

PCoIP® Management Console User Manual

TER0812002

Issue 5



Teradici Corporation
#101-4621 Canada Way, Burnaby, BC V5G 4X8 Canada

p +1 604 451 5800 f +1 604 451 5818
www.teradici.com



The information contained in this document represents the current view of Teradici Corporation as of the date of publication. Because Teradici must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Teradici, and Teradici cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. TERADICI MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Teradici Corporation.

Teradici may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Teradici, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2011 Teradici Corporation. All rights reserved.

Teradici, PC-over-IP and PCoIP are registered trademarks of Teradici Corporation.
The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Revision History

Version	Date	Description
1	April 3, 2009	Initial release
2	August 31, 2009	Updated for release 1.1 of the Management Console <ul style="list-style-type: none"> ▪ Updated Management Console Limitations (see Section 1.2) ▪ Added Migrating to a New Version of the Management Console (see Section 2.6)
3	March 01, 2010	Updated for release 1.2 of the Management Console <ul style="list-style-type: none"> ▪ Replaced PCoIPMC with MC ▪ Added support for Internet Explorer
4	September 17, 2010	Updated for release 1.3.30 of the Management Console <ul style="list-style-type: none"> ▪ Added Device Log Monitoring ▪ Added support for Firmware Release 3.2
5	June 01, 2011	Updated for release 1.5 of the Management Console <ul style="list-style-type: none"> ▪ Added AutoConfig ▪ Added support for Firmware Release 3.3 and 3.4 ▪ Added OSD Logos to profiles ▪ Added Firmware to profiles ▪ Added Profile Application Status page ▪ Changed term Portal to Zero Client ▪ USB device bridging support ▪ Added support for profile scheduling ▪ Configurable DHCP Timeout options

Contents

REVISION HISTORY	3
CONTENTS	4
TABLE OF FIGURES	7
TABLES.....	9
DEFINITIONS	10
INTRODUCTION.....	11
1 OVERVIEW.....	12
1.1 PCoIP Deployment Components	12
1.1.1 Managing PCoIP Devices	12
1.1.2 DNS Server	13
1.2 Management Console Limitations.....	14
1.3 Management Console Concepts.....	14
1.3.1 Groups and Profiles	14
1.3.2 Fixed Seating	16
1.3.3 Device Discovery	16
1.3.4 AutoConfig	21
1.4 Management Console and Firmware Version Compatibility	22
2 INSTALLATION AND SETUP	24
2.1 Management Console Host System Requirements	24
2.2 Contents of the Management Console package.....	24
2.3 Installing the Management Console using VMware Player.....	25
2.4 Installing the Management Console into your existing VMware ESX™ server	25
2.5 Running the Management Console.....	25
2.6 Migrating to a New Version of the Management Console.....	26
2.6.1 Potential Problems and Workarounds	26
2.6.2 What Information is Imported	27
2.6.3 Database Migration Procedure	27
3 VIRTUAL MACHINE FEATURES.....	29

3.1	Refresh Status.....	29
3.2	Set Web Interface Password.....	29
3.3	Change Hostname	29
3.4	Manage Networking	30
3.4.1	View Network Configuration.....	30
3.4.2	Configure IP Address.....	30
3.4.3	Configure DNS.....	31
3.5	Database Management.....	31
3.5.1	Backup Database.....	32
3.5.2	Restore Database.....	32
3.5.3	Delete Database	32
3.6	Change Time Zone.....	32
3.7	Restart Management Console Daemon.....	32
3.8	Halt Virtual Machine	33
4	WEB INTERFACE	34
4.1	Accessing the Management Console Web User Interface	34
4.2	Device Management	37
4.2.1	Device Discovery (optional)	38
4.2.2	Legend	38
4.2.3	Query Devices and Update Database	40
4.2.4	Filtering Devices.....	40
4.2.5	Configure Device Group	41
4.2.6	Linking Devices.....	42
4.2.7	Access Device Web Page.....	43
4.2.8	Summary Device Information.....	44
4.2.9	Device Details	45
4.3	Group Management	48
4.3.1	Manage Groups	49
4.3.2	View Profile Application Status	52
4.3.3	Manage AutoConfig	53
4.3.4	View AutoConfig Status	55
4.4	Profile Management	56
4.4.1	Create a Profile	56
4.4.2	Duplicate a Profile.....	57
4.4.3	Delete a Profile.....	57
4.4.4	Modify Profile Name & Description	57
4.4.5	Modify Profile Properties.....	57
4.5	Power Management	60
4.5.1	Sending Reset and Power off Commands.....	61
4.5.2	Power Management Status.....	62
4.6	Update Firmware.....	63
4.6.1	Import Firmware	64

4.6.2	Update Device Firmware	64
4.6.3	View Status	66
4.7	Device Log Monitoring.....	67
4.7.1	Device Tree.....	67
4.7.2	Logging Controls.....	68
4.7.3	Status	68
4.8	Manage Settings	68
4.8.1	Database Management.....	69
4.8.2	Environment Settings.....	70
4.9	Site Status	70
4.10	Online Help	72
5	GETTING STARTED	73
5.1	Start the Management Console	73
5.2	Discover Devices.....	73
5.3	Adding Devices to a Group	73
5.4	Peering Devices	74
5.5	Next Steps.....	75

Table of Figures

Figure 1-1: PCoIP Deployment Components	12
Figure 1-2: Management Console Groups and Profiles	15
Figure 1-3: DNS Service Configuration Menu	17
Figure 1-4: DNS Service Location (SRV) Dialog Box	18
Figure 1-5: Management Console Manual Device Discovery Feature	21
Figure 2-1: MC VM Console in VMware Player	26
Figure 3-1: Management Console VM Console.....	29
Figure 3-2: Manage MC VM Console Network Settings	30
Figure 3-3: Manage MC VM Console Database	31
Figure 4-1: Web Interface Security Warning in Firefox.....	35
Figure 4-2: Web Interface Security Warning in Internet Explorer	35
Figure 4-3: Management Console License Agreement	36
Figure 4-4: Web Interface Login	36
Figure 4-5: Home Web Page	37
Figure 4-6: Device Management Web Page.....	38
Figure 4-7: Device Management Legend Box	39
Figure 4-8: Adding Devices to a Group.....	42
Figure 4-9: Peering a Pair of Devices	43
Figure 4-10: Summary Device Information Dialog Box.....	44
Figure 4-11: Edit Device Name Using Summary Device Information Dialog Box	44
Figure 4-12: Zero Client Device Details Web Page	46
Figure 4-13: Device Event Log Web Page	48
Figure 4-14: Group Management Web Page.....	49
Figure 4-15: Apply Profile reboot behavior options.....	51
Figure 4-16: Apply Profile date/time picker	52
Figure 4-17: View Profile Application Status Web Page.....	53
Figure 4-18: Manage AutoConfig Web Page	55
Figure 4-19: View AutoConfig Status Web Page	56
Figure 4-20: Profile Management Web Page	56
Figure 4-21: Profile Management – Set Properties Web Page	58
Figure 4-22: Bandwidth Configuration Settings Dialog Box.....	59
Figure 4-23: Add OSD Logo property	59
Figure 4-24: Link to Imported Firmware property	60
Figure 4-25: Power Management Web Page	60
Figure 4-26: Send Device State Change Command Web Page	61

Figure 4-27: Schedule Device State Change Command Web Page.....	62
Figure 4-28: Power Management Status Web Page	63
Figure 4-29: Update Firmware Web Page	64
Figure 4-30: Initial Update Devices Web Page.....	65
Figure 4-31: Second Update Devices Web Page	66
Figure 4-32: Firmware Update Status Web Page.....	66
Figure 4-33: Device Log Monitoring Web Page.....	67
Figure 4-34: Settings Web Page.....	69
Figure 4-35: Database Management Web Page	69
Figure 4-36: Home Web Page	71
Figure 4-37: Help Web Page	72
Figure 5-1: Adding Devices to a Group.....	74
Figure 5-2: Peering a Pair of Devices.....	75

Tables

Table 2-1: Potential Problems Associated with Upgrading the MC	26
Table 4-1: Example AutoConfig rules	54
Table 4-2: Example AutoConfig rule application	54

Definitions

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNS SRV	Domain Name System Service Record
FQDN	Fully Qualified Domain Name
MC	PCoIP Management Console
OS	Operating System
OSD	On Screen Display
PC-over-IP [®]	Personal Computer over Internet Protocol
PCoIP [®]	Personal Computer over Internet Protocol (PC-over-IP [®])
PCoIP Host	Host side of PCoIP system
PCoIP Zero Client	Desktop or client side of PC-over-IP [®] system. For example, PCoIP Portal or PCoIP Integrated Display.
SLP	Service Location Protocol
URL	Uniform Resource Locator, Web site address
VM	VMware Virtual Machine
Zero Client	See PCoIP Zero Client

Introduction

The Teradici PCoIP Management Console (MC) enables administrators to centrally manage a PCoIP deployment. The MC is packaged as a VMware® virtual machine (VM) and runs on VMware Player. A web browser is used to access and control the MC.

Administrators can use the MC to do the following:

- Access and update the configuration of all PCoIP devices
- Apply the same configuration data to groups of devices
- Update device firmware
- Reset devices
- Control the power state of host devices
- View status information
- Manage the monitoring of device event logs
- Automatically configure newly discovered devices with a profile (optionally with firmware and OSD logo) based on device password and IP address values.

This document describes how to install and set up the PCoIP Management Console. It also describes the features of the tool. More detailed information describing the individual PCoIP device configuration fields is available in the PCoIP Administrative Interface User Manual (TER0606004).

This document is broken into the following sections:

- Section 1 provides a description of the components found in a PCoIP deployment along with some important concepts associated with the MC
- Section 2 describes how to install and set up the MC and migrate from an old version of the tool to a new version
- Section 3 details the features of the MC virtual machine
- Section 4 discusses the web interface of the MC, this is the primary mechanism used by administrators to manage the PCoIP devices
- Section 5 describes how to use the MC to perform some basic tasks

Note: First time users of the MC that want to begin using the tool right away should review section 5. This section provides information on how to start the MC, log into the web interface, discover some devices and link a pair of Host and Zero Client devices. After this is done the user will be able to establish a PCoIP session between the linked Host and Zero Client devices. This section also includes recommendations the user should follow to become familiar with the major capabilities of the MC.

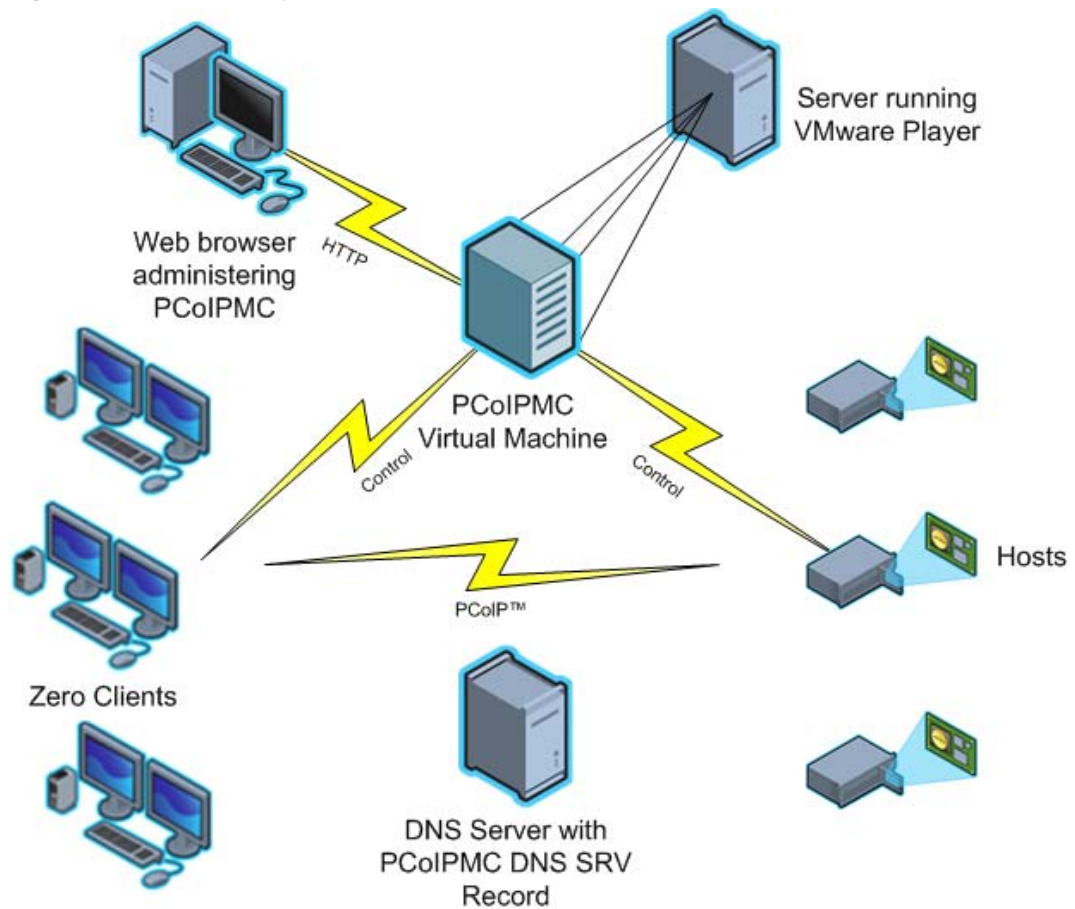
1 Overview

This section describes the components found in a typical PCoIP deployment. It describes some important concepts that help the user understand how to use the MC to manage the PCoIP devices in a deployment.

1.1 PCoIP Deployment Components

Figure 1-1 shows the recommended components found in a PCoIP deployment where individual Host and Zero Client devices are statically grouped together (peered). The PCoIP Management Console, used for peering and configuration, is shown. The figure does not show a connection broker, which is required when Hosts are dynamically assigned to Zero Clients as users log in.

Figure 1-1: PCoIP Deployment Components



1.1.1 Managing PCoIP Devices

A PCoIP deployment is made up of one or more PCoIP Host and Zero Client devices. Each device has multiple configuration settings that can be accessed and controlled using the following mechanisms:

Device Web Interface

Each device can be configured individually via web-based administration interface.

However, users should avoid changing the configuration settings through the device web interface, especially as the deployment grows. Instead, users are encouraged to use the MC; this ensures that all PCoIP devices are configured uniformly and that the MC database accurately reflects the device configuration settings. Refer to the PCoIP Administrative Interface User Manual (TER0606004) for information on the web interface.

PCoIP Management Console

The Teradici PCoIP Management Console (MC) enables administrators to centrally manage a PCoIP deployment. Administrators can use the MC to do the following:

- Access and update the configuration of all PCoIP devices
- Apply the same configuration settings to groups of devices
- Update device firmware
- Reset devices
- Control the power state of Host devices that support power management
- View status information
- Manage the monitoring of device event logs
- Automatically configure newly discovered Zero Clients with a profile (optionally with firmware and OSD logo) based on device password and IP address values.

The MC is packaged as a VMware virtual machine (VM) and runs on VMware Player. This allows users to install and run the MC on any host machine that can run VMware Player.

A web browser is used to access and control the MC.

The MC must be connected to the same network the PCoIP devices are connected to. This is required to allow the tool to communicate with the PCoIP devices.

Connection Broker

A Connection Broker is an optional component that allows an administrator to manage user access to computing resources. This component is not shown in Figure 1-1. In a PCoIP deployment, a connection broker is used to assign connections between PCoIP Host and Zero Client devices and/or RDP sessions between terminal servers and PCoIP Zero Clients. Deployments having one or more of the following requirements must install a connection broker:

- Hosts are dynamically assigned to Zero Clients based on the login credentials of the person using the Zero Client.
- Zero Clients establish RDP sessions with terminal servers.

1.1.2 DNS Server

Figure 1-1 shows a DNS Server with the MC DNS SRV record. This component is optional, but highly recommended. The MC must discover the PCoIP Host and Zero Client devices, and the MC DNS SRV record facilitates automatic device discovery. A Connection Broker DNS SRV record can also be installed on the DNS Server. PCoIP devices use this record to notify the connection broker of their existence.

When a PCoIP device boots it reads these records, which contain the addresses of the MC and/or connection broker. After reading the records, the device sends messages to the MC and/or connection broker notifying them of the devices existence. This ensures the MC and/or connection broker is aware of all the devices in the deployment as they are powered on.

The MC DNS SRV record is not required when one of the following conditions is true:

- All PCoIP devices in a deployment reside on the same network subnet as the MC. In this situation the MC can find the devices using SLP discovery. All devices must set the Enable SLP Discovery configuration setting equal to True.
- The PCoIP MC DNS-Based Discovery Prefix setting of all devices is configured to equal the hostname prefix of the MC. This setting can only be accessed using the MC. It is not accessible through the device web interface or Zero Client OSD interface. Section 1.3.3.2 describes how PCoIP devices use the PCoIP MC DNS-Based Discovery Prefix to contact the MC along with the system requirements that must be met to use this option.

If none of the previous conditions are true users should include a DNS Server in their system and install the MC DNS SRV record. Section 1.3.3.1 describes how to install this record.

1.2 Management Console Limitations

This section describes some limitations of the MC.

- All PCoIP devices managed by the MC must be loaded with firmware release 0.19 or greater. The MC cannot discover devices loaded with older firmware releases. New firmware must be uploaded and activated on devices running firmware releases less than or equal to 0.18. This is done through the device web interface. Refer to the PCoIP Administrative Interface User Manual (TER0606004) for information on how to do this.
- The current release of the MC is only compatible with versions 3.0 and higher of the Firefox web browser and versions 7 and 8 of the Internet Explorer web browser. Support for additional browsers will be included in future releases of the MC.
- The current release of the MC only supports configuring Zero Clients to establish PCoIP sessions. It does not support configuring RDP sessions. If this is required a connection broker should be installed in the deployment.
- The MC supports linking PCoIP Host and Zero Client devices in fixed seating mode where the same Zero Client always connects to the same Host. If dynamically assigning Zero Clients to Hosts is required, the deployment must include a connection broker.
- The MC supports managing up to 2000 PCoIP devices. The tool may be capable of supporting more than 2000 devices, but the current version has been tested with a maximum of 2000 devices. Support for more than 2000 devices will be included in a future release of the tool. Deployments with more than 2000 devices should contact their PCoIP equipment supplier for guidance on how to manage more than 2000 devices.

1.3 Management Console Concepts

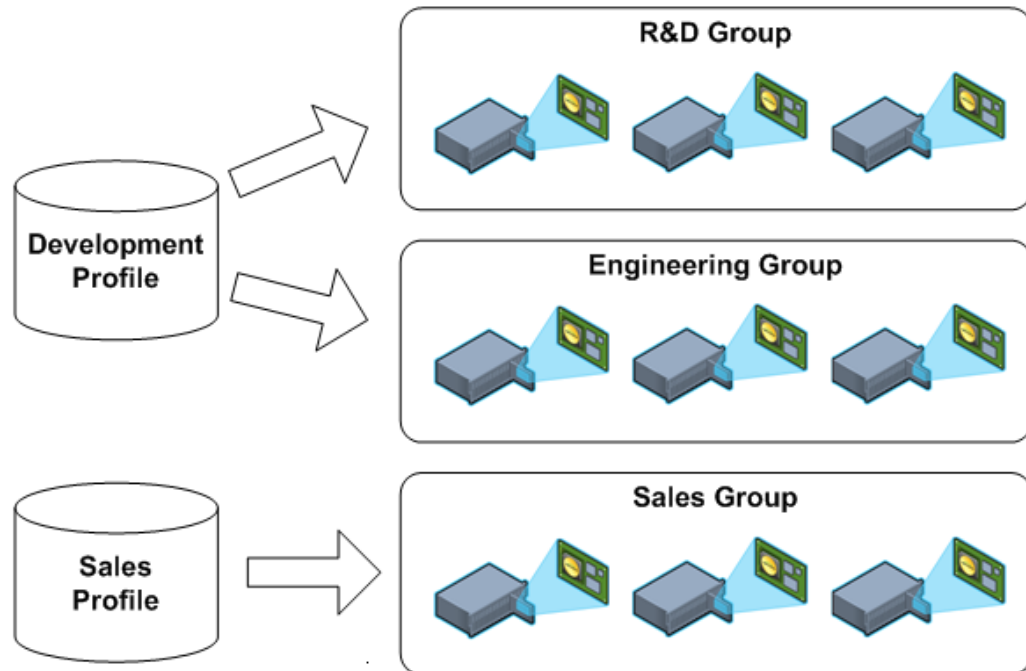
This section describes some key concepts users should be aware of before using the MC.

1.3.1 Groups and Profiles


The MC manages the PCoIP devices using two important concepts (*groups* and *profiles*). A *profile* is a set of device configuration settings and a *group* is a set of one or more devices with a single profile. Figure 1-2 shows one way in which groups of Host devices

could be related to profiles. The figure shows three groups of devices. Two of the groups share the same profile. In this situation all configuration settings defined in the *Development Profile* will be written to the devices in the *R&D* and *Engineering* groups.

Figure 1-2: Management Console Groups and Profiles



Below are some important rules regarding *groups* and *profiles*.

- Each group has one and only one profile associated with it.
- The same profile can be associated with multiple groups.
- All configuration settings in a profile are written to all devices in a group when the profile is applied to the group.
- A profile can contain values for every configuration parameter but this is not required. A profile can be defined that contains a subset of the configuration parameters.
- If the firmware on a device is updated when a profile is applied the profile settings will be written to the device after the new firmware is activated.
- Profiles contain settings that allow users to specify whether a device's firmware is updated based on the version of the firmware running on the device.
- When profile settings are written to devices the settings might not take effect immediately. Some settings are activated after a device is reset. Profile settings that require a reset are preceded by the  symbol within the MC Profile Set Properties and Device Details web pages. Users should consider resetting all devices in the deployment after updating device configuration settings.
- When devices are added to a group and the group profile has not changed, the profile should be applied to the newly added devices and not the entire group. This will minimize the number of device resets.

1.3.2 Fixed Seating

The MC allows an administrator to link individual Host and Zero Client devices so that each Zero Client always establishes a connection to the same Host. This relationship is called *fixed seating*. If a PCoIP deployment requires the ability to dynamically assign Hosts to Zero Clients when users login the administrator must install a connection broker. The MC does not support dynamically assigning Hosts to Zero Clients.

1.3.3 Device Discovery

All PCoIP devices managed by the MC must be discovered by the MC. The MC supports discovering devices in a deployment using one or more discovery mechanisms.

1. It is recommended to install a MC DNS SRV record. Section 1.3.3.1 describes how to install a DNS SRV record.

Note it may not be possible to install a DNS SRV record because the network does not include a DNS server or multiple instances of the MC will be installed on the same network managing subsets of the PCoIP devices.

2. If a DNS SRV record cannot be installed users may be able to configure the devices to automatically notify the MC of their existence. PCoIP devices support a configuration setting called the *PCoIP MC DNS-Based Discovery Prefix*. Section 1.3.3.2 describes how this feature works and the deployment requirements associated with using this discovery method.

Note: The *PCoIP MC DNS-Based Discovery Prefix* setting can only be accessed using the MC. It is not accessible through the device web interface or Zero Client OSD interface.

3. If a DNS SRV record cannot be installed and the deployment cannot use the *PCoIP MC DNS-Based Discovery Prefix* configuration setting then the final automated device discovery option available is SLP discovery. This device discovery method imposes a restriction that limits its usefulness. To use this feature all PCoIP devices and the MC must reside on the same network subnet.
4. If a deployment cannot support any of the previous device discovery options then the administrator can use the MC to configure devices. The MC supports a Manual Discovery feature that allows the MC to find devices. This feature is described in section 1.3.3.3. Below are some shortcomings associated with this approach:
 - If a device has enabled DHCP, the MC will lose contact with a device if its IP address changes. The administrator would need to perform another manual discovery search to find devices that were assigned new IP addresses.

1.3.3.1 DNS Service Record Discovery

When DNS SRV record discovery is used, the PCoIP devices advertise themselves to the MC. All devices that use the DNS server will be able to find the MC. If DNS-SRV discovery is not enabled, the MC must seek out and find devices using methods that are often subject to limitations, such as being unable to search more than its local subnet.

The system requirements for DNS SRV discovery are as follows:

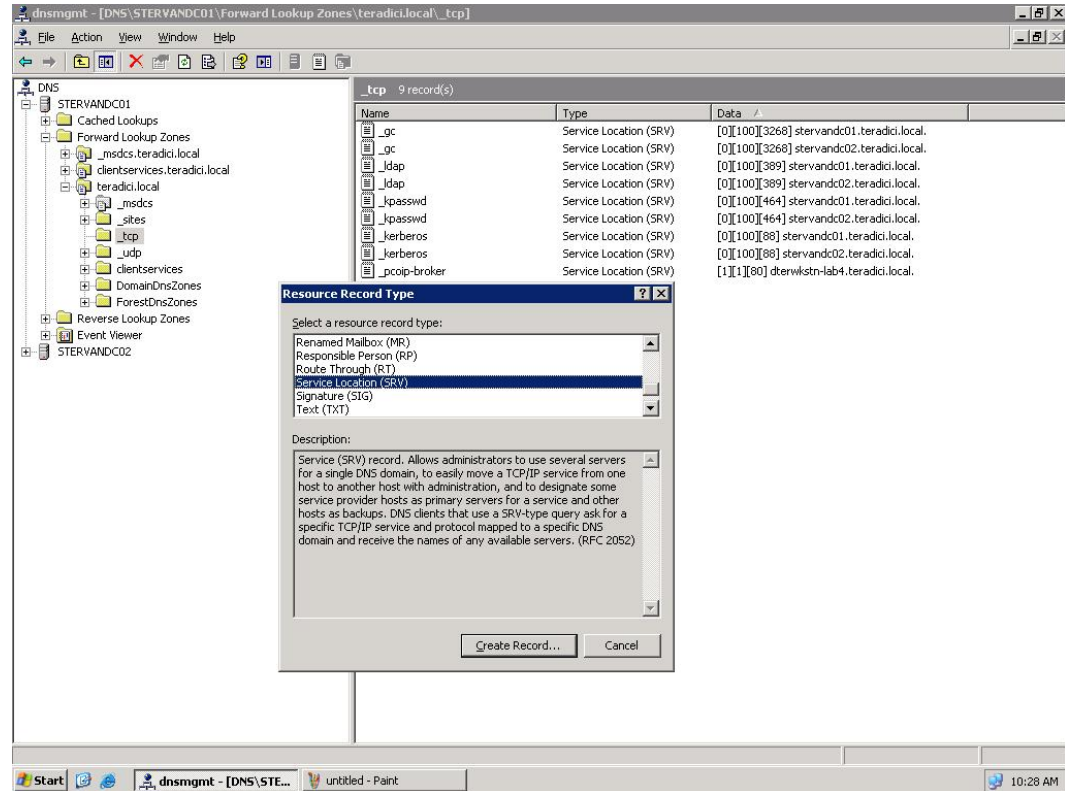
- The deployment must have a DNS Server in the network
- Two DNS records must be installed on the DNS server
 - An A record (name record) for the MC
 - A SRV record (service record) created following the steps below

Add the MC DNS SRV Record to the DNS Server

To add the MC DNS SRV record to DNS Server in Windows 2003 Server, perform the following steps:

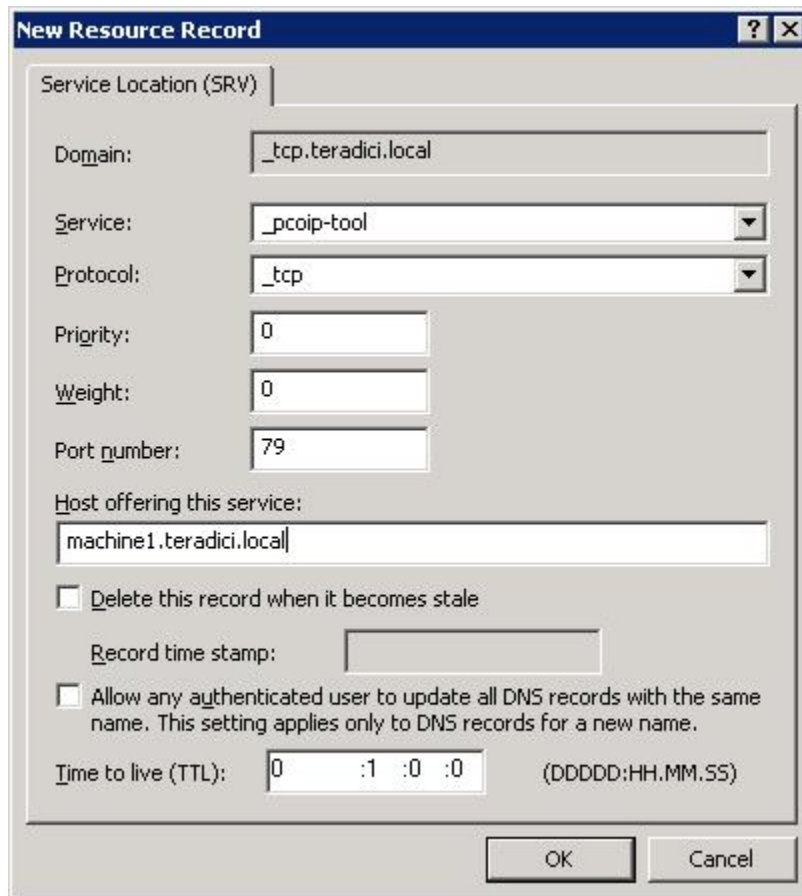
1. Enter DNS service configuration on domain controller.
2. Navigate to local domain and _tcp entry.

Figure 1-3: DNS Service Configuration Menu



3. Right click and select "Other New Records ..."
4. Select "Service Location (SRV)".
5. Fill in the entries as shown in Figure 1-4 and enter the hostname where the MC is installed under "Host offering this service". The "Port Number" in the configuration is not used by the PCoIP devices. However, it may be set to 50000 to reflect the listening port of the CMI server.

Figure 1-4: DNS Service Location (SRV) Dialog Box



The screenshot shows a 'New Resource Record' dialog box with the following fields and values:

- Service Location (SRV):
- Domain:
- Service:
- Protocol:
- Priority:
- Weight:
- Port number:
- Host offering this service:
- Delete this record when it becomes stale
- Record time stamp:
- Allow any authenticated user to update all DNS records with the same name. This setting applies only to DNS records for a new name.
- Time to live (TTL): : : : (DDDD:HH.MM.SS)

Buttons: OK, Cancel

1.3.3.2 PCoIP Management Console DNS-Based Discovery Prefix

Each PCoIP device reads the PCoIP MC DNS-Based Discovery Prefix setting when it boots. If this setting is non-blank then the device attempts to contact the MC by combining the string stored in this setting with variations of the domain name hierarchy.

System Requirements

The system requirements for MC DNS-Based Discovery are as follows:

- The PCoIP devices and MC must be located within the same domain name hierarchy tree (e.g. if a PCoIP device is located in the domain sales.europe.companyname.com, then the MC's domain name can be any one of: sales.europe.companyname.com, europe.companyname.com, or companyname.com)
- The PCoIP devices must enable DHCP in order to get the domain name and hostname (to get DHCP options 15 and 12 respectively)
- The DHCP server must support either DHCP options 12 (hostname), 15 (domain name), or both. Refer to RFC2132. If the DHCP server only supports DHCP options 12, the hostname string must contain the domain name.
- All PCoIP devices managed by a specific MC must have the *PCoIP MC DNS-Based Discovery Prefix* setting equal to the MC's hostname prefix (e.g. if the MC's FQDN is pcoip_mc1.europe.companyname.com, then the field must equal pcoip_mc1).

Algorithm

Each time a PCoIP device boots it executes the MC DNS-Based Discovery algorithm if the *PCoIP MC DNS-Based Discovery Prefix* setting is non-blank. The algorithm uses the setting and the domain name hierarchy to search for a MC.

The PCoIP device obtains the domain name string from the DHCP server using DHCP options 15. Since some DHCP servers may not have DHCP options 15 implemented, the device also obtains the host name using DHCP options 12 (assumed to include the domain name).

Since the device and MC may not be on the same domain (but must be within the same hierarchy), the device composes many FQDN variations using the results from DHCP options 12 and 15. With each FQDN variation, the hostname prefix remains constant however the domain hierarchy level changes.

The device sequentially attempts each FQDN possibility until a hit is found, at which point the device completes DNS-based discovery. The algorithm may take several minutes in order to find the correct FQDN address of the MC (depends on the number of levels in the domain name hierarchy and the MC load).

In detail, the algorithm works as follows. The device uses domain name variations based on the DHCP options 15 string. For each FQDN possibility, the device attempts to transmit a status message to the MC at the FQDN. Upon transmission timeout, the device composes the next FQDN variation by proceeding one level up the domain hierarchy. The last domain name attempted has a single dot in the string. After exhausting the FQDN possibilities (based on the DHCP options 15 string), the device delays for 5 minutes and then uses hostname variations based on the DHCP options 12 string. After failing to contact a MC using the DHCP options 12 string, the device delays 5 minutes and then cycles back to using DHCP options 15. The device continues this process until a MC is contacted.

Example

In the example below, the DHCP options 15 returns sales.europe.companyname.com. DHCP options 12 returns hostmachine1.sales.europe.companyname.com. Note that the DHCP server may return no value for either option. The MC configured the PCoIP MC DNS-Based Discovery Prefix in the device to equal pcoip_mc1.

The device creates the following FQDNs and sequentially attempts contact with the MC:

(attempt #1) pcoip_mc1.sales.europe.companyname.com

(attempt #2) pcoip_mc1.europe.companyname.com

(attempt #3) pcoip_mc1.companyname.com

<device delays for 5 minutes>

(attempt #4) pcoip_mc1.hostmachine1.sales.europe.companyname.com

(attempt #5) pcoip_mc1.sales.europe.companyname.com

(attempt #6) pcoip_mc1.europe.companyname.com

(attempt #7) pcoip_mc1.companyname.com

<device delays for 5 minutes>

(attempt #8) pcoip_mc1.sales.europe.companyname.com (repeat 1-7)

...

Attempts 1 to 3 use the domain name from DHCP options 15 string. Failing to contact the MC, the device uses the DHCP options 12 string for attempts 4 to 7. Failing transmissions for attempt 4 to 7, the device cycles back to using DHCP options 15.

1.3.3.3 Manual Device Discovery

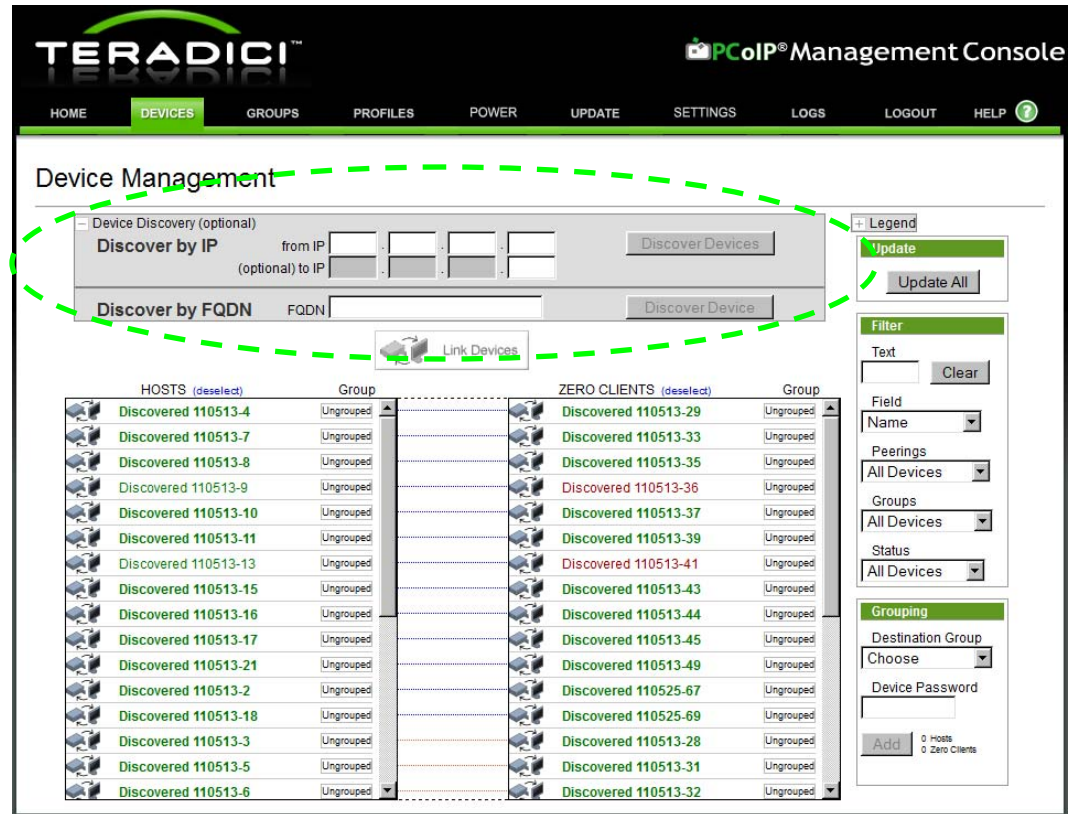
Manual device discovery is not an automated discovery mechanism. This mechanism supports discovering devices that are powered on and connected to the network when the MC is commanded to discover devices.

MC supports manually discovering devices at a specific IP address, in a range of IP addresses or at an FQDN. This option is useful for users that want to quickly begin using the MC. It is also useful when a deployment uses the *PCoIP MC DNS-Based Discovery Prefix* configuration setting described in section 1.3.3.2. In this situation the administrator can discover devices using this feature and configure the *PCoIP MC DNS-Based Discovery Prefix* setting of each device so the devices contact the MC each time they boot.

Figure 1-5 shows the Management Console Device Management web page with the *Device Discovery* feature highlighted.

- When the IP address of a device is known and the device has not been discovered enter the address in the *from IP* field and select *Discover Devices*.
- When a device is on a specific subnet but its IP address is not known the MC can be commanded to discover all devices in a range of IP addresses using both the *from IP* and (*optional*) *to IP* fields. After the address range has been specified select *Discover Devices*. Note that this process can take a few minutes to complete depending on the number of addresses searched. A status bar is displayed while the tool discovers devices.
- When the FQDN of a device is known and the device has not been discovered enter the FQDN in the *FQDN* field and select *Discover Devices*.

Figure 1-5: Management Console Manual Device Discovery Feature



1.3.4 AutoConfig

Any PCoIP Zero Clients newly discovered by the MC may be automatically added to a group and have that group’s profile applied without user interaction. One or more AutoConfig rules can be created that allow one group to have one or more criteria defined. The MC supports the following criteria to decide how Zero Clients are automatically assigned to groups using AutoConfig:

- Each group can have an optional AutoConfig rule associated with it
- Rules are sets of optional password settings and optional IP address ranges as described here:
 - No Password: Add discovered Zero Clients to this group if they have no password configured.
 - Password: Add discovered Zero Clients to this group if they have the identical password configured for the criteria.
 - IP address range: Add discovered Zero Clients to this group if the IP address falls within the range configured by this criteria. Not specifying an IP address range will add all Zero Clients that match the password criteria.

The order of events that occurs when a Zero Client has been discovered is:

1. Device is listed in the AutoConfig status table with a status of Not Started
2. Zero Client IP address and password are compared against all AutoConfig rules.
3. If a match is found then the Zero Client is added to that group

4. If the group's profile contains a firmware rule then the firmware is applied if it passes the criteria and the device is rebooted.
5. The remainder of the profile's properties are now applied to the device.
6. After applying the profile's OSD logo and properties the Zero Client will be rebooted.

1.4 Management Console and Firmware Version Compatibility

MC Version	Supports FW Versions	Fully Configures FW Versions
1.0.26, 1.0.28	0.19-current	0.19-1.10
1.1.20	0.19-current	0.19-2.2 Added the ability to: <ul style="list-style-type: none"> • Configure View Connection Server address • Configure View Connection Server port • Enable/disable View Connection Server SSL • Enable/disable View Connection Server Auto Connect • Configure device bandwidth floor
1.2.20	0.19-current	0.19-3.1.0 Added the ability to: <ul style="list-style-type: none"> • Enable/disable SNMP server • Enable/disable host driver function • Configure session encryption modes • Choose the Korean keyboard layout
1.3.30	0.19-current	0.19-3.2.0 Added the ability to: <ul style="list-style-type: none"> • Danish, Finnish, Norwegian, Swedish, Turkish, Dutch, Polish, Belgian, Russian and Lithuanian Keyboard Layouts • Advanced VMware View Settings • VMware View Kiosk Mode • Enable/disable Peer Loss Overlay

1.4.30, 1.4.40	0.19-current	<p>0.19-3.3.0</p> <p>Added the ability to:</p> <ul style="list-style-type: none"> • Configure View desktop name to select • Enable/disable Zero Client web interface • Selective display of Zero Client On-Screen Display menu entries • VMware View Connection Server address cache behaviour and content • Choose the Estonian, Hungarian, Latvian and Serbian keyboard layouts • Configure VMware View auto-logon
1.5.20	0.19-current	<p>0.19-3.4.0</p> <p>Added the ability to:</p> <ul style="list-style-type: none"> • Configure syslog • Configure static IP address fallback • Choose the Czech, Romanian and Slovenian keyboard layouts • Configure the USB bridging override table

2 Installation and Setup

This section describes how to install and setup the MC. It also describes how to migrate from an old version of the MC to a new version.

2.1 Management Console Host System Requirements

The MC server machine must meet the requirements of the virtualization environment that the MC VM will run in.

1. The MC server machine must meet the requirements of the VMware Player. For a VMware Player installation, please check the VMware Player documentation (http://www.vmware.com/pdf/vmware_player250.pdf) for the most up-to-date requirements. The current requirements are:
 - a. Standard x86-compatible or x86-64-compatible PC
 - b. Processor speed—733MHz or faster
 - c. Memory—512MB minimum, 2GB recommended. You must have enough memory to run the host operating system, the virtual machine and applications on the host and guest operating systems.
 - d. Hard disk—At least 1GB free disk space for each guest operating system. For installation, VMware Player requires approximately 250MB (Windows) or 200MB (Linux) free disk space.
2. The MC server machine CPU requirements differ based on the number of PCoIP devices managed. If the MC manages less than 1000 devices the server machine CPU should be a 2GHz or faster Intel® Pentium® 4 or better processor. If the MC manages 1000 or more devices the server machine CPU should be an Intel® Core™2 Duo Processor or better.
3. The MC VM is configured to use 640 MB of RAM. For best performance, the server machine should have at least 1 GB of RAM to avoid excessive swapping.
4. The MC server machine must have 4 GB of disk space free to accommodate the VM's disk image.

2.2 Contents of the Management Console package

The zip file contains the following files:

1. Teradici_PCoIP_Management_Console_Agreement.pdf: Teradici PCoIP Management Console (“Software”) license file
2. PCoIP_MC_reIA-B-C_vDEF.vmx: Teradici PCoIP Management Console VMware configuration file for the virtual machine that hosts the Management Console.
3. PCoIP_MC_reIA-B-C_vDEF.vmdk: Teradici PCoIP Management Console VMware virtual disk file containing the virtual machine's hard drive. The size of this file will increase as the MC is used. The maximum size of the file is 4GB.
4. README.txt: file describing the contents of the zip file
5. TER0812002_Issue_X-PCoIP_Management_Console_User_Manual.pdf: Teradici PCoIP Management Console User Manual, where X is the issue number
6. TER0904003_Issue_X-PCoIP_MC_Release_Notes.pdf: Teradici PCoIP Management Console Release Notes, where X is the issue number

2.3 Installing the Management Console using VMware Player

1. The MC is distributed as a VMware virtual machine (VM) contained in a zip file. The VM is run using VMware Player. VMware Player is a free application that can be downloaded from <http://www.vmware.com/download/player/>. Follow the directions provided by VMware to download and install this application on the MC host machine.
2. After installing the VMware Player application extract the contents of the file PCoIP_MC_relA-B-C_vDEF.zip into a folder on the MC host machine. The release number (A-B-C) and build ID (DEF) are encoded in the filename.
3. To start the MC, open the folder from step 2 then double click the file PCoIP_MC_relA-B-C_vDEF.vmx to launch VMware Player and have it load the MC VM. The MC can also be started from within VMware Player, selecting File->"Open a Virtual Machine", navigating to the PCoIP_MC_relA-B-C_vDEF.vmx file and clicking "Open". Once VMware Player has launched the MC at least once, the MC can be restarted from within VMware Player's startup screen by double clicking on the PCoIP MC entry in the list of recently opened VMs.

2.4 Installing the Management Console into your existing VMware ESX™ server

1. The recommended method to import the MC VM into a VMware ESX server is to use the VMware vCenter™ Converter Standalone Client. This free tool can be downloaded from <http://www.vmware.com/products/converter/>. Install the tool before continuing.
2. Click the *Convert Machine* button to launch the *Conversion wizard*.
3. Select source type "VMware Workstation or other VMware virtual machine" and use the Browse... button to locate the PCoIP MC's .vmx file. Click Next.
4. Select destination type "VMware Infrastructure virtual machine" and enter the address, user name and password of either the VMware vCenter or the VMware ESX host. Click Next.
5. Edit the Virtual machine name, if desired, and click Next.
6. Review the options and click Next.
7. Click Finish to begin the conversion. Once complete, start the VM through VMware vSphere™ Client or your preferred mechanism.
8. Please read section 2.2 "Contents of the Management Console package" to learn about the contents of the MC virtual machine.

2.5 Running the Management Console

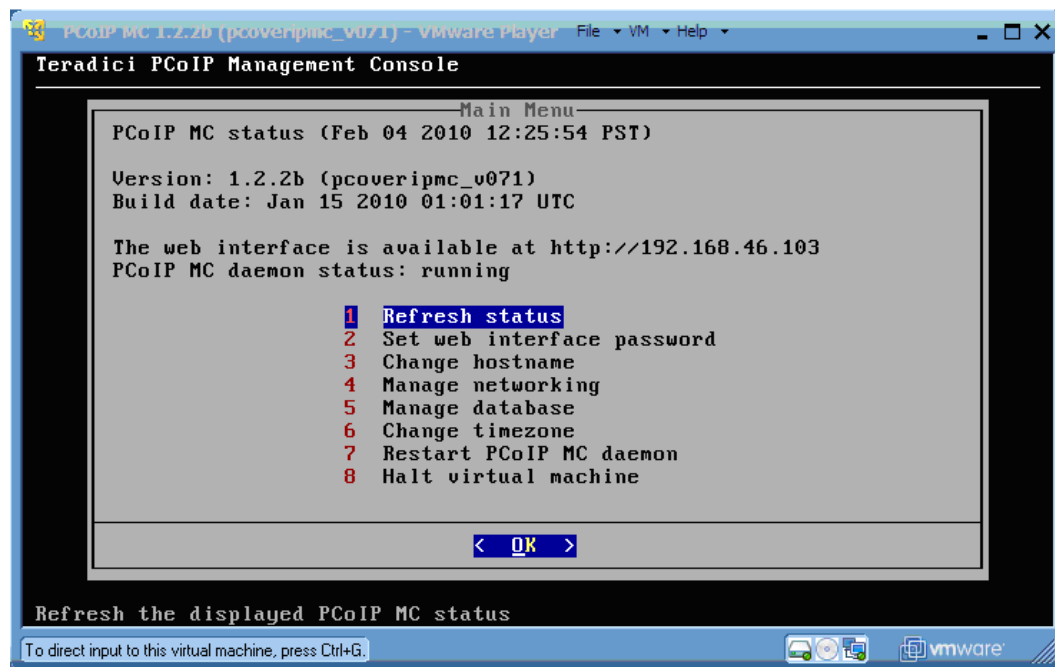
Before running the MC, make sure the MC host machine and PCoIP devices are connected to the same network. The MC supports both DHCP and static IP addressing.

As the VM boots, the VMware console shows a series of standard Linux boot messages before displaying the MC console interface shown in Figure 2-1.

Once the VM is up, the console displays the MC URL (web site address). The URL is equal to <http://192.168.46.103> in the following figure.

Note: Along the bottom of the window the VMware Player describes how to interact with the VM and how to return to the host OS.

Figure 2-1: MC VM Console in VMware Player



2.6 Migrating to a New Version of the Management Console

Periodically new releases of the MC will be released. These releases include support for new features and/or include bugs fixes. The following information is described in this section:

- Potential problems that can occur when migrating to a new version of the MC along with recommendations on how to avoid them
- Information that will and will not be imported from a backed up database
- Steps the administrator should follow when migrating to a new version of the MC

2.6.1 Potential Problems and Workarounds

Table 2-1 lists the problems that can occur when installing a new version of the MC. It includes recommendations for the administrator to follow to avoid or workaround each problem.

Table 2-1: Potential Problems Associated with Upgrading the MC

Problem	Workaround
The database restore feature can only import databases created by old versions of the MC.	Administrators should not attempt to import databases created by a newer version of the MC into older versions of the MC.

<p>When a deployment installs a new version of the MC the PCoIP Host and Zero Client devices may loose contact with the MC.</p>	<p>This problem will not occur if the IP address of the new instance of the MC is the same as the old version of the MC. Administrators are recommended to assign a static IP address to the MC.</p> <p>If the MC IP address is assigned by a DHCP Server and the deployment has installed a MC DNS SRV Record the PCoIP devices will eventually re-establish contact with the new version of the MC. The devices will be out of contact with the MC for up to n seconds, where n is equal to the value of the Time-To-Live field included in the MC DNS SRV Record. The administrator can force the devices to contact the new MC by resetting the devices. The administrator can also import the database of the old version of the MC, which will make the MC aware of the PCoIP devices in the deployment.</p>
---	--

2.6.2 What Information is Imported

When a database is imported into the MC the following information will be populated:

- Device information for all devices (device details, profile, group and peering information)
- Previously imported firmware images
- Profiles
- Groups

If the imported database was created by an instance of the MC running release 1.1.x or higher the following additional information will be populated. Databases created by release 1.0.x of the MC do not export these settings.

- MC web interface password
- MC network configuration settings
- MC hostname

The following settings are not imported.

- MC time zone settings

Note: When migrating to a new version of the MC the administrator is responsible for reconfiguring all of the settings that were not imported.

2.6.3 Database Migration Procedure

This section lists the steps that should be followed when migrating to a new version of the MC.

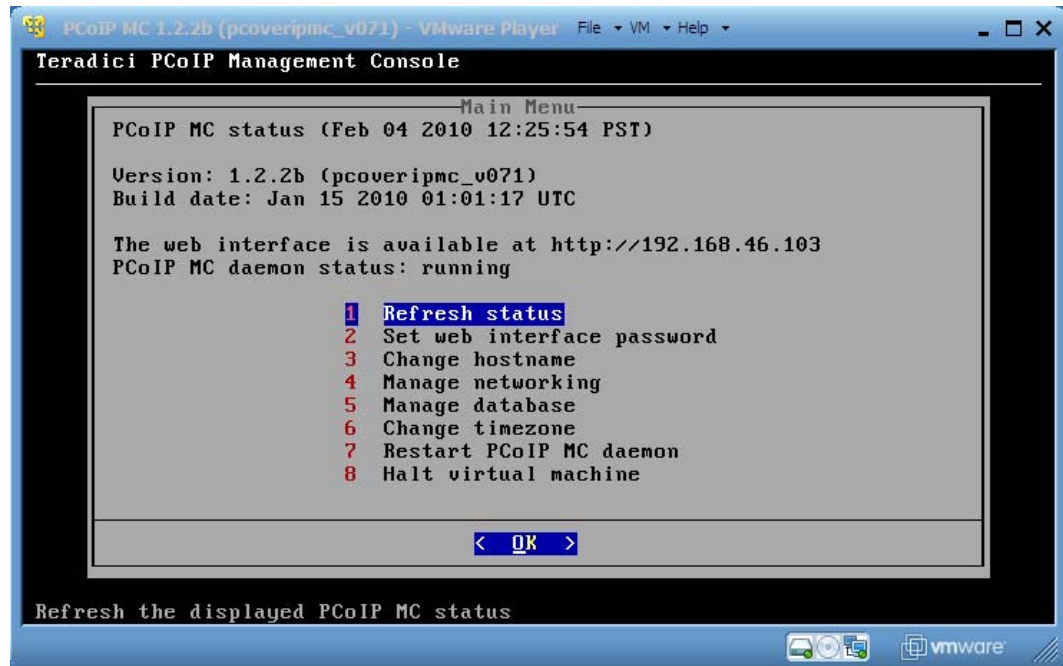
1. Use the old version of the MC to backup the current MC database. Refer to section 3.5.1.
2. Download the backed up database to a host computer. Refer to section 4.8.1.

3. Section 2.6.2 above lists the settings that will and will not be imported by the new version of the MC when a database is restored. Prior to shutting down the old version of the MC write down the values of the settings that will not be imported.
4. Shutdown the old version of the MC. Refer to section 3.8.
5. Install and begin running to the new version of the MC.
6. Upload the database to the MC from the host computer. Refer to section 4.8.1.
7. Restore the database from the imported database. Refer to section 3.5.2.
8. Configure the settings that were not imported when the database was restored.

3 Virtual Machine Features

The top level menu of the PCoIP Management Console is shown in Figure 3-1. This menu appears after opening the MC in the VMware Player. This section describes the features accessed and controlled through this interface, which is referred to as the “MC VM console” throughout this document.

Figure 3-1: Management Console VM Console



3.1 Refresh Status

The *Refresh status* option allows the user to refresh the information displayed on the MC VM Console window.

3.2 Set Web Interface Password

The MC web interface is protected by a password. When a browser connects to the MC web interface the user is prompted to enter a password. To configure this password select the *Set web interface password* option on the MC VM console.

3.3 Change Hostname

The default hostname of the MC equals *pcoip-mc*. The MC registers this hostname with the DNS server if one is present on the network. Users can update this field using the *Change hostname* option shown in Figure 3-1.

If a deployment installs more than one copy of the MC the hostname of each instance should be set equal to unique values.

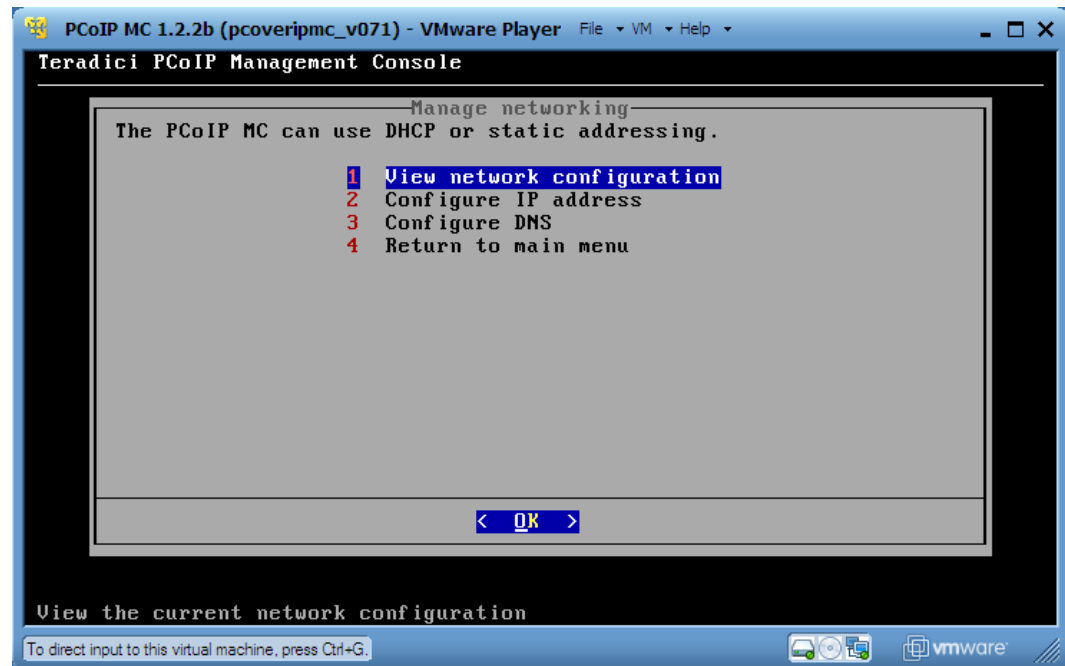
If the deployment does not install a MC DNS SRV record the administrators should configure the *PCoIP MC DNS-Based Discovery Prefix* field of each PCoIP device to equal the hostname prefix of the MC. Section 1.3.3.2 provides additional details on this field and the system requirements associated with using it. To configure this field the user must configure the *PCoIP MC DNS-Based Discovery Prefix* setting in the profiles and apply the profiles to all the devices in the deployment.

3.4 Manage Networking

The MC communicates with a web browser through a network connection and must be assigned a unique IP address. By default the MC uses DHCP to acquire an IP address. The MC network settings can be modified to use a static IP address if a DHCP server does not exist on the network or the administrator wishes to assign a static IP address. To modify the MC network settings select the *Manage networking* option shown in Figure 3-1.

Figure 3-2 shows the MC Manage networking options.

Figure 3-2: Manage MC VM Console Network Settings



3.4.1 View Network Configuration

The *View network configuration* option allows the user to view the current network configuration settings of the MC.

3.4.2 Configure IP Address

The *Configure IP address* option allows the user to select DHCP or static IP addressing. When the user chooses static IP addressing they must configure the MC IP address, subnet mask, gateway address, broadcast address and domain. The gateway address,

broadcast address and domain are optional and can be left blank. After the IP address settings are updated the MC restarts the network interface using the new settings.

3.4.3 Configure DNS

The *Configure DNS* option allows the user to configure the Domain Name Server(s) and search domain(s) used by the MC. The MC queries the DNS Server(s) to determine if the MC DNS SRV record and Connection Broker DNS SRV record are present. The status of these records is reported in the site status on the Home web page, see section 4.9.

Note: When the MC is configured to use DHCP, the DNS settings configured here may be overwritten by the settings configured in the DHCP server.

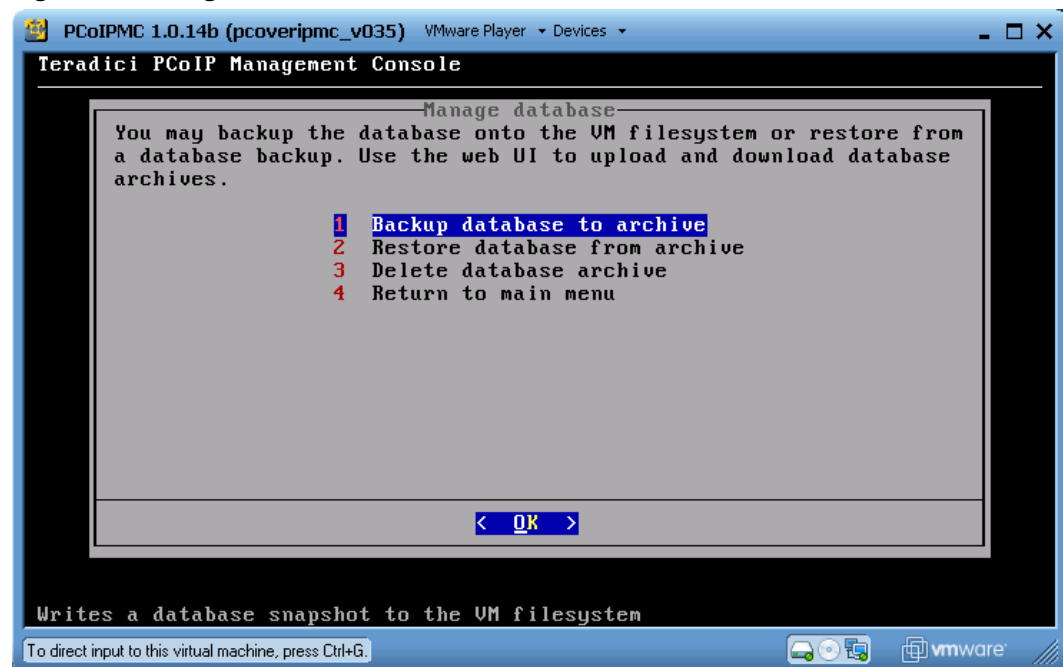
3.5 Database Management

The MC maintains a database containing information on the discovered PCoIP devices, configuration data entered by the administrator, such as device name, and other information such as firmware images that can be downloaded to PCoIP devices. The MC VM console supports commands that allow an administrator to backup and restore this database.

This feature should be used when upgrading the MC. Prior to installing the new version of the MC the user should backup the MC database, export it to an external PC, install the new version of the MC and finally import the backed up database.

Select the *Manage database* option on Figure 3-1 to access these commands. Figure 3-3 shows the MC Manage database options.

Figure 3-3: Manage MC VM Console Database



3.5.1 Backup Database

The *Backup database to archive* command allows an administrator to take a snapshot of the current database contents and store it in an archive. The archive resides within the MC VM.

This command should be used in conjunction with the download database command on the Database Management web page to backup and store the contents of the database somewhere outside of the MC VM. Refer to section 4.8.1 for information on how to download a backup file to the host PC from the MC VM.

3.5.2 Restore Database

The *Restore database from archive* command allows an administrator to update the active MC database from a previously stored archive. When this command is used the archive must already reside within the MC VM.

This command should be used in conjunction with the upload command on the Database Management web page to restore the MC database from an archive located outside of the MC VM, possibly on the MC host machine. Refer to section 4.8.1 for information on how to upload a backup file to the MC VM from a host PC.

Note: Section 2.6.2 describes the specific information that will and will not be imported into the MC by the Restore Database command.

3.5.3 Delete Database

The *Delete database archive* command allows the administrator to delete a database archive from the MC VM.

3.6 Change Time Zone

The MC retrieves the current time from the host machine. The host machine provides this time in Coordinated Universal Time (UTC) form. The host does not provide time zone information, which means the user must configure the time zone.

To configure the time zone select the *Change timezone* option on the MC VM console. The user must select a geographic area that determines the time zone. For example, the user should select America/New York if located in the same time zone as New York City.

Note: The MC can be used without configuring the time zone. The time displayed at the top of the MC VM console will be incorrect and the timestamps displayed on various screens in the MC Web Interface will be incorrect. Users are recommended to configure the time zone to match their time zone.

3.7 Restart Management Console Daemon

To restart the MC daemon select the *Restart MC daemon* option on the MC VM console. A message indicating the daemon is restarting is displayed on the MC VM console while the VM restarts. This can be used to determine when the restart is complete. This command should be executed if the MC daemon status reported on the console interface shown in Figure 3-1 is *stopped*. It should also be executed if the Management Console Health shown in the Site Status section of the home page is not *Good*.

3.8 Halt Virtual Machine

To perform a clean shutdown of the MC VM select the *Halt virtual machine* option on the MC VM console. The MC VM can be restarted at a later time. When the MC VM is restarted the MC database is restored to the state it was in when the MC VM was last stopped.

4 Web Interface

The MC web interface is the primary mechanism used by administrators to manage all PCoIP devices in a deployment. This section describes the features accessed and controlled through this interface.

4.1 Accessing the Management Console Web User Interface

Connect a computer to the same network the MC server machine is connected to. Note this computer can be the server machine itself. Open a web browser and enter the web page URL of the MC (shown on the VM console during boot up).

The MC web server has been tested and is compatible with the Firefox® 3.0 or higher and Internet Explorer® 7 and 8 web browsers. If you attempt to log into the MC web interface using a different browser an error message is displayed that lists the supported browsers.

When the web browser first connects to the MC the user will see a security warning similar to the screen shown in Figure 4-1 for Firefox or Figure 4-2 for Internet Explorer.

Internet Explorer users should follow these instructions:

- Right-click on pcoipmc_cacert.p7b and choose "Install Certificate".
- When the Certificate Import Wizard appears click the "Next >" button.
- In the next window choose to "Automatically select the certificate store based on the type of certificate." and click the "Next >" button.
- Click the "Finish" button to complete the import. The PCoIP MC CA Root Certificate is now added to the Windows' Trusted Root Certification Authorities certificate store.
- Restart Internet Explorer so that it rescans the Windows' certificate store.

Firefox users should follow these instructions:

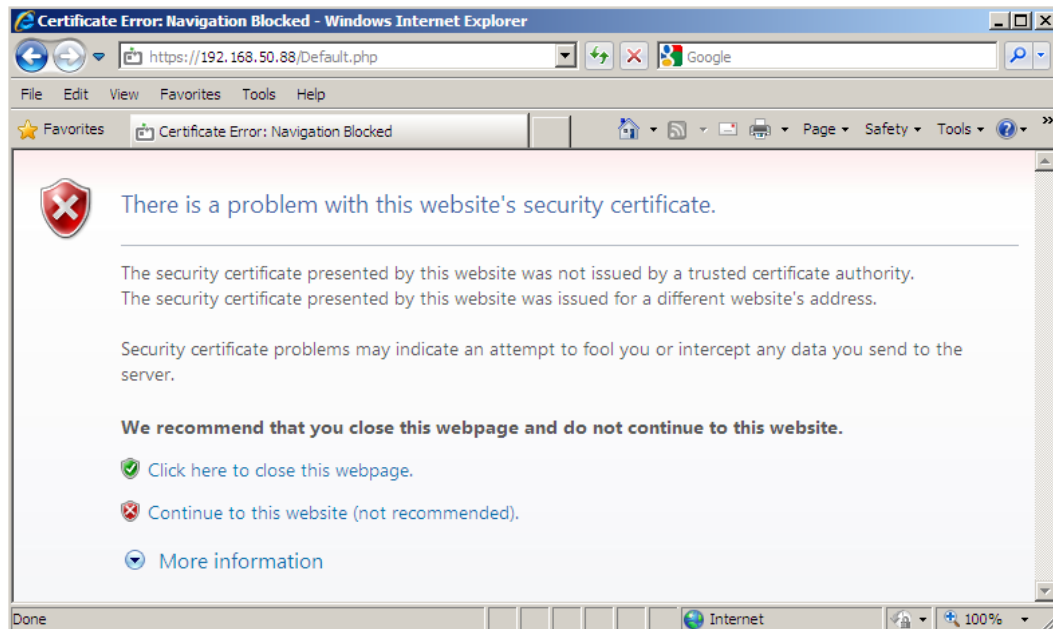
- Open the "Tools" menu and select "Options"
- Click on the icon labeled "Advanced" at the top of the window
- Go to the "Encryption" tab and click the "View Certificates" button
- Go to the "Authorities" tab and click the "Import..." button
- In the Select File dialog open pcoipmc_cacert.pem.
- When the Downloading Certificate dialog appears, check the option labeled "Trust this CA to identify web sites" and then click the "OK" button. The PCoIP Management Console Root CA certificate will now appear in the list on the Authorities tab.

Note: In Firefox you can also disable the certificate warnings by adding an exemption for the MC. To do this, click on "I Understand the Risks" on the "This Connection is Untrusted" warning page and follow the directions given to add an exemption.

Figure 4-1: Web Interface Security Warning in Firefox

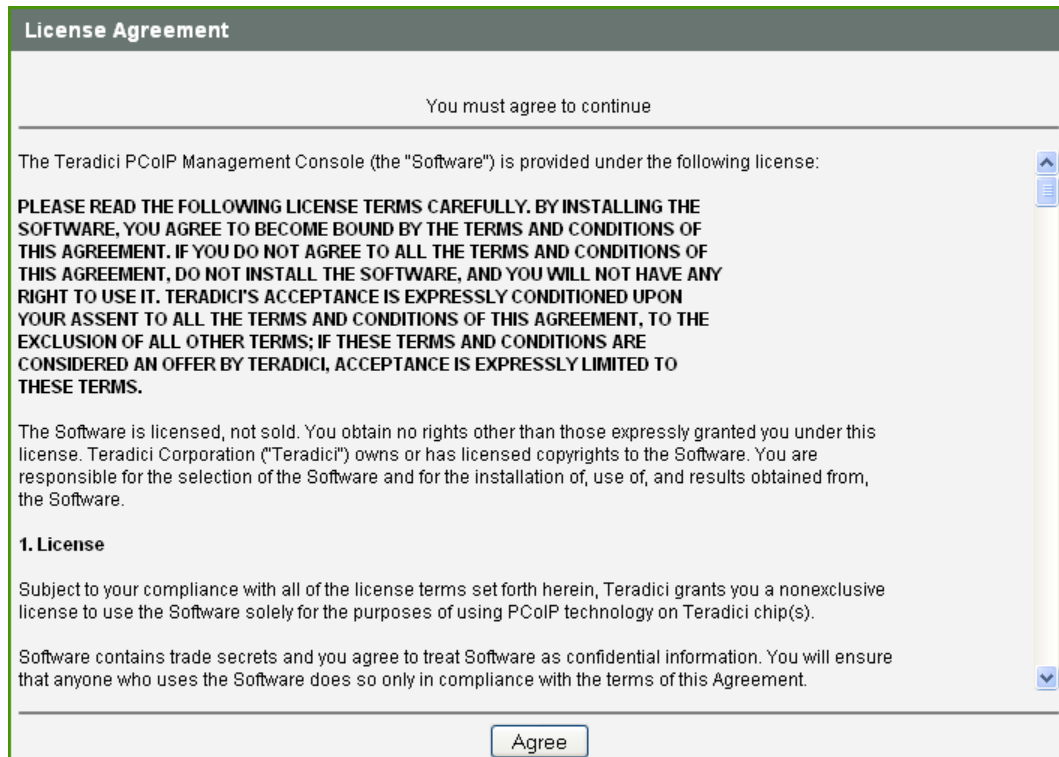


Figure 4-2: Web Interface Security Warning in Internet Explorer



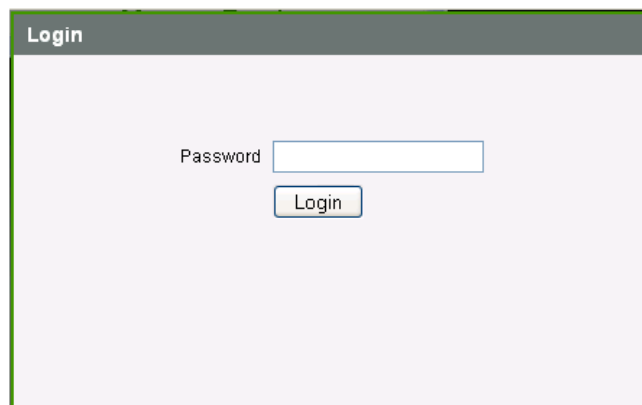
After adding the security exception in Firefox or installing the certificate in either browser it will connect to the MC and the user is prompted to accept the MC License Agreement shown in Figure 4-3. This process must be completed once. Future logins to the MC will not prompt the user to accept this agreement. The license agreement can also be viewed by clicking the *License Agreement* link near the bottom of the MC web pages. The MC License Agreement document is also included in the MC .zip file.

Figure 4-3: Management Console License Agreement



After accepting the license agreement the web browser connects to the MC and the user is prompted to enter a password as shown in Figure 4-4. The default password is blank. Section 3.2 describes how to modify this password.

Figure 4-4: Web Interface Login

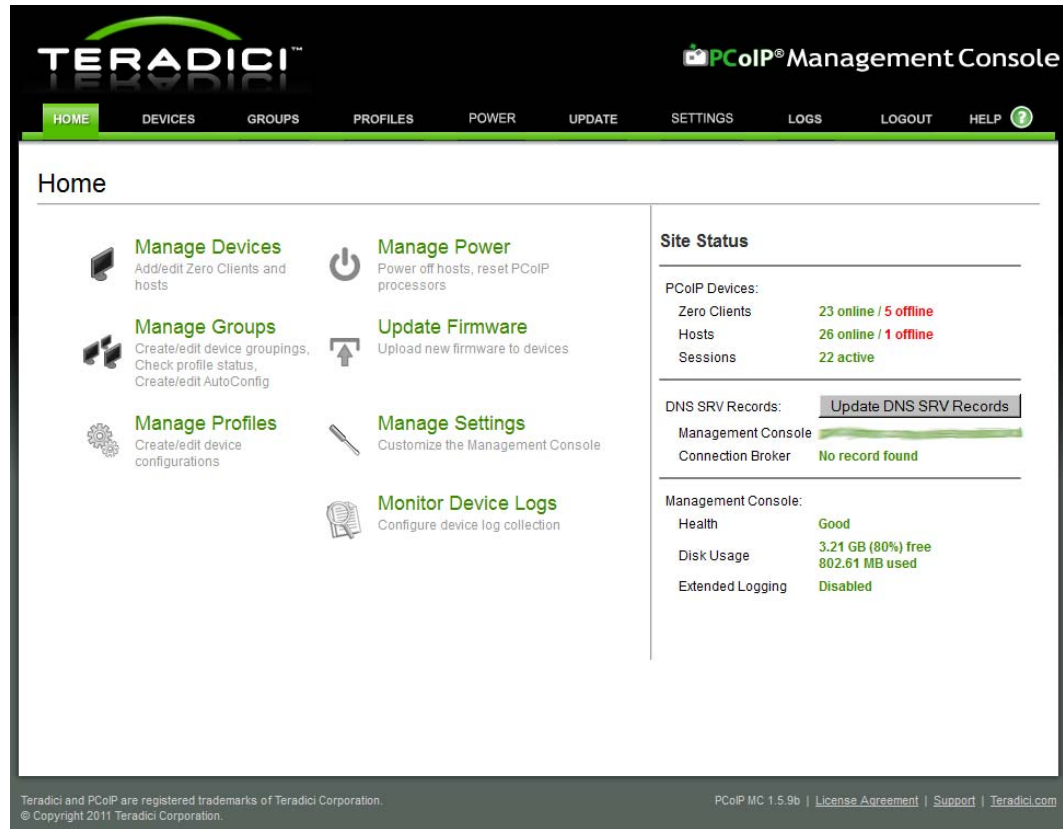


After logging in, the MC Home web page, shown in Figure 4-5, is displayed. Administrators can do the following from this web page:

- Manage devices (see section 4.2)
- Manage groups of devices (see section 4.3)
- Manage device profiles (see section 4.4)
- Reset devices (see section 4.5)
- Control the power state of Host devices (see section 4.5)
- Update device firmware (see section 4.6)

- Manage the monitoring of device event logs (see section 4.7)
- Upload/Download MC database archives (see section 4.8)
- Customize the MC configuration settings (see section 4.8)
- View site status information (see section 4.9)
- Access online help (see section 4.10)

Figure 4-5: Home Web Page

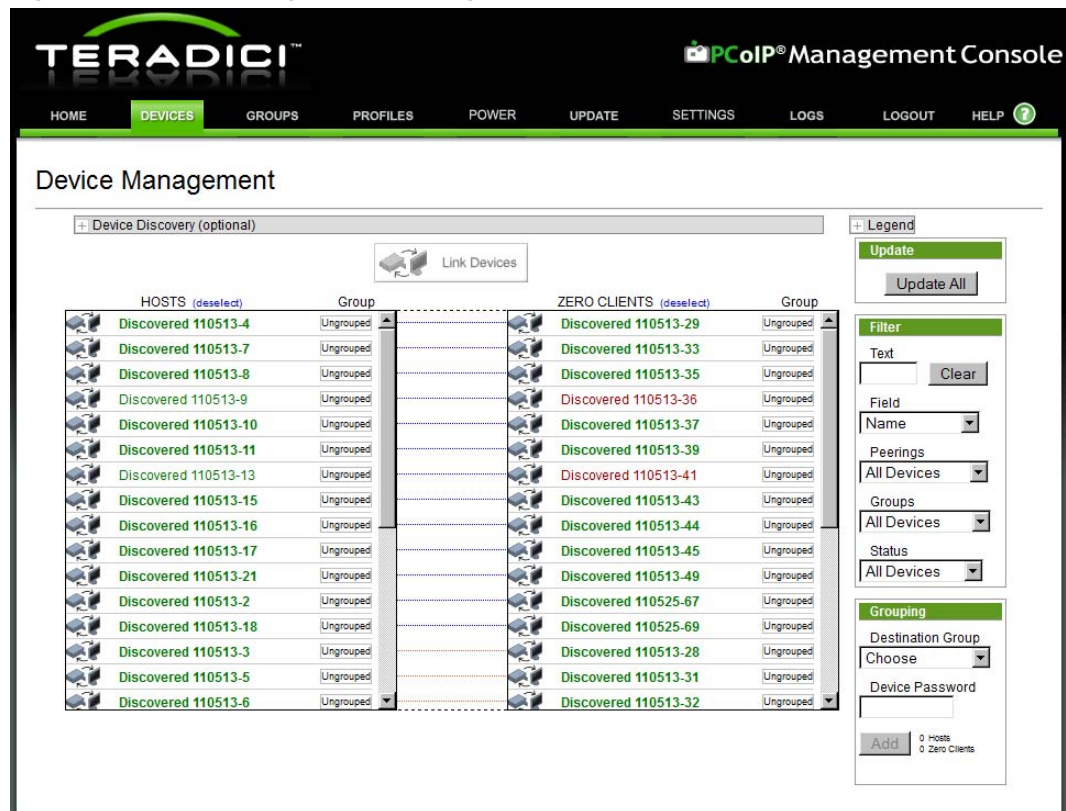


4.2 Device Management

The *Device Management* web page, shown in Figure 4-6, supports the following actions:

- Discover devices manually
- Query devices and update database
- Display a subset of devices based on various filter criteria
- Configure the group each device belongs to
- Link Host and Zero Client devices
- Open a web browser connected to device's web page
- View summary information about a device
- Configure the Name of each device
- View device details (device configuration settings, profile settings)
- Delete a device from the MC database

Figure 4-6: Device Management Web Page










4.2.1 Device Discovery (optional)

Section 1.3.3.3 describes the *Device Discovery (optional)* feature.

4.2.2 Legend

The device management *Legend*, shown in Figure 4-7, provides information that explains the meaning of special symbols and line colors displayed on the Device Management page. Open the *Legend* by selecting the “+” symbol next to the *Legend* text.

Figure 4-7: Device Management Legend Box

Legend	
Links	
	Devices peered by PCoIP MC
	Peering found in devices, not maintained by PCoIP MC
	Peering found in Zero Client, host accepts any connections, not maintained by PCoIP MC
BOLD	Device in session
TEXT	Device online
TEXT	Device offline
	Peering off screen or filtered
Devices	
	Host - Click to Login
	Zero Client - Click to Login
	Peered - Click to Login

The MC may draw a line between Host and Zero Client devices. The line indicates the two devices are linked. Host and Zero Client devices are considered linked if a PCoIP session was or still is active between the devices. The color of the line is important.



- A **green line** indicates the two devices have been peered by the MC, which means the MC database contains information about the device peering.
- A **blue** or **orange** line indicates the MC has found peering information in the device configuration settings read from the devices. The **blue line** indicates the Host and Zero Client are peered directly with each other while the **orange line** indicates the Host device is configured to accept connections from any Zero Client. If the administrator wishes to have the MC maintain this peering information the user should link the devices in the MC. Refer to section 4.2.6 for details on how this is done.
- A dashed line indicates the device is peered with another device but the other device is not drawn on the active screen. This may happen in deployments with large numbers of devices.

The bold/non-bold state of the device field name provides an indication of whether the device is currently in a session. If a session is active between a Host and Zero Client the MC will display the device field name in **bold** characters.

The green/red colour of the device field name provides an indication of whether the device is currently online. If a device's last known state was online the MC will display the device field name in green characters; otherwise the device field name will appear in red characters.

The following device symbols provide an indication of whether devices are peered.

- Peered devices are represented by the  symbol.

- Unpeered Host devices are represented by the  symbol
- Unpeered Zero Client devices are represented by the  symbol

4.2.3 Query Devices and Update Database

The MC database contains a snapshot of each device's configuration settings. The MC automatically queries each device once an hour and updates its internal database. Users wishing to force the tool to refresh its internal copy of the device settings can do this using the *Update* box on the upper right hand side of the Device Management web page. This feature allows the user to update one, multiple or all devices discovered by the MC. Keep in mind that updating a large number of devices can take a few minutes.

To update one device select the device to update and then click the *Update Device* button.

To update multiple devices select the devices by holding down the Shift button and selecting the devices. After the devices are selected click the *Update Devices* button.

To update all devices ensure no devices are selected by clicking the deselect links at the top of the HOSTS and ZERO CLIENTS columns. When no devices are selected click the *Update All* button.

Users may want to know when the update completes. A future release of the MC will display a status bar that provides this information. To view the update time using the current version of the tool users should set the Field option in the Filter box equal on the Device Management web page equal to *Last Updated*.

4.2.4 Filtering Devices

The *Filter* box supports different ways of filtering the PCoIP devices displayed in the HOSTS and ZERO CLIENTS columns. This can be useful when searching for specific devices or subsets of devices. Administrators can filter devices using one or more of the following options.

- The *Field* dropdown menu allows users to select the device data field displayed in the HOSTS and ZERO CLIENTS columns. Users can select from *Name*, *Unique ID*, *MAC Address*, *IP Address*, *Firmware Version*, *FQDN* or *Last Updated Time*.
 - The *Name* field is a user defined value assigned to each device managed by the MC. This field is stored in the MC database. It is not stored in the device configuration settings. Section 4.2.8.1 describes how to configure the device *Name*.
 - The *Unique ID* and *MAC Address* fields are read-only device configuration fields provisioned at the factory.
 - The *IP Address* is configured statically in the device or dynamically by a DHCP server.
 - The *Firmware Version* is determined by the firmware loaded on the device.
 - The *FQDN* is the device FQDN if one has been registered with the deployments DNS server. If the FQDN is not registered with the DNS server the MC displays the device IP address.
 - The *Last Updated* option displays the timestamp of when the MC last updated its internal database with the actual device configuration settings.
- The *Text* field allows administrators to enter a text string. The MC displays all devices in which the device *Field* value matches the string. For example, if the *Field* menu

specifies *Firmware Version* and the user enters the string *1.9* in the *Text* field the tool displays all devices loaded with release 1.9.

- The *Peerings* dropdown menu allows administrators to display all devices, peered devices or unpeered devices.
- The *Groups* dropdown menu allows administrators to display all devices, grouped devices, ungrouped devices, and devices in individual groups.
- The *Status* dropdown menu allows administrators to display all devices, online devices, offline devices, devices with an active session and devices without an active session.

4.2.5 Configure Device Group

All devices managed by the MC should be added to a group. If a device is not in a group the following actions cannot be performed on the device.

- Apply a profile to the device
- Peer the device
- Send power management commands to the device
- Update firmware on the device
- Edit the device name

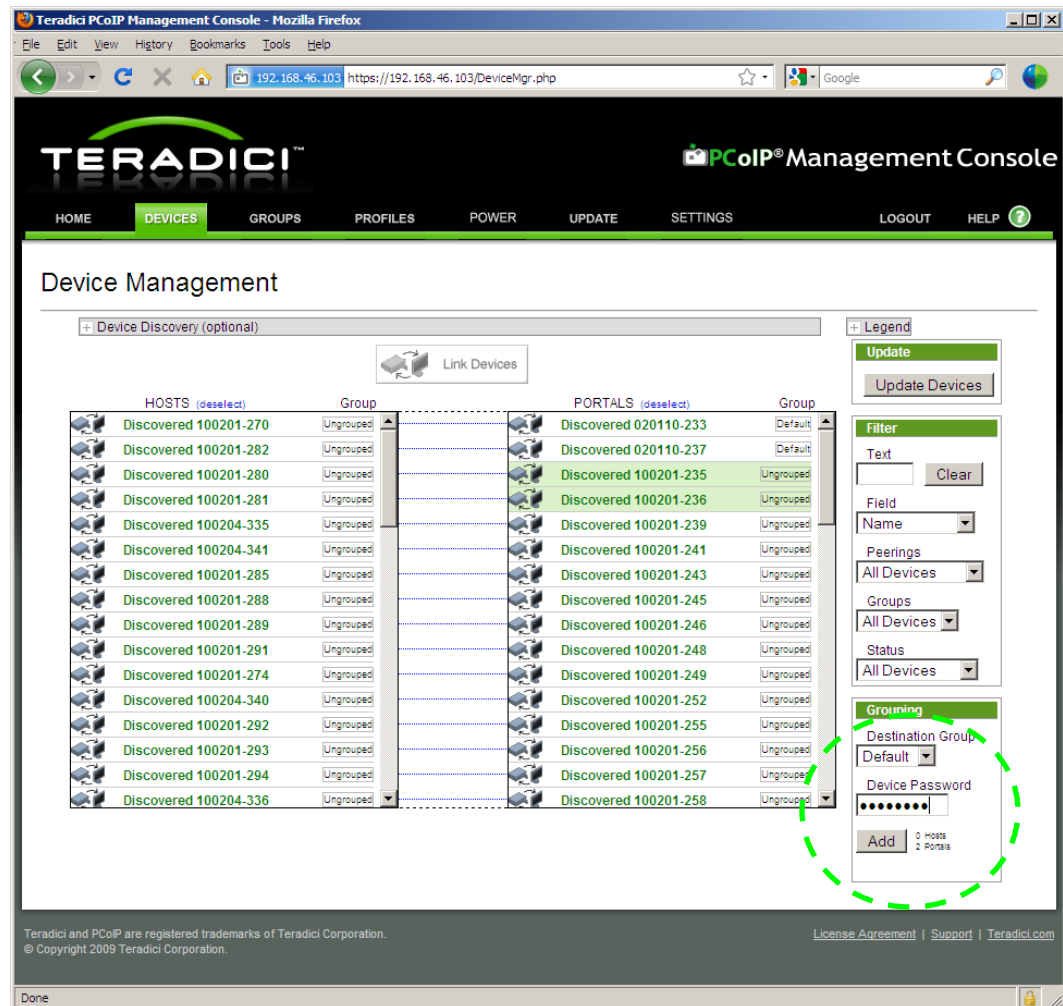
The concepts associated with a MC group are explained in section 1.3.1.

Users can add or reassign one or more devices to a group by executing the following steps.

1. Select the device or devices to be added to the group. Multiple Zero Client or Host devices can be selected by holding down the shift key while selecting the devices.
2. Select the group to add the devices to using the *Destination Group* dropdown menu.
3. Enter the device password in the *Password* field.
4. Select the *Add* button. The selected devices are then added to the specified group if the device password is correct. The group field for each device successfully added to the group will be updated to equal the new group.

Figure 4-8 shows the Device Management web page when adding two Zero Clients (“Discovered 100201-235” and “Discovered 100201-236”) to the Default group.

Figure 4-8: Adding Devices to a Group

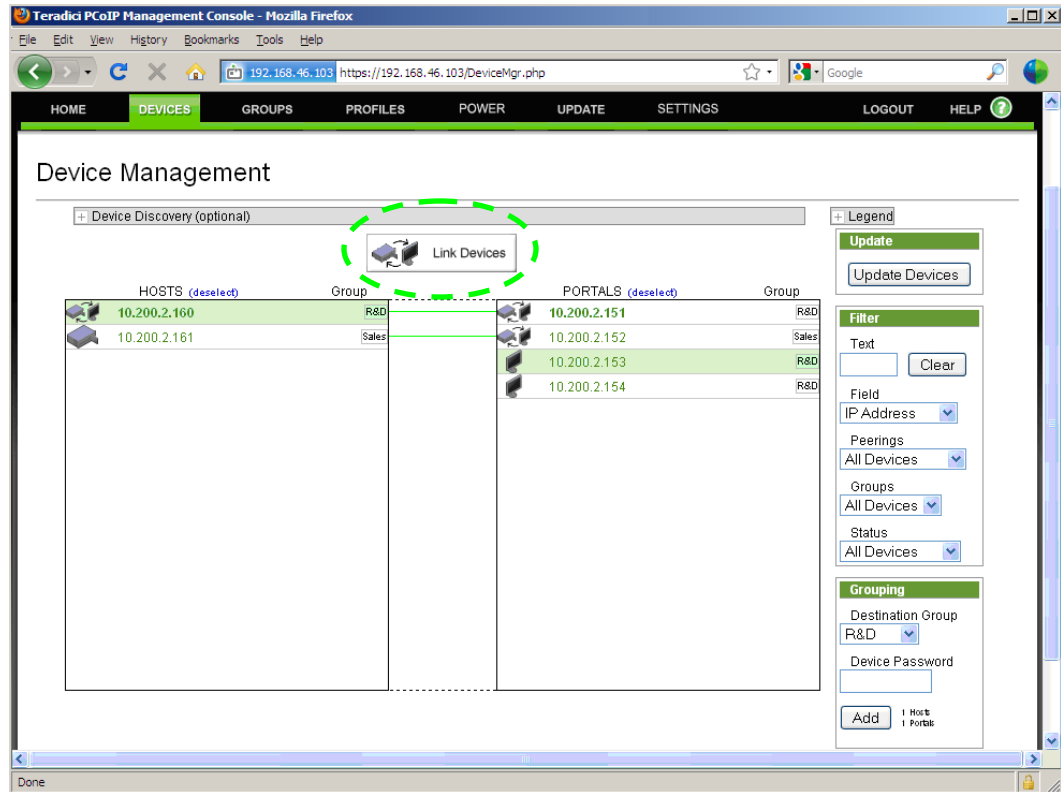


4.2.6 Linking Devices

Individual Host and Zero Client devices can be linked together. After two devices are linked, the Zero Client will always establish a PCoIP session with the linked Host when a user initiates a connection and the Host will only accept connections from the linked Zero Client. To link a Host and Zero Client execute the following steps.

1. Select the Host and Zero Client devices to be linked. In Figure 4-9 the devices 10.200.2.160 and 10.200.2.153 are selected.
2. Select the *Link Devices* button displayed below the *Device Discovery* command. After two devices are linked a green line appears connecting them. This indicates the devices are linked in the MC database. At this point the Zero Client will connect to the Host 10.200.2.160 when the user selects *connect* on the Zero Client OSD. Section 4.2.2 provides additional details on the meaning of lines connecting devices.

Figure 4-9: Peering a Pair of Devices



Note: After two devices are linked by the MC the MC updates the Zero Client device session configuration data if it detects a change in a peered Host device’s IP address. When the MC detects that a Host’s IP address has changed, it looks up the Host’s peer in the database and attempts to write the new IP address into the Zero Client session settings. It will keep trying to update the Zero Client until it succeeds. This feature only works if both endpoints are discoverable by SLP or they advertise themselves to the MC through DNS SRV or the device PCoIP MC DNS-Based Discovery Prefix configuration field is equal to the address of the MC managing the device.

Note: This feature is disabled when the *Brokered* setting equals Yes. See section 4.8.2 for additional details.

4.2.7 Access Device Web Page

All PCoIP devices have an embedded web server that provides an administrator with access to device configuration settings and status. Administrators can access this web server using a standard web browser. The MC provides multiple quick links that access the device’s web page. Refer to the PCoIP Administrative Interface User Manual (TER0606004) for additional information on the device web server.

To access a device’s web page from the Device Management web page select the symbol to the left of the device *Field*. Host symbols are either or based on whether or not the device is linked and Zero Client symbols are either or .

4.2.8 Summary Device Information

Administrators can view summary information about each device by clicking on the device *Field* in the list of HOSTS or ZERO CLIENT devices. After doing this a dialog box appears that provides information about the device. Figure 4-10 displays a summary information dialog box.

Figure 4-10: Summary Device Information Dialog Box



In addition to displaying summary information about a device the dialog box allows the user to configure the device name, view additional device details, delete the device from the MC database and view the device event log.

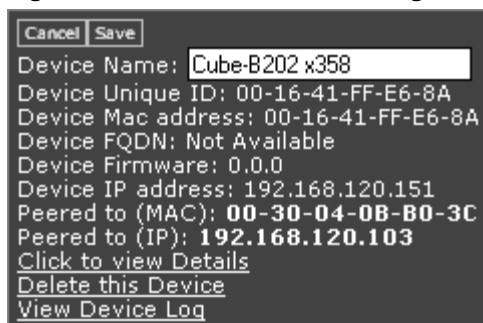
4.2.8.1 Configure Device Name

An administrator should configure the *Name* of each device in the system and the device names must be unique. The *Name* field is a string that users can set equal to whatever they want. Users should consider including location information in the name to simplify locating the device, but this is up to the administrator to decide.

When a device is first discovered, the MC sets the *Name* equal to a string containing a timestamp and a unique number. Users can modify the *Name* by executing the following steps.

1. Click on the device to display the summary device information dialog box.
2. Click on the summary device window again. This opens a text editing field that shows the current device *Name*.
3. Enter the new device *Name*.
4. Select the *Save* button to update the device *Name*. Figure 4-11 displays the summary information dialog box while the device name is being edited.

Figure 4-11: Edit Device Name Using Summary Device Information Dialog Box



Note: The device must be part of a group before the *Name* can be configured.

4.2.8.2 Access Device Details

The MC maintains additional device details not shown on the Device Management page. To access these details for an individual device execute the following steps.

1. Click on the device to display the summary device information dialog box.
2. Select the *Click to view Details* link in the summary device information dialog box. Section 4.2.9 describes the features of the Device Details web page.

4.2.8.3 Delete Device from Management Console Database

To delete a PCoIP device from the MC database execute the following steps.

1. Click on the device to display the summary device information dialog box.
2. Click on the *Delete this Device* link in the summary device window.

Note: All information maintained on the device by the MC is deleted. This includes the device name, group, peering information and other information.

4.2.8.4 View Device Event Log

All PCoIP devices maintain a persistent event log containing messages that may be useful in diagnosing problems. To view a device's event log execute the following steps.

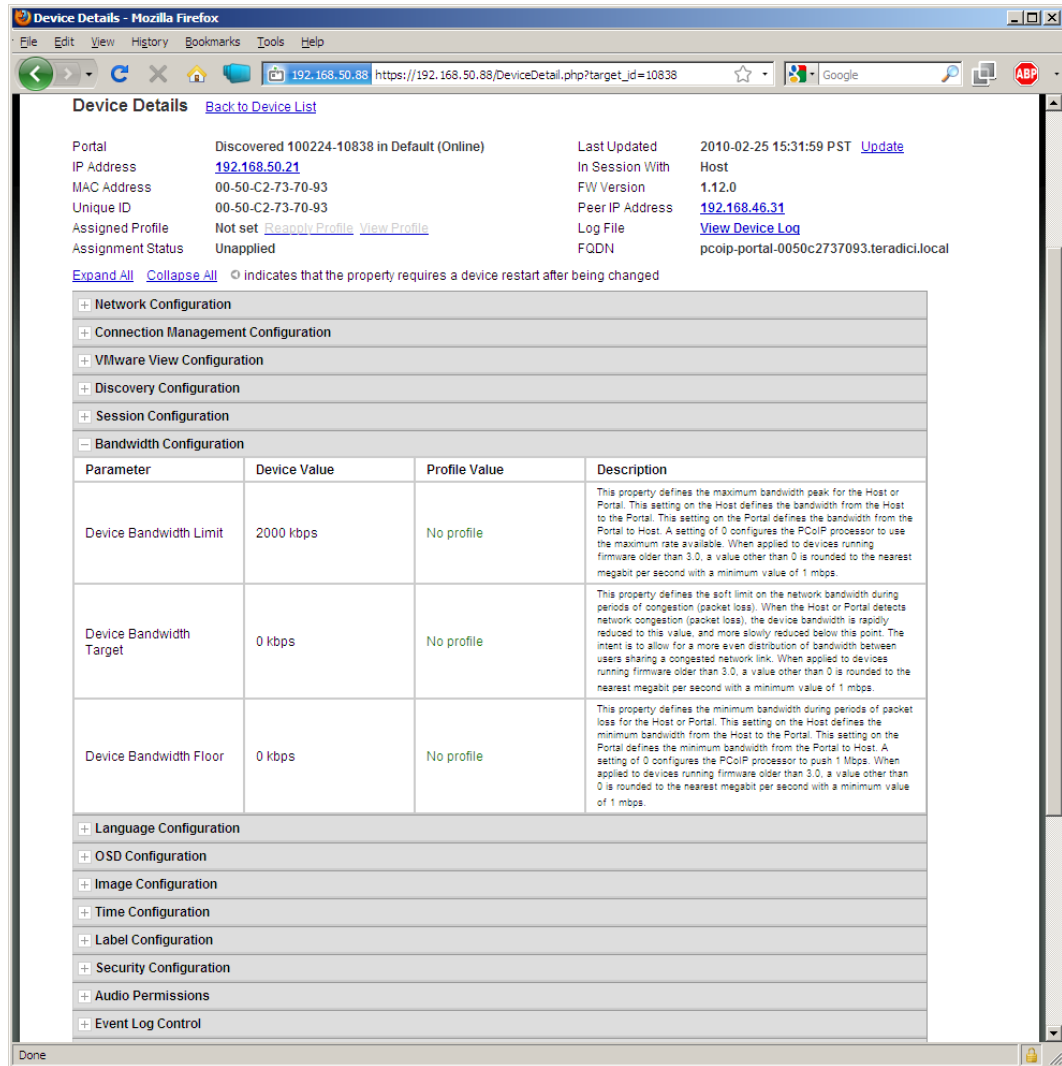
1. Click on the device to display the summary device information dialog box.
2. Click on the *View Device Log* link in the summary device window.

4.2.9 Device Details

Section 4.2.8.2 describes how to access the device details web page. Figure 4-12 shows a Zero Client device details web page, which supports the following actions:

- Display device configuration settings and status
- Refresh the MC device configuration settings by querying the device
- Write the current profile settings to the device
- Open the device's profile
- Open a web browser connected to device's web page
- Open a web browser connected to device's peer web page
- View the device's event log

Figure 4-12: Zero Client Device Details Web Page



4.2.9.1 Device Configuration and Status

The device details web page displays device configuration and status data in addition to device profile data. When the web page is first displayed the device categories are collapsed.

- Users can open individual categories by selecting the “+” next to the category name. The *Bandwidth Configuration* category is expanded in Figure 4-12.
- Users can view all of the categories by selecting the *Expand All* link.
- Users can collapse all of the categories by selecting the *Collapse All* link.

Below is a list of the possible values assigned to each *Profile Value* and a description of the meaning.

- <value> – The parameter is specified in the profile and defined to equal <value>.
- **Not in profile** – The parameter is not specified in the profile.
- **Read only** – The parameter cannot be specified in the profile.

Below is a list of the possible values assigned to each *Device Value* and a description of the meaning.

- <value> – The parameter is specified in the device and equal to <value>.

- **(Empty string)** – The parameter is not configured in the device. Some fields such as the Connection Management System (CMS) address equal this when the device is not configured to use a CMS.
- **Not supported** – Certain device parameters are only applicable to specific devices or device models. This value is displayed for device parameters that are not supported by a device.

4.2.9.2 Refresh Device Settings Stored in Management Console

The information shown in the *Device Value* column is a copy of the data stored in the device. The MC keeps track of the last time it updated its internal copy of the device data. The *Last Updated* field on the Device Details web page displays this timestamp.

Administrators can force the MC to refresh its internal copy of the device values by selecting the *Update* link.

4.2.9.3 Write Profile Settings to Device

The *Reapply Profile* link allows the user to write the device profile settings to the device. This can be useful in situations when the administrator wants to write the profile settings to a single device in a group.

4.2.9.4 Open Device Profile

The *View Profile* link opens the Profile Management web page for the profile associated with this device. Administrators can use this link to quickly access and/or modify the profile settings.

4.2.9.5 Access Device & Peer Web Pages

All PCoIP devices have an embedded web server that provides an administrator with access to device configuration settings and status. Administrators can access this web server using a standard web browser. The MC provides multiple quick links that access the web page.

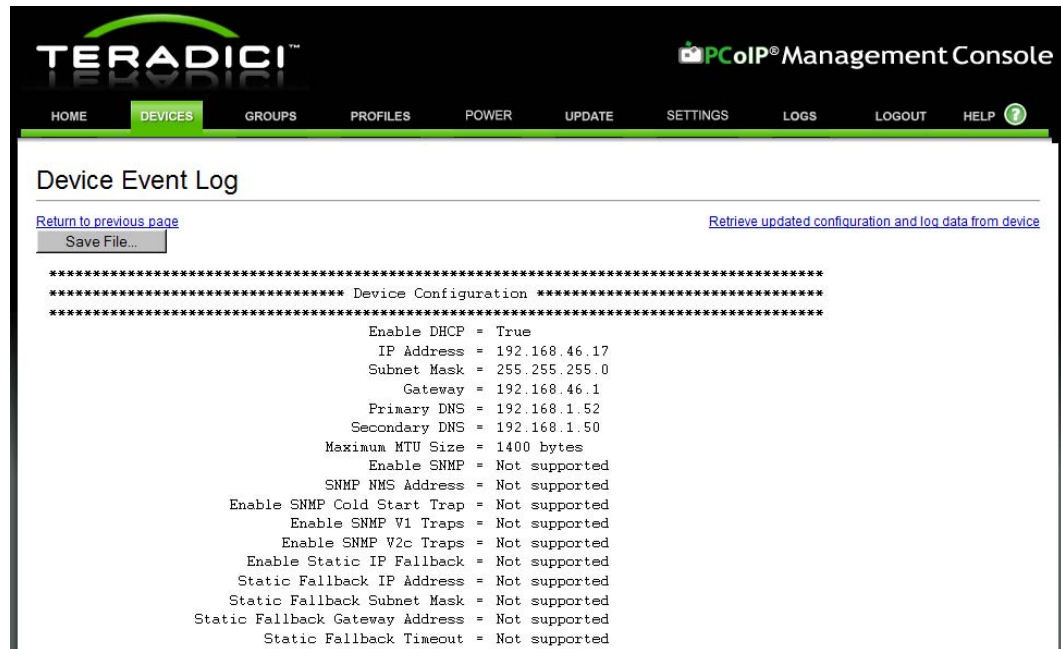
- To access a device's web page from the Device Details web page select the *IP Address* link.
- To access the peer device's web page from the Device Details web page select the *Peer IP Address* link.

4.2.9.6 View Device Log

All PCoIP devices maintain a persistent event log containing messages that may be useful in diagnosing problems. Administrators can access this event log by selecting the *View Device Log* link. Figure 4-13 shows a Device Event Log web page.

The administrator can save the event log to a file using the *Save File* button or retrieve the most recent event log data from the device using the *Retrieve updated log data from device* link.

Figure 4-13: Device Event Log Web Page

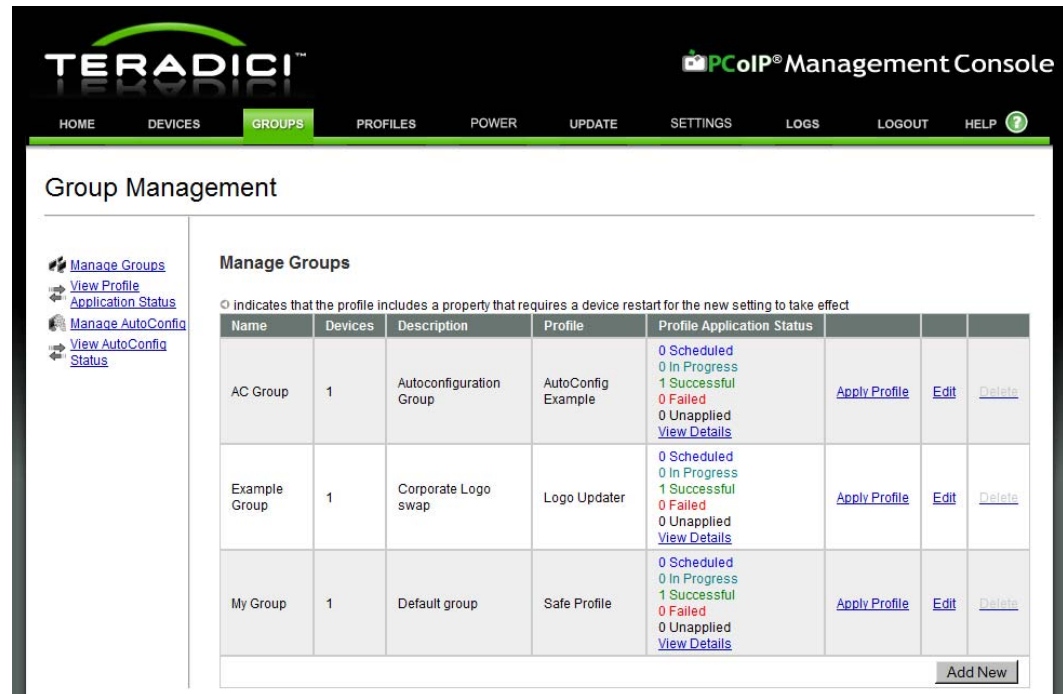


4.3 Group Management

The *Group Management* web page, shown in Figure 4-14, allows administrators to view the currently defined groups and the number of devices in each group, manage AutoConfig rules and view profile application status information. Administrators can initiate the following actions using this web page.

- Create/Modify/Edit/Delete groups
- Apply a profile to all devices in a group
- View profile application status information
- Create/Modify/Edit/Delete AutoConfig rules
- Enable/Disable AutoConfig globally
- View AutoConfig status information

Figure 4-14: Group Management Web Page



4.3.1 Manage Groups

The Manage Groups subcategory allows administrators to view, create, edit and delete groups and select a profile to associate with each group. For groups with profiles this page shows an application status summary and provides a method to apply the profile settings to the entire group.

4.3.1.1 Create a Group

The *Add New* button allows administrators to create a new group. After selecting this button the user is prompted to enter the group *Name*, *Description* and *Profile* associated with the new group.

Note: When the MC is initially started the *Default* group is created. This is done to simplify the use of the MC by not forcing users to create a group. Administrators are free to use this group or delete it.

4.3.1.2 Modify a Group

The *Edit* link allows the administrator to modify the group *Name*, *Description* and/or *Profile* associated with a group.

4.3.1.3 Delete a Group

The *Delete* link allows the administrator to delete a group. A group can only be deleted if there are no devices in the group. The *Delete* link is not active (grayed out) when a group has one or more devices in it.

4.3.1.4 Profile Application Status

The Profile Application Status column provides a summary of the state of profile application to the devices in the group. When the *Details* link is clicked the tool displays

the View Profile Application Status page with the filter set to this group. Figure 4-14 shows the summary for the Sales group. Below is a description of each status category:

- **Successful** – The profile was successfully written to the device.
- **Scheduled** – The MC has scheduled the profile to be written to the device.
- **Failed** – The MC attempted but failed to write the profile to the device. Typically this problem occurs when devices are offline.
- **Unapplied** – The profile has been modified since it was last written to the device. This allows users to know when they need to re-apply a profile to one or more devices in a group.

4.3.1.5 Apply a Profile to a Group

The *Apply Profile* link allows an administrator to write the device profile settings to every device in a group.

Profiles can contain properties that require a device reboot when the profile is applied. The Apply Profile confirmation dialog displays radio buttons to select automatic or manual device rebooting. Figure 4-15 shows the reboot behavior choices. The default behavior is to automatically reboot the device.

Profiles can be scheduled to be applied in the future. Clicking in the field *Apply Profile at Date/Time* will display a graphical date/time picker. Figure 4-16 shows the date/time picker.

To determine when the profile has been written to all devices in the group the administrator should watch the Group Management web page until the number of *Scheduled* updates equals 0. At this point the MC has completed all attempts to write the profile to the devices in the group. If a device was offline when the MC attempted to write the profile the status is marked as *Failed*. Further information is available by clicking View Details which displays View Profile Application Status with the filter set to this group.

Figure 4-15: Apply Profile reboot behavior options

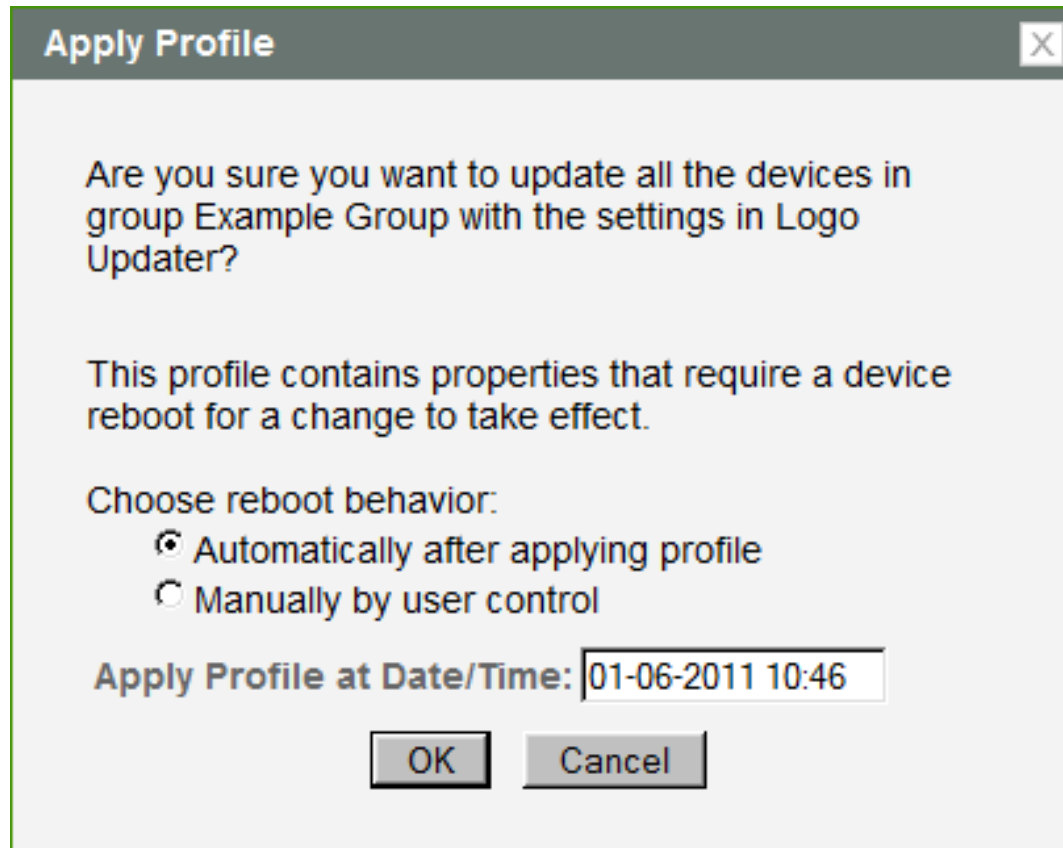
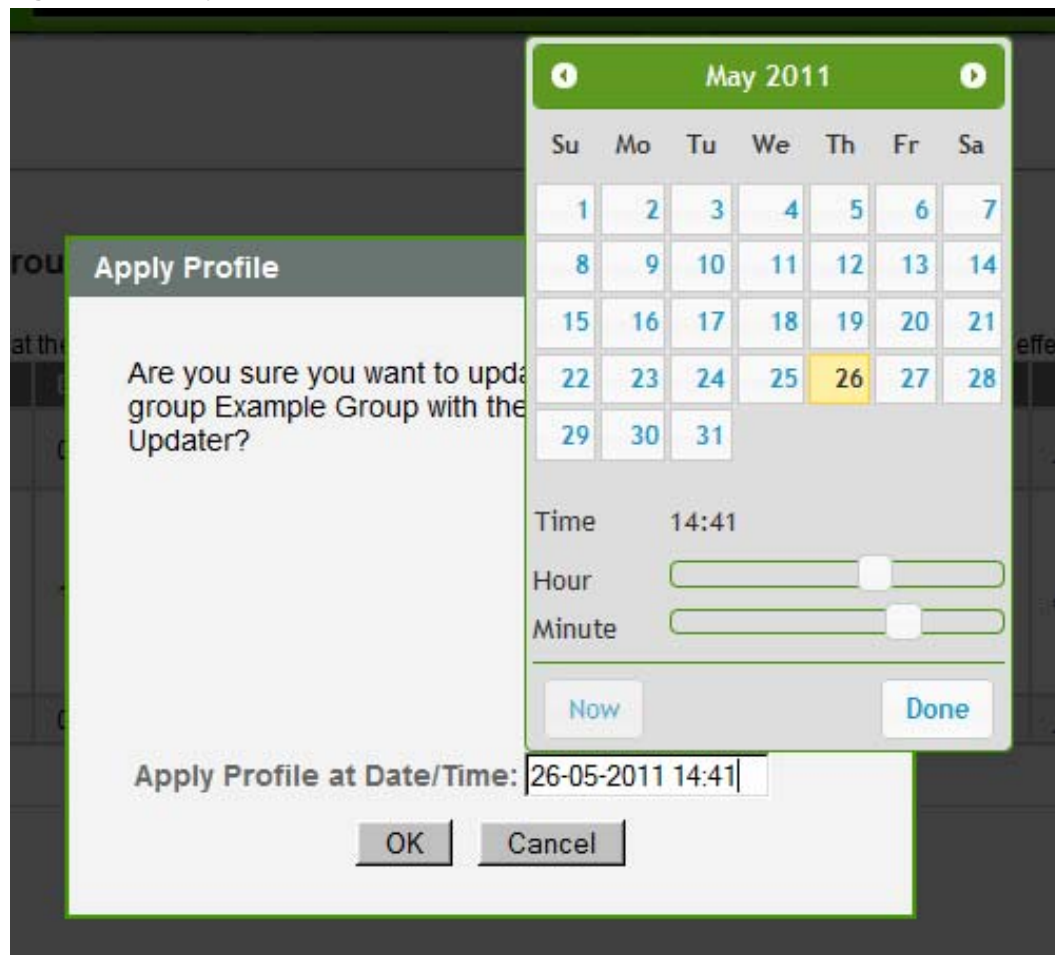


Figure 4-16: Apply Profile date/time picker






4.3.2 View Profile Application Status

The *Profile Application Status* subcategory, shown in Figure 4-17, provides detailed status information that shows the current state of profile application for grouped devices.

The Profile column also displays icons representing the expected reboot behavior of devices when the profile is applied.

The legend contains the following description of each reboot icon:

	indicates that the profile includes a property that requires a device restart for the new setting to take effect
	indicates that the profile was scheduled by AutoConfig
	indicates that upon profile application the device will be rebooted automatically

Below is a description of each status category:

- **scheduled** – The MC has scheduled the profile to be written to the device.
- **OSD logo scheduled** – The MC has scheduled the profile’s included OSD logo to be written to the device.

- **firmware scheduled** – The MC has scheduled the profile’s selected firmware to be written to the device.
- **complete** – The profile along with any included OSD logo and firmware was successfully written to the device.
- **failed** – The MC attempted but failed to write the profile to the device. Typically this problem occurs when devices are offline.
- **OSD logo done** – The MC has complete writing the OSD logo to the device.
- **firmware pending reboot** – The MC has completed writing the profile’s selected firmware to the device and requires a reboot before the profile properties will be written.
- **firmware done** – The MC has completed writing the profile’s selected firmware to the device which has also been rebooted.
- **unapplied** – The profile has been modified since it was last written to the device. This allows users to know when they need to re-apply a profile to one or more devices in a group.

Figure 4-17: View Profile Application Status Web Page

Group Management

Profile Application Status

Legend

- ⊖ indicates that the profile includes a property that requires a device restart for the new setting to take effect
- ⚙ indicates that the profile was scheduled by AutoConfig
- ⏻ indicates that upon profile application the device will be rebooted automatically

View: All groups | All statuses | All time

Group	Profile	Name	IP	MAC	Status
Example Group	⏻ Logo Updater	⚙ Discovered 110513-14	192.168.46.31	00-1A-64-88-00-58	complete 2011-05-19 08:31:36 PDT

4.3.3 Manage AutoConfig

The Manage AutoConfig subcategory, shown in Figure 4-18, allows administrators to enable or disable the AutoConfig feature and configure the AutoConfig rules. By default, AutoConfig is disabled and no AutoConfig rules are defined.

An AutoConfig rule can optionally be created for each group. Newly discovered Zero Client devices are automatically added to a group and have that group's profile applied when conditions 1, 2 and 3 are all true.

Condition 1: The AutoConfig feature is enabled.

Condition 2: The group's AutoConfig rule has no IP address ranges OR the Zero Client's IP address is within one of the rule's IP ranges.

Condition 3: The Zero Client has either a blank password or password protection is disabled and the AutoConfig rule has "Add device with no password" checked OR the Zero Client's password is one of the rule's passwords.

The following examples illustrate how AutoConfig rules are applied. The MC is configured with AutoConfig enabled and has two AutoConfig rules.

Table 4-1: Example AutoConfig rules

Group	Device Password Cdn3	IP Range Cdn2
Group A	<input type="checkbox"/> Add device with no password PASSWORD	<Empty>
Group B	<input checked="" type="checkbox"/> Add device with no password	192.168.50.1 - 192.168.50.254

Table 4-2: Example AutoConfig rule application

Note: AutoConfig is enabled so condition 1 is always true.

Zero Client		Group A Rule		Group B Rule		AutoConfig Result
IP	Password	Cdn 2	Cdn 3	Cdn 2	Cdn 3	
192.168.60.10	PASSWORD	TRUE	TRUE	FALSE	FALSE	Added to Group A
192.168.50.10	PASSWORD	TRUE	TRUE	TRUE	FALSE	Added to Group A
192.168.60.20		TRUE	FALSE	FALSE	TRUE	Not added to any group
192.168.50.20		TRUE	FALSE	TRUE	TRUE	Added to Group B

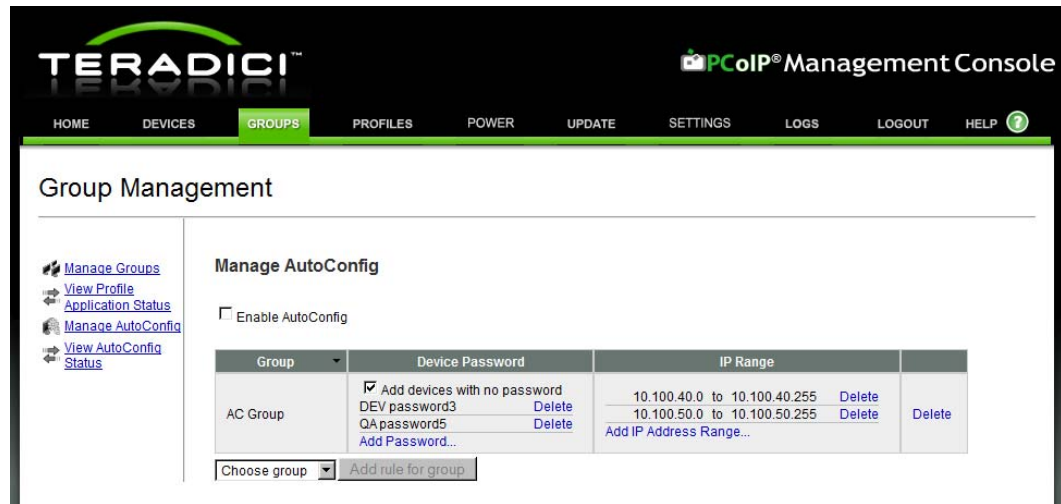
To create a new AutoConfig rule:

1. Optionally disable AutoConfig before adding or editing rules. This is recommended practice so interim rule configurations do not result in unexpected group memberships.
2. Choose an existing group from the *Choose Group* select box and click *Add rule for group*. When a new rule is created it has no IP ranges, no specific passwords and Add device with no password is checked. If AutoConfig is enabled this rule will match all Zero Clients with no password.
3. To restrict the rule's password matching click *Add Password* to add one or more specific passwords to the rule. Once the rule contains one or more specific passwords the *Add devices with no password* checkbox can be cleared if desired. There is no limit on the number of specific passwords a rule can have.
4. To restrict the rule's IP address matching click *Add IP Address Range* to add one or more IP address ranges. There is no limit on the number of IP address ranges a rule can have.
5. If AutoConfig was disabled in step 1 enable it now to make the current rule configuration active.

When two rules conflict with each other the Manage AutoConfig screen will display a warning. Leaving rule conflicts unresolved will result in unexpected group memberships as the AutoConfig feature randomly selects which rule gets applied to a Zero Client that satisfies more than one rule.

After creation, AutoConfig rules can be freely edited by adding and removing specific passwords and IP address ranges and changing the Add devices with no password checkbox. Again, it is recommended to disable AutoConfig before editing the rules and to re-enable it when done.

Figure 4-18: Manage AutoConfig Web Page



4.3.4 View AutoConfig Status

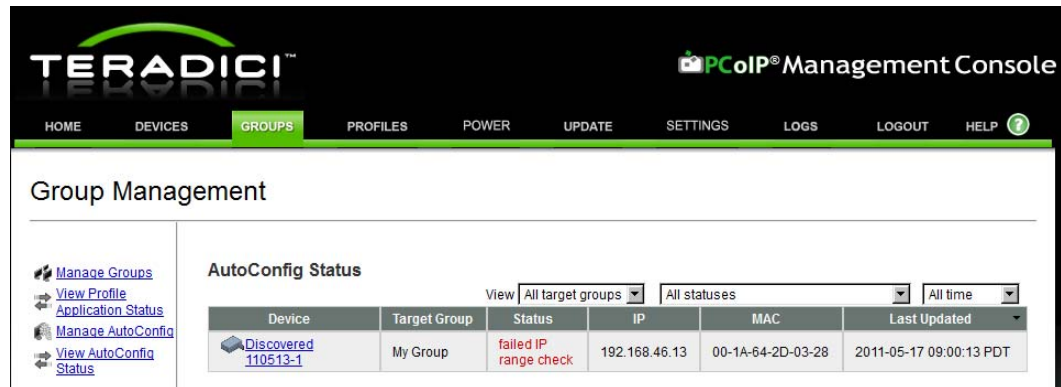
The *View AutoConfig Status* subcategory, shown in Figure 4-19, provides status information that shows if devices have been discovered and fit the criteria of existing AutoConfig rules along with the profile application status.

When AutoConfig is disabled on the Manage AutoConfig web page newly discovered Zero Clients will not appear on the View AutoConfig Status web page.

Below is a description of each status category:

- not started – The MC has not yet checked this device for AutoConfig rule compatibility.
- **failed** – The device failed to be added to this group for a reason other than AutoConfig criteria.
- **failed offline** – The device could not be reached for verification of AutoConfig rule criteria.
- **failed IP range check** – The device does not match the AutoConfig rule IP range criteria.
- **failed password check (no password)** – The device does not match the no password setting for this rule.
- **failed password check (no match)** – The device does not match the password criteria for this rule.
- **added to group** – The MC has completed adding the device to this group and will proceed to apply the profile.

Figure 4-19: View AutoConfig Status Web Page

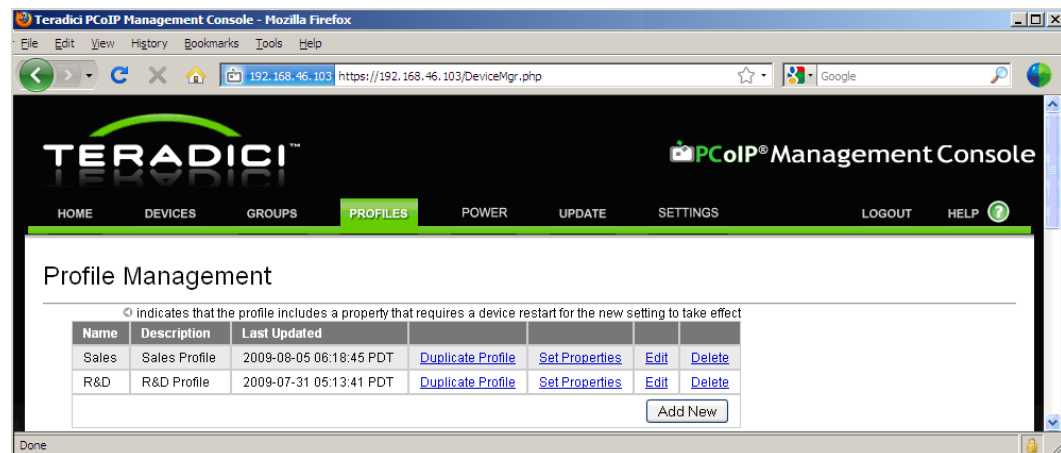


4.4 Profile Management

The *Profile Management* web page, shown in Figure 4-20, allows administrators to view the currently defined profiles along with the time each profile was last modified/updated. Administrators can initiate the following actions using this web page.

- Create new profiles
- Duplicate profiles
- Delete profiles
- Modify the profile *Name* and *Description*
- Modify the profile properties (device configuration settings)

Figure 4-20: Profile Management Web Page



4.4.1 Create a Profile

The *Add New* button allows administrators to create a new profile. After selecting this button the user is prompted to enter the profile *Name* and *Description*.

4.4.2 Duplicate a Profile

The *Duplicate Profile* link creates a new profile with the same profile properties as the selected profile. The administrator should select the *Edit* link to set the profile *Name* and *Description* after duplicating a profile.

Note: Administrators may find it useful to create an initial profile containing the settings that are common across all devices in the deployment. After the initial profile is setup the profile can be duplicated and the unique profile settings can then be configured.

4.4.3 Delete a Profile

The *Delete* link allows the administrator to delete a profile. The *Delete* link will not work if a profile is associated with one or more groups. To delete a profile assigned to one or more groups use the Group Management web page to first assign a different profile to the group(s) currently using the profile.

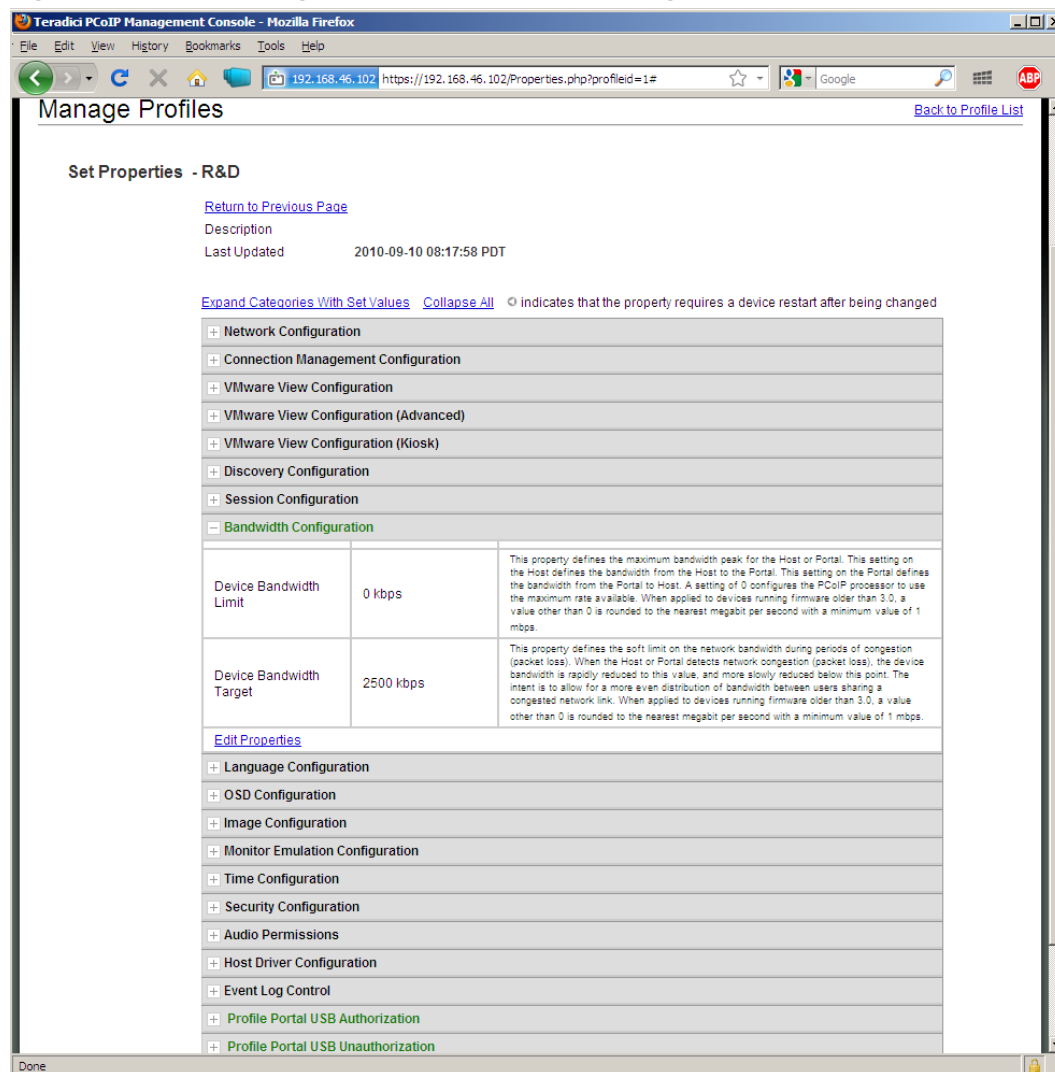
4.4.4 Modify Profile Name & Description

The *Edit* button allows users to configure the profile *Name* and *Description*. After selecting this button the user is prompted to enter the profile *Name* and *Description*.

4.4.5 Modify Profile Properties

The *Set Properties* link allows administrators to configure the properties of a profile. Figure 4-21 shows the Profile Management Set Properties web page.

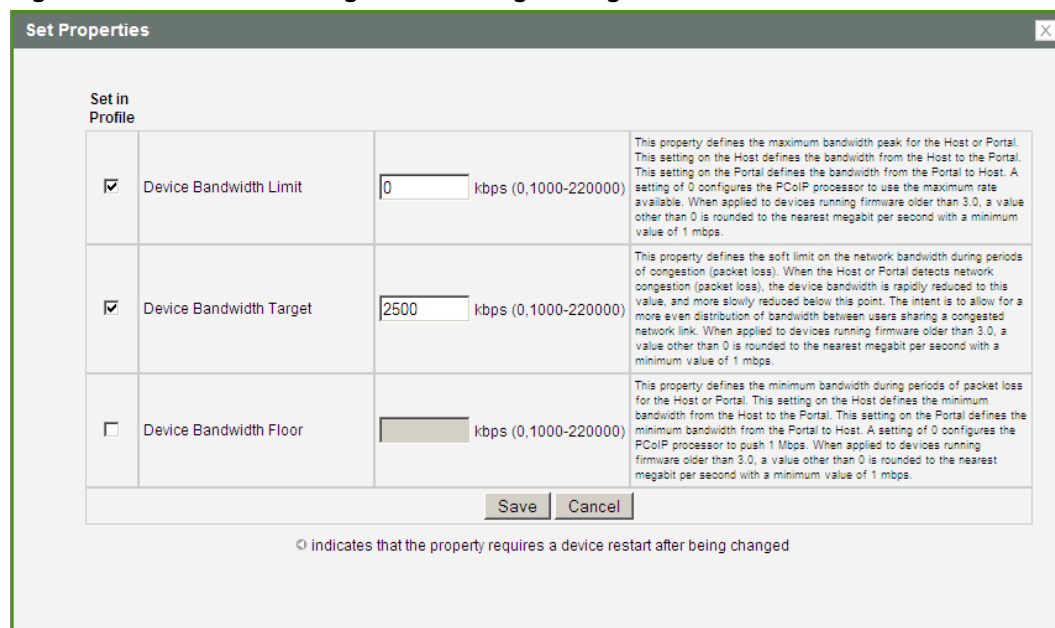
Figure 4-21: Profile Management – Set Properties Web Page



Each group of devices managed by the MC can have a profile assigned to it. The concepts associated with a MC profile are explained in section 1.3.1. An important thing to be aware of is the fact profiles can be created that do not define values for every profile property.

To define individual profile settings expand the profile property category. The *Bandwidth Configuration* category is expanded in the previous figure. When a category is expanded the *Edit Properties* link is accessible. Select this link to open a dialog box used to specify the category property settings. Figure 4-22 shows the Bandwidth Configuration Settings dialog box. Each checkbox on the left determines whether a setting is included in the profile and the fields on the right determine the value of each profile setting.

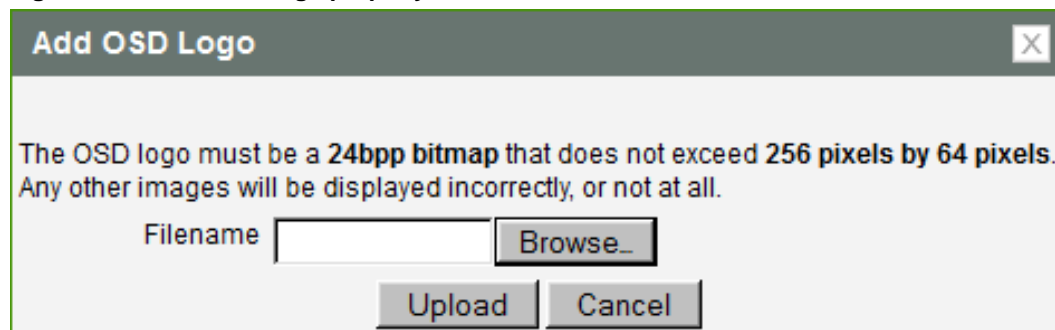
Figure 4-22: Bandwidth Configuration Settings Dialog Box



4.4.5.1 OSD Logo in a profile

An OSD logo may be uploaded into a profile to be applied to all devices in a group. Choose *Profile OSD Logo->Set OSD Logo* and have an image file prepared that is a **24bpp bitmap** that does not exceed **256 pixels by 64 pixels**. Use the *Browse* button to locate your image file and the *Upload* button to import the file to the MC. Figure 4-23 shows the *Add OSD Logo* dialog.

Figure 4-23: Add OSD Logo property



4.4.5.2 Firmware in a profile

A firmware file can be assigned in a profile along with upgrade criteria that must be met before the firmware is pushed to each device.

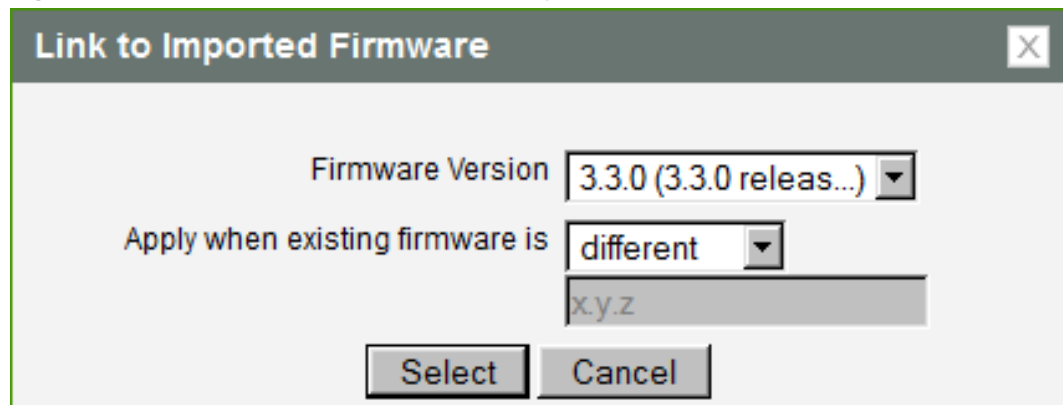
To associate firmware with a profile choose *Profile Firmware->Set Firmware* in the profile properties. Choose the *firmware version* from the existing firmware versions in the select box. The firmware file must have been previously imported into the MC (see section 4.6.1). Figure 4-24 shows the *Link to Imported Firmware* dialog.

Choose the *firmware replacement criteria* from these options:

- Different: Firmware will be overwritten on the device if its version is different from the firmware version listed in the select box.

- Less than: Firmware will be overwritten on the device if its version is less than the x.y.z firmware version you enter in the following text entry field.

Figure 4-24: Link to Imported Firmware property

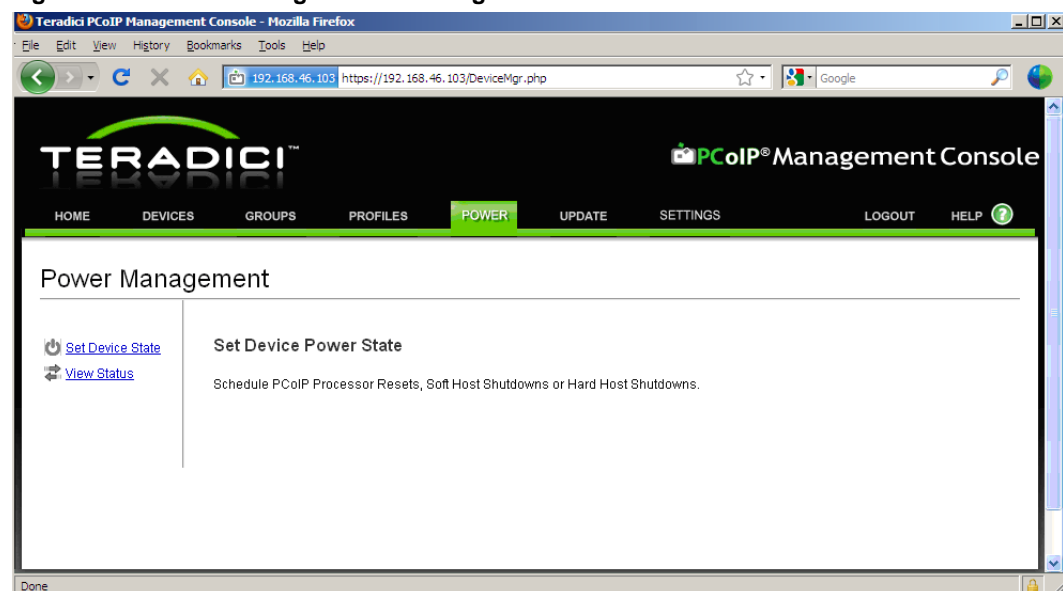


4.5 Power Management

The *Power Management* web page, shown in Figure 4-25, supports the following actions:

- Send reset commands to PCoIP Host and Zero Client devices
- Send power off commands (hard-S5 and soft-S5) to host PCs/Workstations
- Schedule reset and power off commands to be sent in the future
- Displays the current power state of host PCs/Workstations
- Displays status information on the last or next scheduled reset and power off commands for each PCoIP device

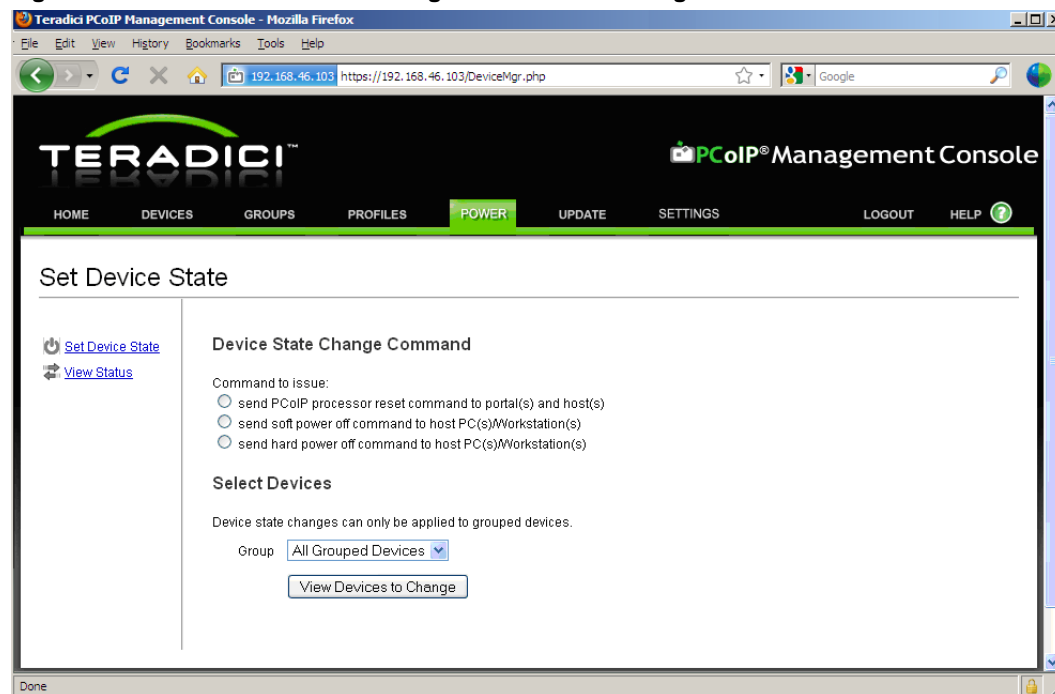
Figure 4-25: Power Management Web Page



4.5.1 Sending Reset and Power off Commands

The *Set Device State* link on the Power Management web page allows administrators to schedule reset and power off commands to be sent to PCoIP devices. When this link is selected the web page shown in Figure 4-26 appears.

Figure 4-26: Send Device State Change Command Web Page



Reset commands can be sent to both Host and Zero Client devices, while power off commands can only be sent to Host devices.

Reset Commands

- A PCoIP Zero Client will reset immediately when it receives a reset command.
- A PCoIP Host device will schedule a deferred reset when it receives a reset command. A deferred reset is a reset that occurs the next time the host PC/Workstation is powered-off or restarted.

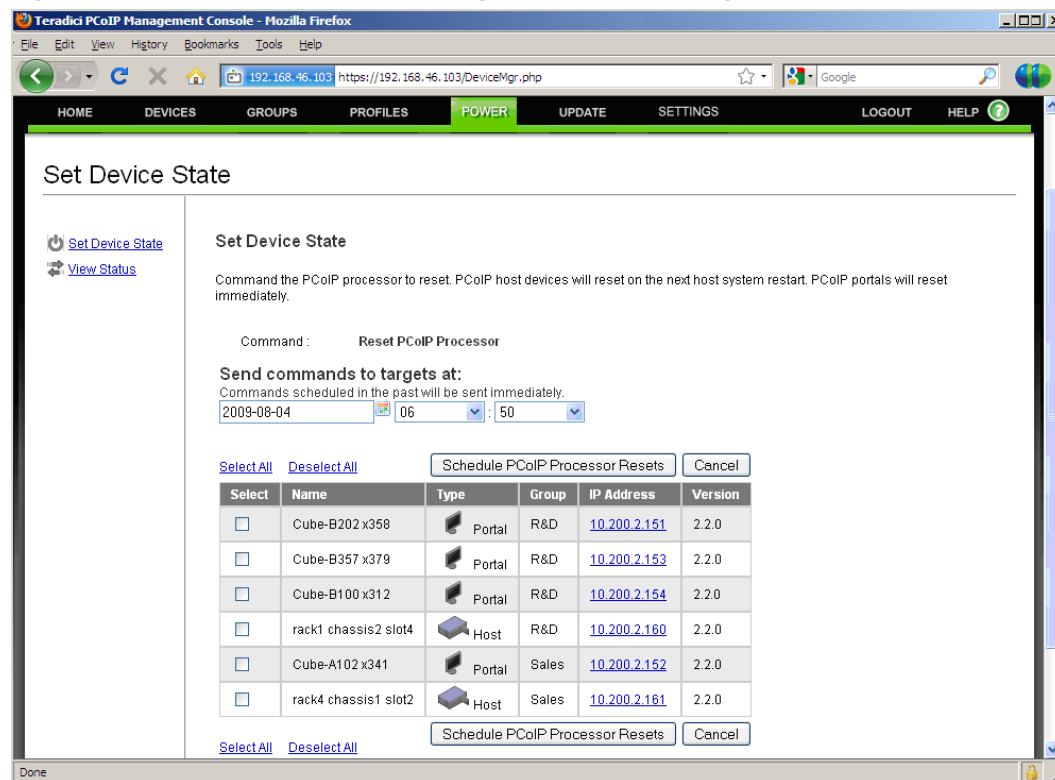
Power off Commands

- Soft power off commands sent to Host PCoIP devices trigger the same action that occurs when the user presses the host PC/Workstation power button for less than 4 seconds. The action taken by the host is dependent on how the operating system is configured. It may initiate a software controlled shutdown or cause the host to enter the Standby state.
- Hard power off commands sent to Host PCoIP devices trigger the same action that occurs when the user presses the host PC/Workstation power button for more than 4 seconds. This immediately shuts down the PC/Workstation by turning off power.

Note: Host workstation must be configured to support power state transitions initiated by the PCoIP Host card. Some systems do not support this feature or it may be optional. Refer to your PCoIP system supplier documentation to determine if this feature is supported.

To send a reset or power off command to a device the administrator must select the command type by selecting one of the radio buttons shown in Figure 4-26. After doing this the administrator can filter the devices the command may be sent to using the *Groups* dropdown menu. When the *View Devices to Change* button is selected a new web page appears. Figure 4-27 shows the web page that supports sending the PCoIP Processor Reset command.

Figure 4-27: Schedule Device State Change Command Web Page



The administrator can choose to send the commands immediately or in the future by specifying the date and time the command will be sent. The command will be sent immediately if the specified date/time is less than or equal to the current time.

The administrator must choose which devices the command will be sent to by selecting the checkbox next to each target.

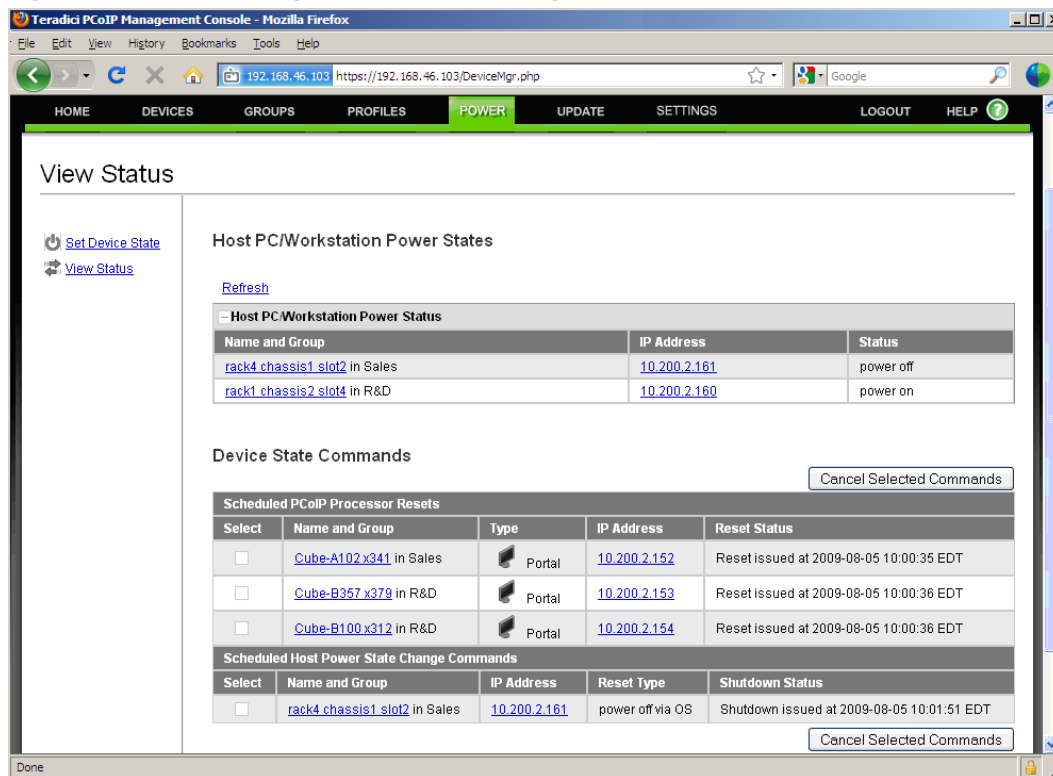
To schedule the command(s) the administrator must click the *Schedule PCoIP Processor Resets* button after configuring the date/time and selecting the devices to send the command to.

After scheduling the command(s) the administrator can view the status of the command(s) by selecting the *View Status* link on the left side of the screen. The following section describes the Power Management Status web page.

4.5.2 Power Management Status

The *View Status* link on the Power Management web page allows administrators to view status information on commands sent to and pending commands that have not yet been sent to PCoIP devices. It also displays the current power state of host PCs/Workstations. When this link is selected the web page shown in Figure 4-28 will appear.

Figure 4-28: Power Management Status Web Page



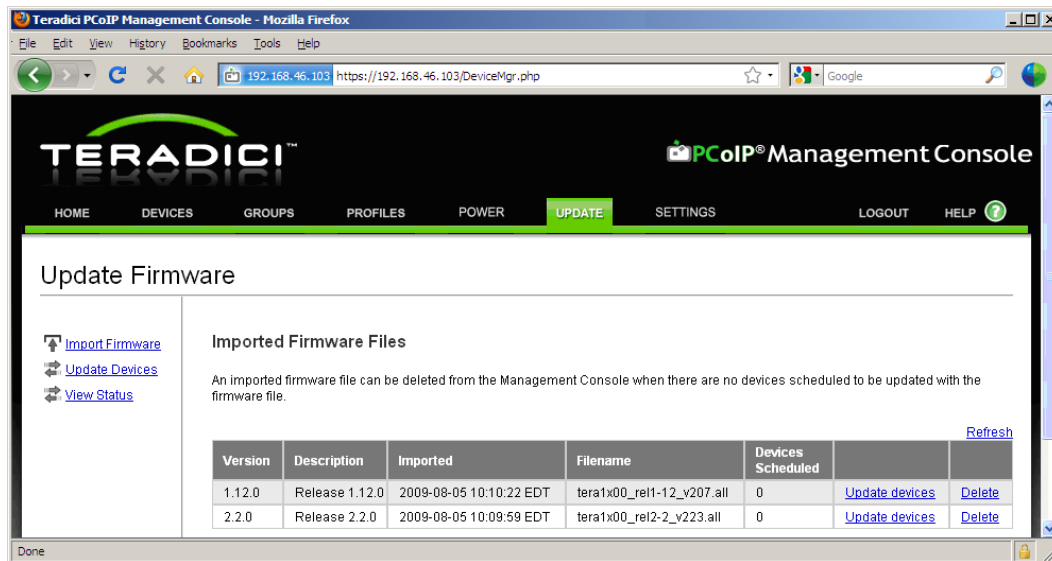
In addition to providing status information this web page can also be used to cancel commands that are scheduled to be sent in the future.

4.6 Update Firmware

The *Update Firmware* web page, shown in Figure 4-29, allows administrators to update the firmware running on PCoIP devices. Administrators can initiate the following actions using this web page.

- Upload new firmware images to the MC VM
- Schedule firmware updates for one or more PCoIP devices
- View the status of scheduled firmware updates

Figure 4-29: Update Firmware Web Page



4.6.1 Import Firmware

The *Import Firmware* link allows an administrator to transfer a firmware release file from the host machine to the MC VM. The administrator is prompted to locate the file containing the firmware release on the host machine file system and assign a description to the firmware release.

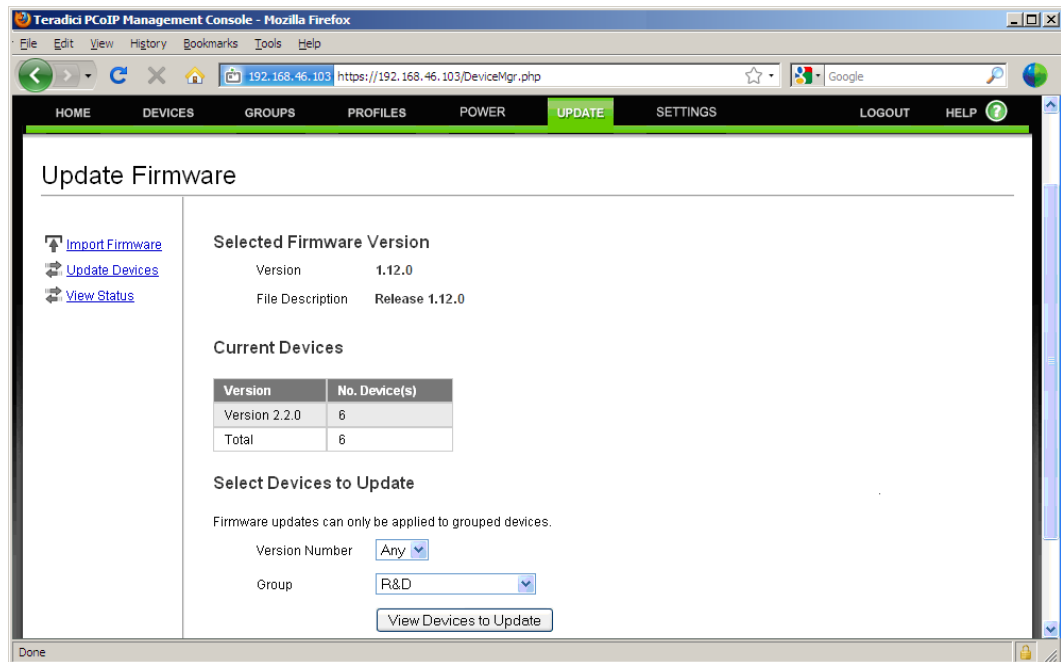
The MC supports storing a maximum of 10 firmware images. Old firmware release should be deleted if this limit is reached and the administrator needs to import additional firmware releases.

4.6.2 Update Device Firmware

The *Update Devices* link next to an imported firmware release allows an administrator to specify the devices to update and the time the update will take place. This allows users to schedule firmware updates to take place at night. Figure 4-30 shows the update devices web page that appears after selecting the *Update Devices* link.

This page displays the firmware version to download, shown under the *Selected Firmware Version* text. This page displays a table with summary information about the firmware versions running on the *Current Devices* managed by the MC. The *Version Number* and *Group Name* dropdown menus allow the administrator to update specific groups of devices and/or devices loaded with specific versions of firmware.

Figure 4-30: Initial Update Devices Web Page



When the *View Devices to Update* button is selected the MC displays the second update devices web page that lists the devices that match the *Version Number* and *Group Name* specified by the user. This new page is shown in Figure 4-31.

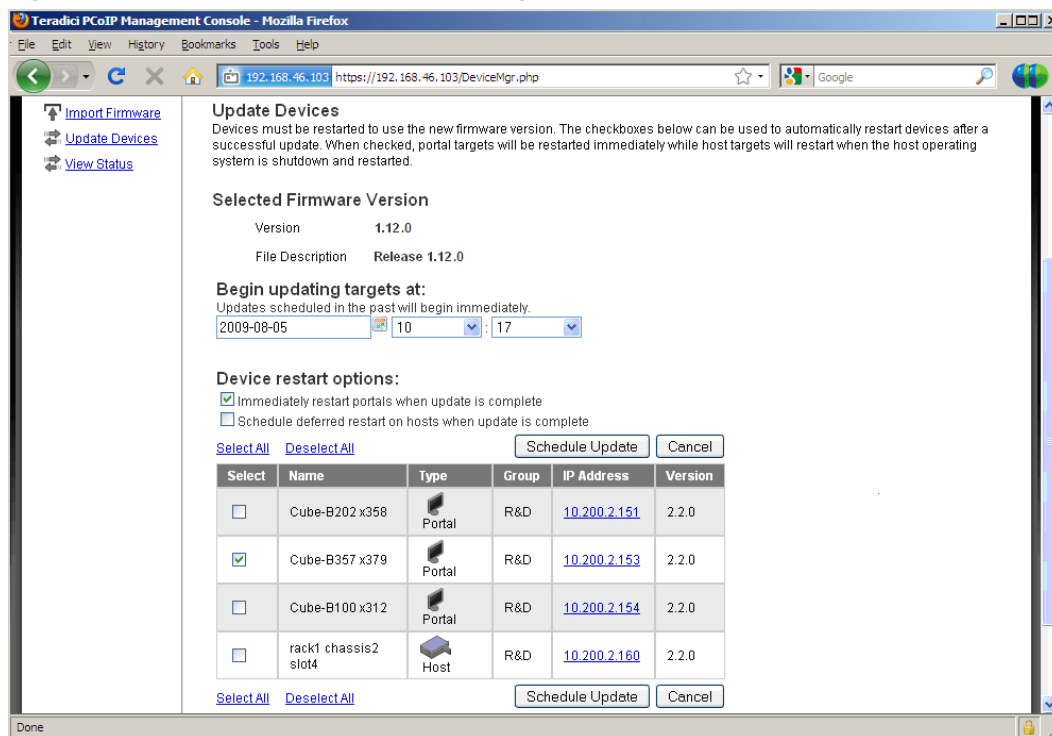
This web page allows the user to specify the time the update will occur with the fields under the *Begin updating targets at* text.

Users can specify the reset options they wish to use.

- Zero Client devices can be commanded to reset when the firmware update completes
- Host devices can be commanded to schedule a deferred reset, which will trigger a reset the next time the host operating systems shuts down

Users must also specify the devices to update by checking the boxes next to the devices they wish to update. After the options have been configured the user should select the *Schedule Update* link to initiate the firmware update.

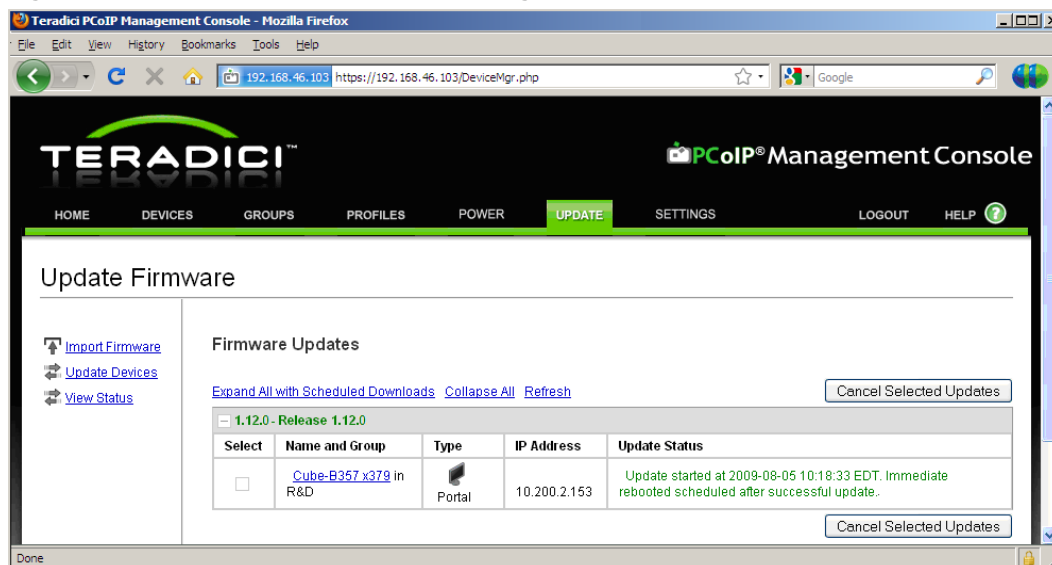
Figure 4-31: Second Update Devices Web Page



4.6.3 View Status

The *View Status* link allows the user to view the current status of all scheduled and completed firmware updates. Figure 4-32 shows the Firmware Update Status web page.

Figure 4-32: Firmware Update Status Web Page

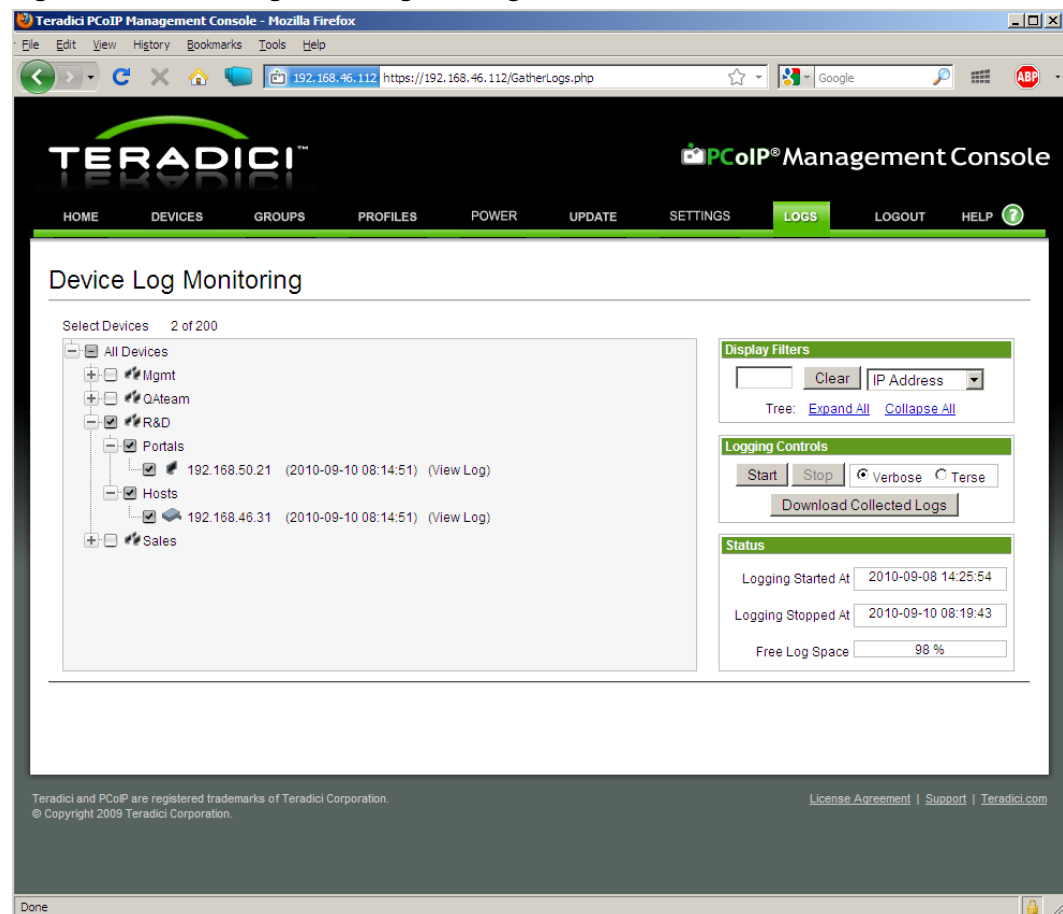


4.7 Device Log Monitoring

The *Device Log Monitoring* web page, shown in Figure 4-33, allows administrators to collect logs over time from a selection of PCoIP devices. Administrators can initiate the following actions using this web page.

- Choose devices to be monitored
- Start and stop log monitoring of the chosen devices
- Download a .tar.gz archive of collected logs
- View status of log monitoring
- View individual device log

Figure 4-33: Device Log Monitoring Web Page



4.7.1 Device Tree

The device tree displays all grouped devices and is used to select which devices will be monitored. Using the checkboxes individual devices, all Zero Clients or hosts within a group, an entire group or all grouped devices can be selected for monitoring. Once log monitoring is started the selection cannot be changed until it is stopped. The same display filters that appear in the Devices page are included here.

Up to 200 devices can be enabled for log monitoring at a time.

4.7.2 Logging Controls

Once a selection of devices has been made using the device tree, the event log filter mode may be set to verbose or terse. This setting will override profile settings and settings made directly on the device. If the device is set to a different event log filter mode during log monitoring, it will be overwritten to the setting made here the next time logs are retrieved by the log monitoring process.

To begin monitoring logs press the *Start* button. This button empties the Management Console's storage of any previously collected logs and starts the log monitoring process. The selection of devices being monitored and the event log filter mode cannot be changed until log monitoring is stopped. An attempt to collect logs will be made every 300 seconds.

The *Download Collected Logs* button may be pressed to format the logs collected into individual .txt files per device, archived into .tar.gz format, and presented as a downloadable file.

When log monitoring is no longer needed, press *Stop* to end the log monitoring service and enable the device tree and event log filter mode controls. The logs collected from the last time the Start button was pressed will remain available for download until the Start button is pressed again.

4.7.3 Status

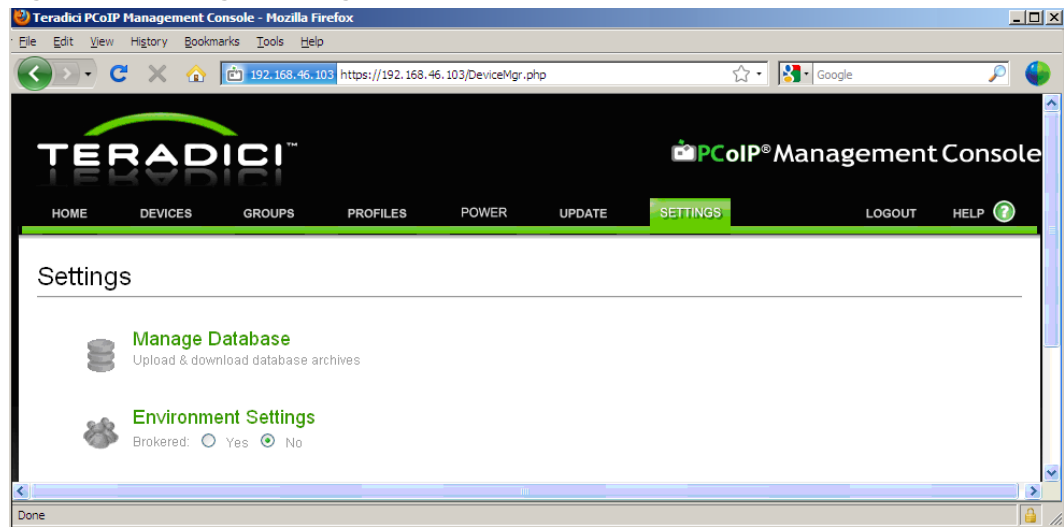
Localized date/time stamps are displayed for when log monitoring was started and stopped. Log monitoring in the Management Console has a finite storage limit which is displayed as Free Log Space. This amount is shown as a percentage where 100% is empty and 0% is full. When Free Log Space becomes full the oldest log data will be overwritten with new log data; therefore, this is a display which should be checked periodically.

4.8 Manage Settings

The *Settings* web page, shown in Figure 4-34, supports the following actions:

- Uploading and downloading MC database archive files
- Configuring MC environment settings

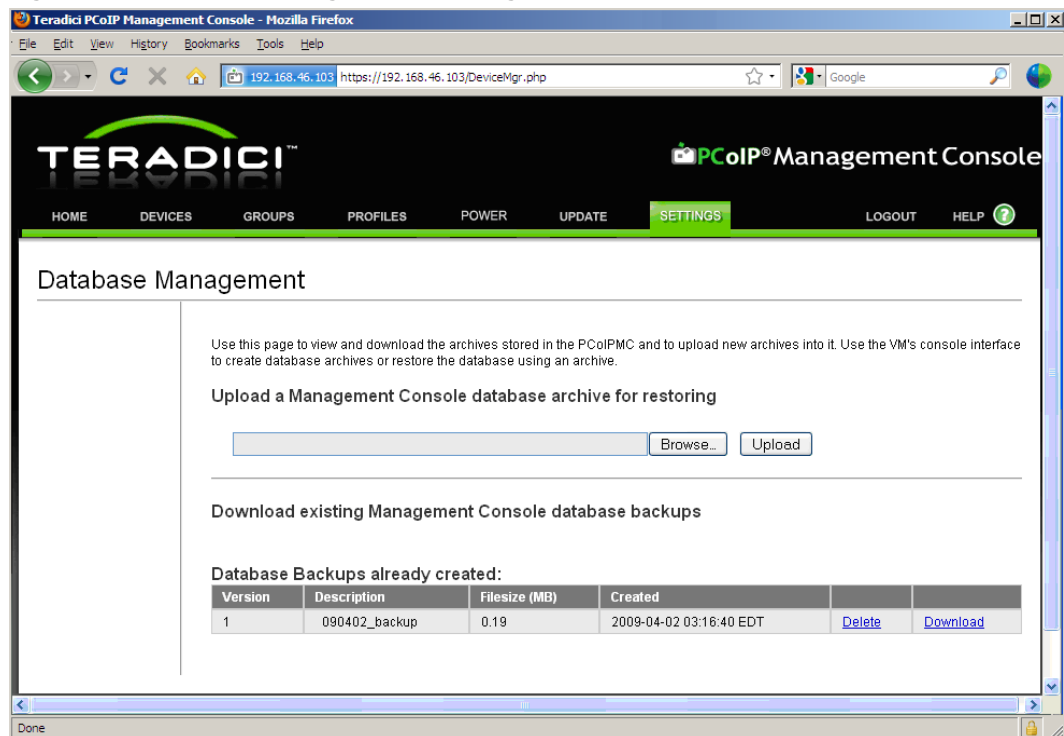
Figure 4-34: Settings Web Page



4.8.1 Database Management

The *Manage Database* link on the Settings web page allows administrators to upload and download database files from the MC VM. When this link is selected the web page shown in Figure 4-35 appears.

Figure 4-35: Database Management Web Page



Uploading a Database

The *Browse* and *Upload* buttons allow an administrator to transfer a database archive from the host PC running the web browser to the MC VM. Select the *Browse* button and

choose database archive to upload. Click the *Upload* button after selecting the file. This will initiate the transfer of the database file into the VM.

After a database is uploaded to the VM the user must restore the database from the imported file to begin using it. This process is performed using the MC VM console. Refer to section 3.5.2 for information on how to restore the MC database.

Downloading a Database

The *Download link* allows an administrator to transfer a database archive from the MC VM to the host PC running the web browser. When this link is selected the user must select the destination directory to download the archive to.

Database archives can be created using the MC VM console backup database command. Refer to section 3.5.1 for information on backing up the MC database.

4.8.2 Environment Settings

The *Brokered* configuration setting shown in Figure 4-34 should be set equal to *Yes* if the deployment is using a connection broker to manage Host and Zero Client peerings. The setting should be *No* if the deployment will use the MC to manage the Host and Zero Client peerings

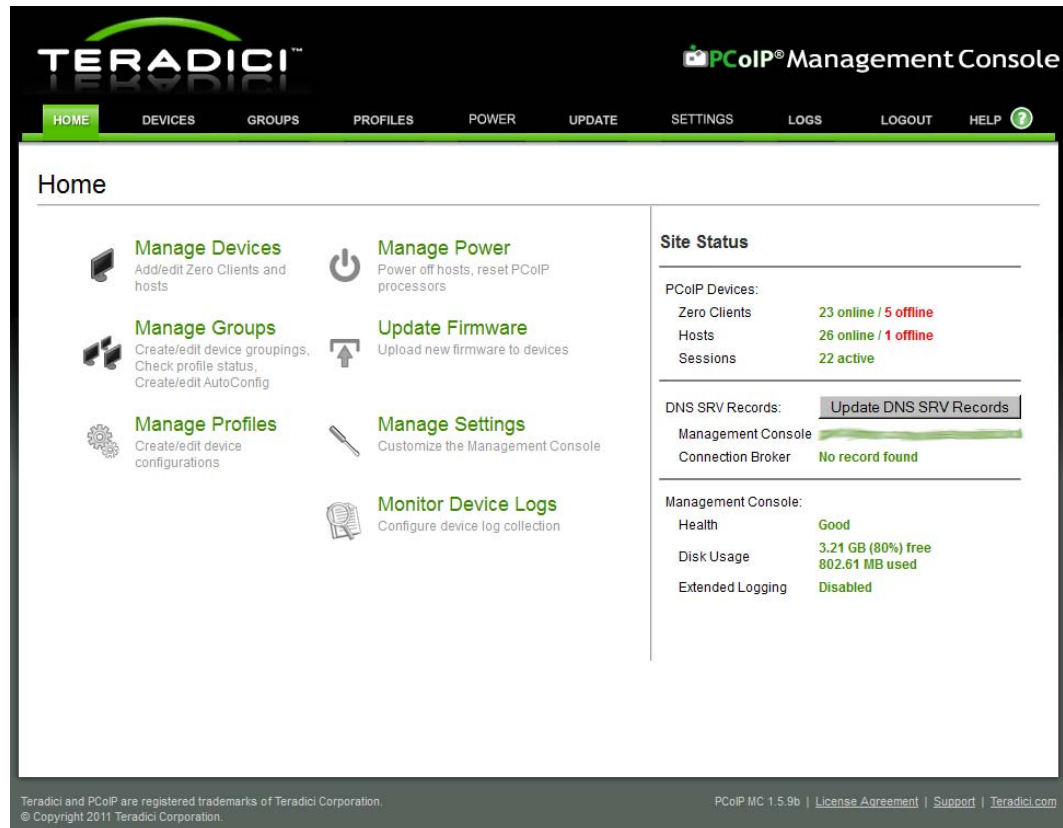
Note: The *Link devices* button on the Device Management page is disabled when this setting is *Yes*. This prevents the MC from manipulating device peering information. In a brokered environment the device peering information is maintained by the connection broker.

Note: When the *Brokered* setting is changed from *No* to *Yes* the MC deletes all peering information from its database. If the administrator later changes the setting to *No* the Host and Zero Clients must be linked again. Administrators that want to re-enable the old peerings should backup the database prior to changing the setting to *Yes*.

4.9 Site Status

The right side of the Home web page displays summary information on all of the PCoIP devices discovered by the MC.

Figure 4-36: Home Web Page



The following status information is displayed:

- Number of online and offline PCoIP Zero Clients discovered by the MC
- Number of online and offline PCoIP Hosts discovered by the MC
- Number of active PCoIP sessions
- FQDN of the MC found in the MC DNS SRV record if one exists
- FQDN of the Connection Broker found in the PCoIP Connection Broker DNS SRV record if one exists
- Current state of the MC
- Disk Usage information for the MC. The MC uses up to 4GB of disk space. When the usage begins to approach this limit the status will turn red indicating the administrator must clean up the MC database. Options to reduce memory usage include limiting the number of firmware images stored in the database along with the number of database backups stored in the VM.

Note: A device is considered offline when the last attempt to rediscover the device failed. Rediscovery attempts are performed at the following times:

- User clicks *Update* on the device details web page
- Once an hour if the device is online
- Once every 15 minutes if the device is offline
- After a firmware update if the deployment has a MC DNS SRV record. If the record does not exist the device will be rediscovered by one of the other mechanisms listed here.
- After a profile is applied (or the application fails)

Note: The MC considers sessions to be active only when the host PC/Workstation is powered on (in the S0 state) and a session is active between the Host and Zero Client. If the host PC/Workstation is in a low power state (S3, S4 or S5) the session is considered inactive.

Note: Site status information is updated when the administrator reloads the home web page. The DNS SRV records are checked every five minutes by the MC or when the *Update DNS SRV Records* button on the home web page is selected.

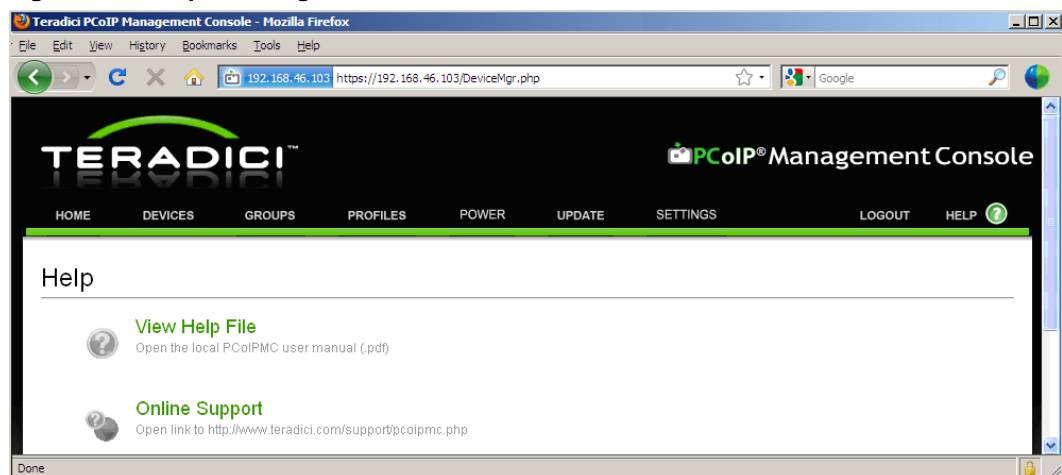
4.10 Online Help

All MC web pages include *HELP* link in the upper right hand corner. When this link is selected the screen shown in Figure 4-37 appears. This web page has two links which provide access to the following information:

- *View Help File* opens a copy of this document
- *Online Support* opens a new browser window at the Teradici MC support website. The URL for this site is <http://www.teradici.com/support/pcoipmc.php>.

Note: The online support link can also be accessed by selecting the *Support* link at the bottom of any of the MC web pages.

Figure 4-37: Help Web Page



5 Getting Started

This section provides instructions on how to begin using the MC. After completing the following steps an administrator will be able to establish a PCoIP session using a pair of PCoIP Host and Zero Client devices.

5.1 Start the Management Console

Follow the instructions described in sections 2.2 and 2.5. After doing this the MC VM will be active on the MC Host machine.

Follow the instructions described in section 4.1 to open a web-browser and log into the MC web interface.

5.2 Discover Devices

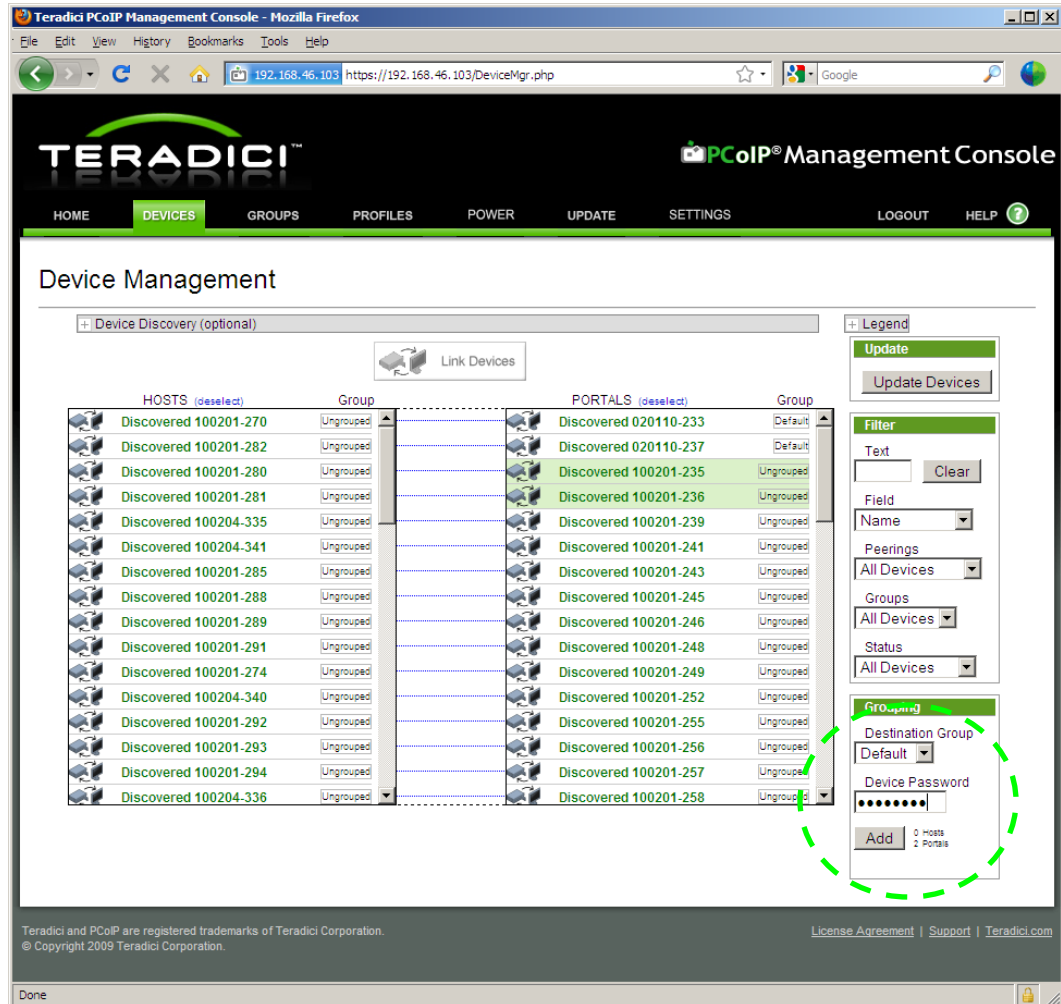
Open the MC Device Management web page. Verify the MC has discovered the devices you wish to link (peer). If the devices have not been discovered use the Manual Device Discovery feature to discover the devices. The Manual Device Discovery feature is described in section 1.3.3.3.

5.3 Adding Devices to a Group

Once the PCoIP devices are discovered the administrator must add them to a group. This is done using the Device Management web page, see Figure 5-1. The steps below walk the user through the process of adding 2 Zero Clients to the *Default* group.

1. Open the MC Device Management web page.
2. While pressing the “Shift” key click on the devices you wish to add to a group. All of the selected devices will be highlighted.
3. After selecting the devices open the *Destination Group* dropdown menu on the right-hand side of the screen. Select the group you wish to add the devices to. In this case the *Default* group was selected.
4. Enter the device password in the Password field on the right-hand side of the screen. In this example all of the devices have been assigned the same password. Users are recommended to assign the same password to all devices in a deployment.
5. Select the *Add* button below the Destination Group dropdown menu. The MC will then add the selected devices to the *R&D* group.

Figure 5-1: Adding Devices to a Group



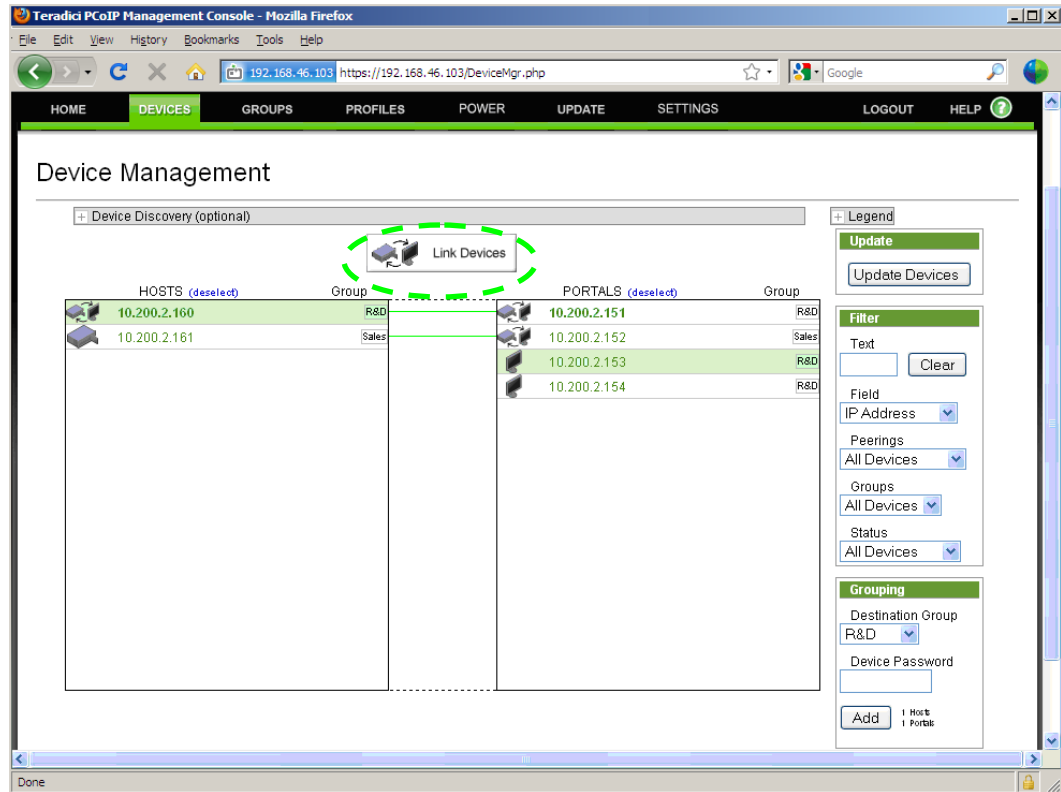
Note: After a device is successfully added to a group the group name appears in the Group column for each device. In Figure 5-1 the first Zero Client device is part of the *Default* group and the third Zero Client device is not part of a group.

5.4 Peering Devices

Each pair of Host and Zero Client devices can be peered, which means they are linked together. After a Host and Zero Client have been peered, a PCoIP session can be started from the Zero Client. To start a PCoIP session the user must select the connect button on the Zero Client OSD. This section describes how to link/peer pairs of Host and Zero Client devices.

1. Open the MC Device Management web page.
2. Select the Host and Zero Client devices to be peered. In Figure 5-2 the devices 10.2.200.160 and 10.200.2.153 are selected.
3. Select the *Link Devices* button. The devices will be peered after doing this. At this point the Zero Client will connect to the Host 10.200.2.160 when the user selects *connect* on the Zero Client OSD.

Figure 5-2: Peering a Pair of Devices



5.5 Next Steps

Below is a list of suggestions for the administrator to follow in order to become more familiar with the MC.

- Review section 1 of this document to become familiar with the different components in a PCoIP deployment. This section also describes some fundamental concepts the administrator must be aware of to use the MC.
- Update the time zone of the MC using the VM Console interface. Refer to section 3.6.
- Create a profile and set one or more properties within the profile. A relatively benign parameter that could be configured is the *OSD Screensaver Text* field in the OSD Configuration settings. Refer to section 4.4.
- Create a Group and assign the profile created in the previous step to the new group. Refer to section 4.3.
- Assign some devices to the new group. Refer to section 4.2.5.
- Write the profile settings to the devices in the new group and verify the settings were written to the devices. Refer to sections 4.3.1.5 and 4.3.2.
- Create an AutoConfig rule matching the criteria of an undiscovered Zero Client. Choose a group for this AutoConfig rule that uses a profile with a relatively benign parameter. Refer to sections 4.3.3 and 4.3.4.
- Query and view the current device settings. Refer to section 4.2.9.2.
- Query and view the data stored in the device event log. Sections 4.2.8.4 and 4.2.9.6 describe two different ways of doing this.

- Download new firmware to a device. Refer to section 4.6
- Send reset commands to a device and view power management status information. Refer to section 4.5.
- Backup the MC database and download it from the MC VM to an external server. Refer to sections 3.5.1 and 4.8.1.
- Upload a backed up copy of the MC database to the MC VM and restore the active database from the uploaded file. Refer to sections 3.5.2 and 4.8.1.