes the VCDN datastore. However, you are not asked to supply the datastore name or administrator password. Also, the uninstall doesn't warn that the last remaining copy of the datastore is being removed.