PCoIP® Management Console User Manual

TER0812002

Issue 10

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.

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. Visit http://www.teradici.com/teradici/pat.php for more information.

Revision History

Version	Date	Description
10	May 24, 2013	Updated for release 1.9 of the Management Console • Upgraded the MC VM's guest operating system to Ubuntu Server 12.04.2 LTS • Added support for Firmware Release 4.1
9	August 13, 2012	Updated for release 1.8 of the Management Console • Added support for Firmware Release 4.0.0 • Added support for Firmware Release 4.0.1 • Added support for Tera2 devices • Added DHCP Option Matching in AutoConfig • Added Persistent AutoConfig • Added Display Topology Configuration to profiles • Enhanced Login process
8	January 20, 2012	Updated for release 1.7.1 of the Management Console • Added support for Firmware Release 3.5.1
7	December 02, 2011	Updated for release 1.7 of the Management Console • Added support for Firmware Release 3.5 • Added Certificates to profiles • Added Session Connection Type
6	October 01, 2011	Updated for release 1.6 of the Management Console • Added Remote Power Down • Added Import and Export to profiles • Added Retry and Apply AutoConfig • Added Manage Device Naming • Added Delete button to Device Management
5	June 01, 2011	Updated for release 1.5 of the Management Console • 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
4	September 17, 2010	Updated for release 1.3.30 of the Management Console • Added Device Log Monitoring • Added support for Firmware Release 3.2
3	March 01, 2010	Updated for release 1.2 of the Management Console • Replaced PCoIPMC with MC • Added support for Internet Explorer
2	August 31, 2009	Updated for release 1.1 of the Management Console

		• Updated Management Console Limitations (see Section 1.2) • Added Migrating to a New Version of the Management Console (see Section 2.6)
1	April 3, 2009	Initial release

Contents

Table of Figures

Tables

Definitions

CA	Certificate Authorities
CMI	Connection Management Interface – interface provided by the client or host, used to communicate with an external connection management server
CMS	Connection Management Server – an external management entity (third party) that manages and controls the client/host through the CMI interface
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 PC-over-IP system
PCoIP zero client	Desktop or client side of PC-over-IP system
SLP	Service Location Protocol
SSL	Secure Socket Layer (security protocol)
TERA1100	Teradici 1st generation PCoIP zero client processor
TERA1200	Teradici 1st generation PCoIP host processor
TERA2140	Teradici 2nd generation PCoIP zero client processor
TERA2240	Teradici 2nd generation PCoIP host processor
TERA2321	Teradici 2nd generation PCoIP zero client processor
VM	Virtual Machine

Introduction

The management console for PCoIP® protocol devices (MC) lets you centrally manage a PCoIP deployment. The MC is packaged as a VMware virtual machine (VM) and runs on VMware Player, VMware Workstation and VMware ESX server. A web browser is used to access and control the MC.

The MC lets you:

- Access and update the configuration of your PCoIP devices
- Apply the same configuration data to groups of devices
- Update device firmware
- Reset devices
- Control the power state of host devices
- Remotely power down zero clients
- 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, IP address and DHCP option values

About this Document

This document describes how to install and set up the management console. It also describes the features of the tool. For more details about the individual PCoIP device configuration fields, see the *PCoIP Zero Client and Host Administrator Guide* (TER1206003).

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 for managing your PCoIP devices.
- Section 5 describes how to use the MC to perform some basic tasks, such as starting the MC, logging into the web interface, discovering some devices, and linking a pair of host and zero client devices. It also includes recommendations for familiarizing yourself with the major capabilities of the MC.

Note: If you haven’t used the MC before, and want to begin using the tool right away, review Section 5. The information in this section gets you to a point where you can establish a PCoIP session between the linked host and zero client devices, as well as a PCoIP session in VMware View environment.

1 Overview

This section describes the components found in a typical PCoIP 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). It shows the MC used for peering and configuration. The figure does not show a connection broker, which is required when hosts are dynamically assigned to zero clients as users log in.

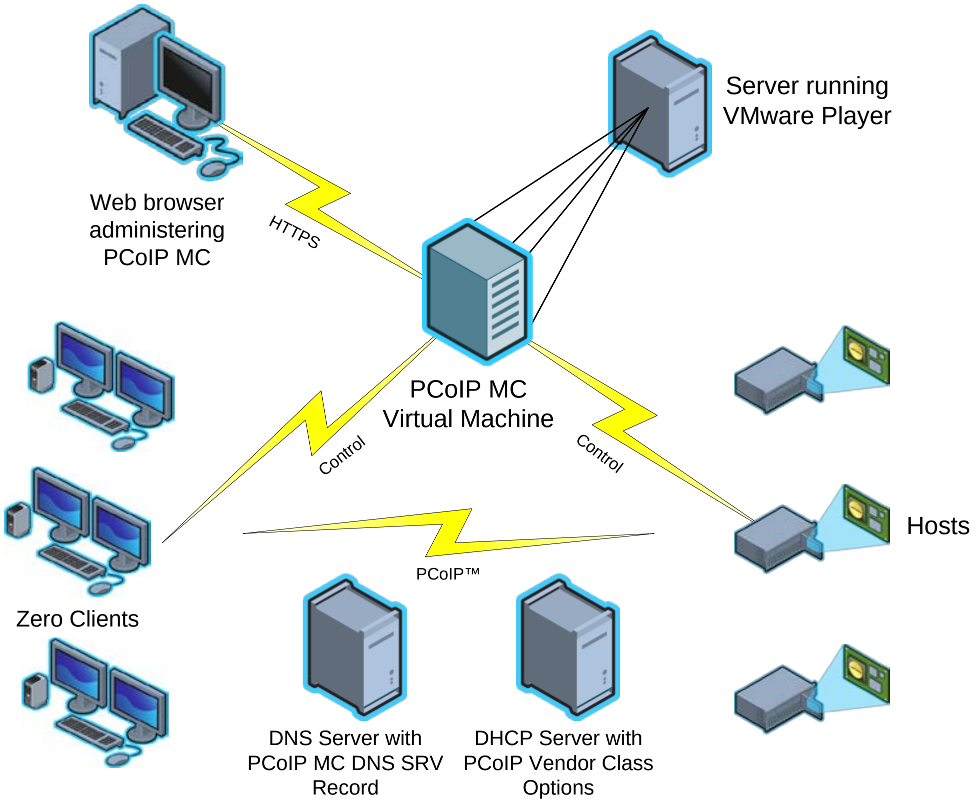


Figure 1-1: PCoIP Deployment Components

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 you can access and control using the following mechanisms:

Device Web Interface

Although you can configure each device individually via a web-based administration interface, you are encouraged to use the MC (especially as the deployment grows). This ensures that all PCoIP devices are configured uniformly and that the MC database accurately reflects the device configuration settings.

For information about the device web interface, see the *PCoIP Zero Client and Host Administrator Guide* (TER1206003).

PCoIP Management Console

The management console for PCoIP protocol devices (MC) lets you centrally manage a PCoIP deployment. It lets you:

- Access and update the configuration of your 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
- Power off zero client devices
- 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, IP address and DHCP option values

The MC is packaged as a VMware virtual machine (VM) and runs on VMware Player. This lets you install and run the MC on any host machine that can run VMware Player. You can also install and run the MC on any VMware ESX server. See section 2.4 for details on installing the MC into your existing VMware ESX server.

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

The MC must be connected to the same network to which the PCoIP devices are connected. This lets the tool communicate with the PCoIP devices.

Connection Broker

A connection broker is an optional component that lets you manage user access to computing resources. Note that 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. Deployments having the following requirement must install a connection broker:

- hosts are dynamically assigned to zero clients based on the login credentials of the person using the zero client

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. You can also install a connection broker DNS SRV record 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 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:

- PCoIP DHCP Vendor Class Options are configured in the DHCP server. See section 1.3.3.2 for details on configuring these options.

- 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 have the **Enable SLP Discovery** configuration setting set to *True*.
- The **PCoIP MC DNS-Based Discovery Prefix** setting for all devices is set to the hostname prefix of the MC. You can only access this setting through the MC. You cannot access it through the device web interface or zero client OSD interface. Section 1.3.3.3 describes how PCoIP devices use the **PCoIP MC DNS-Based Discovery Prefix** setting to contact the MC. It also describes the system requirements to use this option.

If none of the previous conditions are true, include a DNS server in your system and install the MC DNS SRV record. See section 1.3.3.1 for details on installing this record.

1.1.3 DHCP Server

A DHCP server with the PCoIP DHCP Vendor Class options (shown in Figure 1-1) is also an optional component that is highly recommended. Like MC DNS SRV records, DHCP options facilitate automatic device discovery. You can use these options in place of a DNS SRV record.

When a PCoIP device boots, it sends DHCP option 60 containing a PCoIP Vendor ID and requests DHCP option 43, which contains the address of the MC. After receiving the address, the device sends messages to the MC advertising its existence.

The PCoIP DHCP Vendor Class options are not required when one of the following conditions is true:

- The MC DNS SRV record is installed in the DNS server. See section 1.3.3.1 for details on installing this record.
- All PCoIP devices in a deployment are located on the same network subnet as the MC. In this situation, the MC can find the devices using SLP discovery. All devices have the **Enable SLP Discovery** configuration setting set to **True**.
- The **PCoIP MC DNS-Based Discovery Prefix** setting for all devices is set to the hostname prefix of the MC. You can only access this setting through the MC. You cannot access it through the device web interface or zero client OSD. Section 1.3.3.3 describes how PCoIP devices use the **PCoIP MC DNS-Based Discovery Prefix** setting to contact the MC. It also describes the system requirements to use this option.

If none of the previous conditions are true, include a DHCP server in your system and configure the PCoIP DHCP Vendor Class options. See section 1.3.3.2 for details on configuring this record.

Note: DHCP Options discovery is only available on PCoIP devices with firmware version 3.5.0 or higher.

1.2 Management Console Limitations

This section describes some limitations of the MC.

- 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. You must use the device web interface to load and activate new firmware on each device running firmware releases less than or equal to 0.18. See the *PCoIP Zero Client and Host Administrator Guide* (TER1206003) for more details.
- 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 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, include a connection broker in the deployment.
- The MC supports managing up to 2000 PCoIP devices. The tool may be able to support more than 2000 devices, but the current version was tested with a maximum of 2000 devices. Support for more than 2000 devices will be included in a future release of the tool. If your deployment has more than 2000 devices, contact your PCoIP equipment supplier for help on managing more than 2000 devices.

1.3 Management Console Concepts

This section describes some key concepts to note before using the MC.

1.3.1 Groups and Profiles

The MC manages the PCoIP devices using two important concepts (groups and profiles):

- **Profile:** a set of device configuration settings
- **Group:** a set of one or more devices with a single profile

Figure 1-2 shows an example of how 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 example, configuration settings defined in the Development Profile are written to the devices in the R&D and Engineering groups.

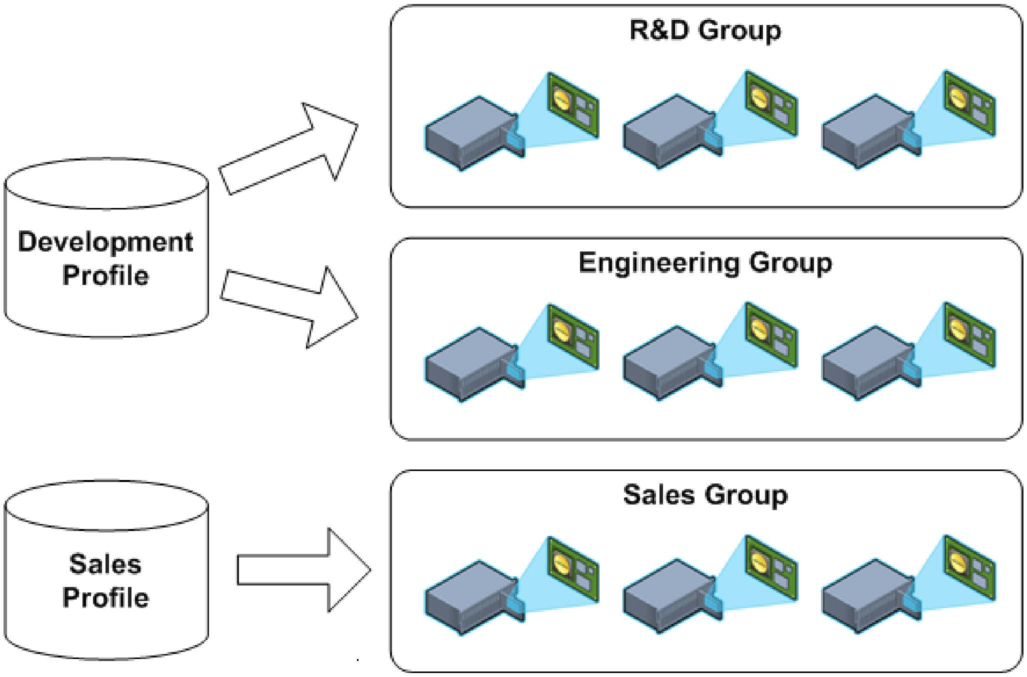


Figure 1-2: Management Console Groups and Profiles

Note some important rules regarding groups and profiles:

- Each group has 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. You can define a profile that contains a subset of the configuration parameters.
- If the firmware on a device is updated when a profile is applied, the profile settings are written to the device after the new firmware is activated.
- Profiles contain settings that let users specify if 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** webpages. Consider resetting your devices in the deployment after updating device configuration settings.
- When devices are added to a group and the group profile has not changed, apply the profile to the newly added devices and not the entire group. This minimizes the number of device resets.

1.3.2 Fixed Seating

The MC lets you 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. To dynamically assign hosts to zero clients when your users log in, you must install a connection broker. The MC does not support dynamically assigning hosts to zero clients.

1.3.3 Device Discovery

The MC must discover PCoIP devices before it can manage them. The MC supports discovering devices in a deployment using one or more discovery mechanisms:

Recommended approaches:

- Install a MC DNS SRV record. When DNS SRV record discovery is used, the PCoIP devices advertise themselves to the MC. Devices that use the DNS server can 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.

Note: Do not install a DNS SRV record if:

- Your network does not have a DNS server.
- You want to have multiple instances of the MC on your network to manage subsets of your PCoIP devices. If you install a service record, the devices point to only one instance of the MC.

See section 1.3.3.1 for details on installing a DNS SRV record.

- Install PCoIP DHCP Vendor Class. When DHCP Options discovery is used, the PCoIP devices advertise themselves to the MC. Devices that use the DHCP server can find the MC. If DHCP is not enabled, the MC must locate devices using methods that are often subject to limitations, such as being unable to search more than its local subnet.

Note: Do not install DHCP Options if:

- Your network does not have a DHCP server.
- You have PCoIP devices with a firmware version earlier than 3.5.0 in the network. DHCP Options discovery is only available to PCoIP devices with firmware version 3.5.0 or higher.

See section 1.3.3.2 for details on configuring DHCP Vendor Class Options.

If you cannot install a DNS SRV record or DHCP Vendor Class Options:

- You 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.**

Note: You can only access the **PCoIP MC DNS-Based Discovery Prefix** setting using the MC. You cannot access it through the device web interface or zero client OSD interface.

See section 1.3.3.3 for details.

- If you cannot install a DNS SRV record or use the **PCoIP MC DNS-Based Discovery Prefix** configuration setting, 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.
- If a deployment cannot support any of the previous device discovery options, you can use the MC to configure devices. The MC supports a manual discovery feature that lets the MC find devices.

Note: If you use this approach, note that if a device has DHCP enabled, the MC loses contact with a device if its IP address changes. Should this occur, you must perform another manual discovery search to find devices that were assigned new IP addresses.

See section 1.3.3.4 for more details.

1.3.3.1 Installing a DNS Service Record on the DNS Server

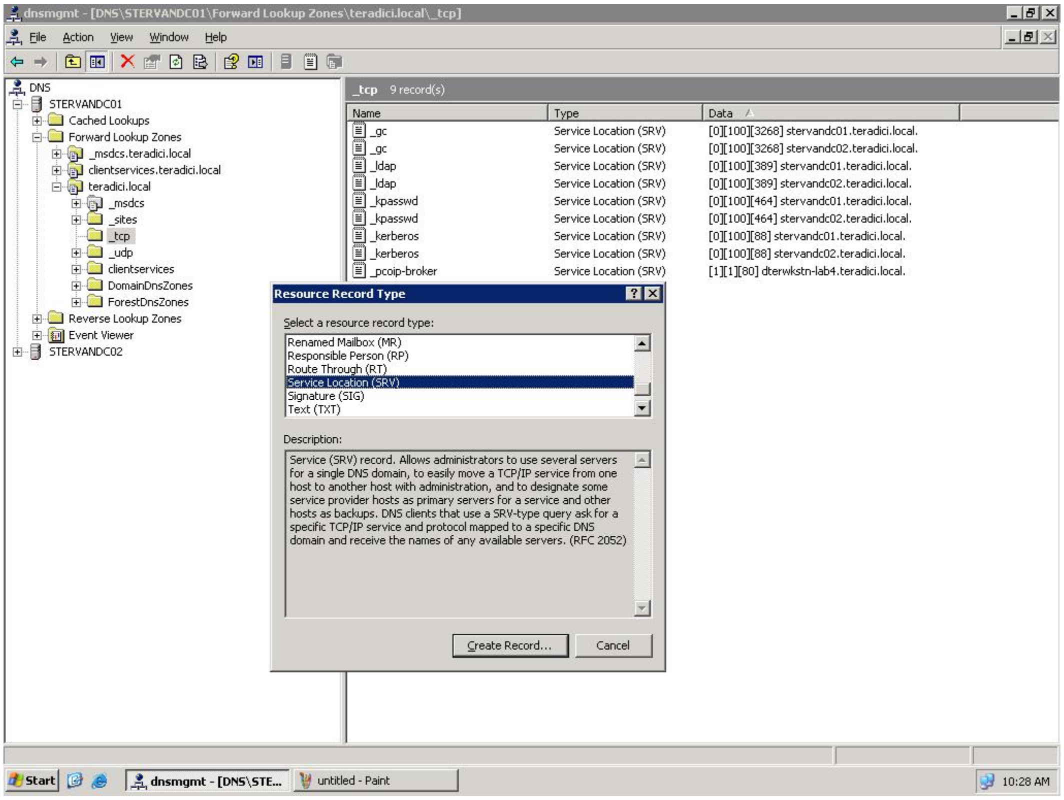
Before you can install the DNS service record:

- The deployment must have a DNS server in the network
- Two DNS records must be installed on the DNS server
    1. An A record (name record) for the MC
    2. A SRV record (service record) created

Note: The following steps are an example of how to install a DNS SRV record to a DNS server in Windows Server 2003. If you use a different type of server, modify the steps accordingly.

To add the MC DNS SRV record to DNS server in Windows Server 2003:

1. Enter DNS service configuration on domain controller.
2. Navigate to the **local domain**, and then select the **_tcp entry** folder.



Name	Type	Data
_gc	Service Location (SRV)	[0][100][3268] stervandc01.teradici.local.
_gc	Service Location (SRV)	[0][100][3268] stervandc02.teradici.local.
_ldap	Service Location (SRV)	[0][100][389] stervandc01.teradici.local.
_ldap	Service Location (SRV)	[0][100][389] stervandc02.teradici.local.
_kpasswd	Service Location (SRV)	[0][100][464] stervandc01.teradici.local.
_kpasswd	Service Location (SRV)	[0][100][464] stervandc02.teradici.local.
_kerberos	Service Location (SRV)	[0][100][88] stervandc01.teradici.local.
_kerberos	Service Location (SRV)	[0][100][88] stervandc02.teradici.local.
_pcoip-broker	Service Location (SRV)	[1][1][80] dterwkstn-lab4.teradici.local.

Select a resource record type:

Renamed Mailbox (MR)
Responsible Person (RP)
Route Through (RT)
Service Location (SRV)
Signature (SIG)
Text (TXT)

Description:

Service (SRV) record. Allows administrators to use several servers for a single DNS domain, to easily move a TCP/IP service from one host to another host with administration, and to designate some service provider hosts as primary servers for a service and other hosts as backups. DNS clients that use a SRV-type query ask for a specific TCP/IP service and protocol mapped to a specific DNS domain and receive the names of any available servers. (RFC 2052)

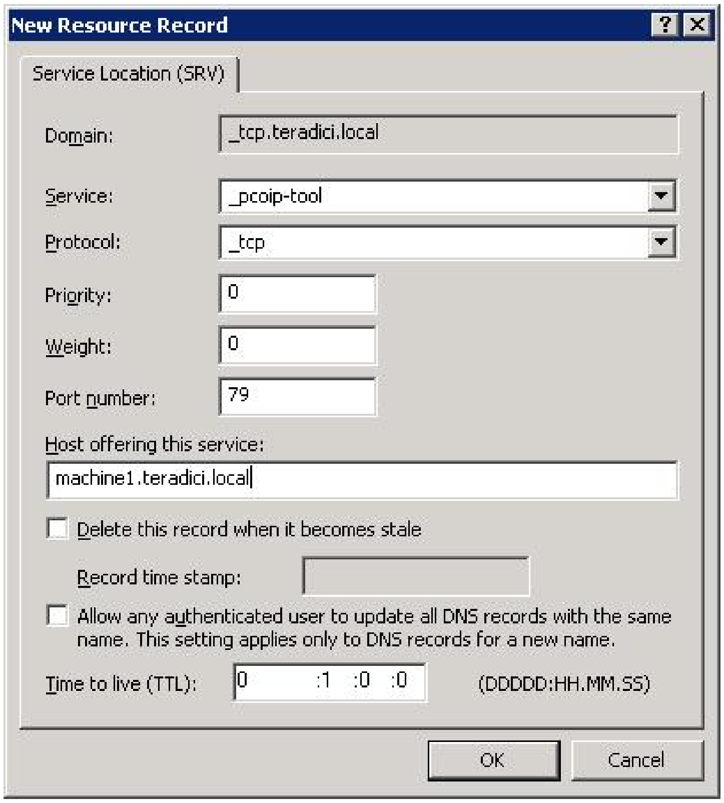
Create Record... Cancel

Figure 1-3: DNS Service Configuration Menu

3. Right-click, and then select **Other New Records …**
4. Select **Service Location (SRV)**.

5. Fill in the entries as shown in Figure 1-4. (Enter the hostname where the MC is installed under the heading **Host offering this service**.)

   Note: The PCoIP devices do not use the **Port Number** setting. You can choose to set it to **50000** to reflect the listening port of the CMI server.



Domain: _tcp.teradici.local

Service: _pcoip-tool

Protocol: _tcp

Priority: 0

Weight: 0

Port number: 79

Host offering this service: machine1.teradici.local

□ 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): 0 :1 :0 :0 (DDDDD:HH.MM.SS)

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

1.3.3.2 Configuring DHCP Vendor Class Options on the DHCP server

Before you can install the DHCP options:

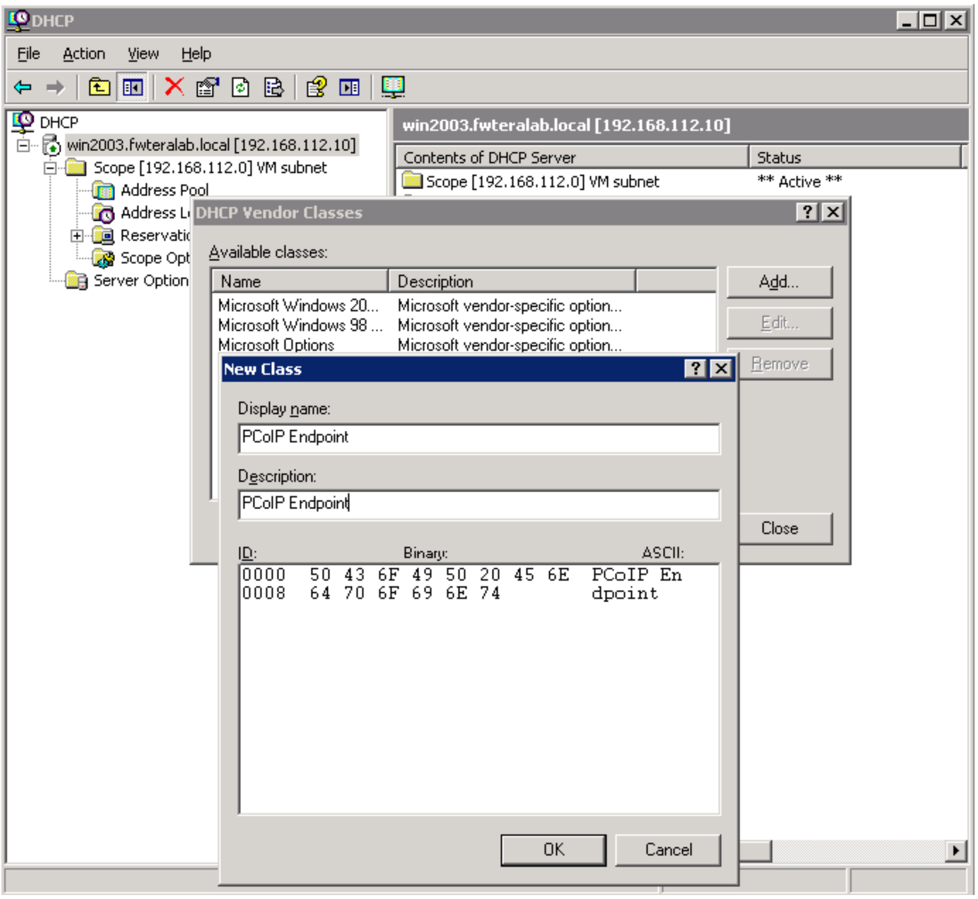
- The deployment must have a DHCP server in the network.
- The PCoIP devices must enable DHCP to send a request and receive the address of the MC in response.
- The DHCP server must support both DHCP Options 60 (Vendor class identifier) and 43 (Vendor specific information). See RFC2132 for details on the DHCP options.

Note: The following steps are an example of how to configure DHCP Vendor Class Options in a DHCP server in Windows Server 2003. If you use a different type of server, modify the steps accordingly.

To add the PCoIP DHCP vender class options to the DHCP server in Windows Server 2003:

1. Enter the DHCP service configuration on the DHCP Server console.
2. Right-click the DHCP server in the tree, and then choose **Define Vendor Classes…**
3. Click **Add** to add a new DHCP Vendor Class.
4. Enter **PCoIP Endpoint** in the **Display name** field.
5. Enter **PCoIP Endpoint** in the **ASCII** column as the Vendor ID.

Note: For Cisco VXC 2111 and VXC 2211 PCoIP devices with firmware version 4.0.0 or higher use **VXC2111** and **VXC2211** respectively as the Vendor ID.



Contents of DHCP Server	Status
Scope [192.168.112.0] VM subnet	** Active **

Available classes:

Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...

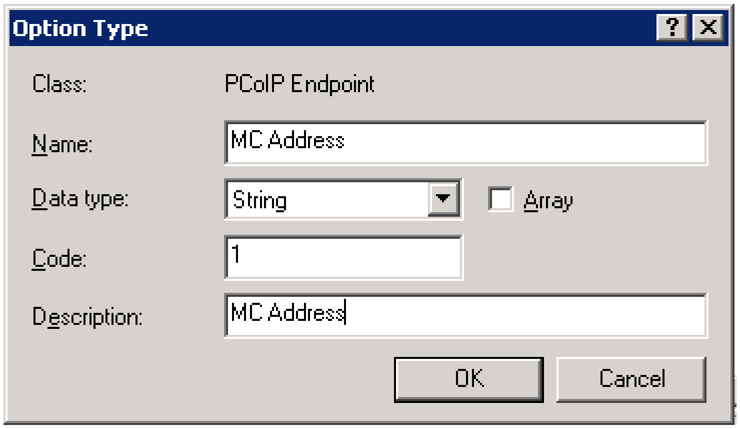
Display name: PCoIP Endpoint

Description: PCoIP Endpoint

```
ID:           Binary:                      ASCII:
0000   50 43 6F 49 50 20 45 6E   PCoIP En
0008   64 70 6F 69 6E 74         dpoint
```

Figure 1-5: Add a new DHCP Vendor Class Configuration

6. Click **OK** to save and close the dialog.
7. Right-click the DHCP server in the tree, and then choose **Set Predefined Options…**
8. Select **PCoIP Endpoint** as the **Option** class, and then click **Add**…
9. Enter the name **MC Address**, data type **String**, code **1**, and description **MC Address**, and then click **OK**.



Class: PCoIP Endpoint

Name: MC Address

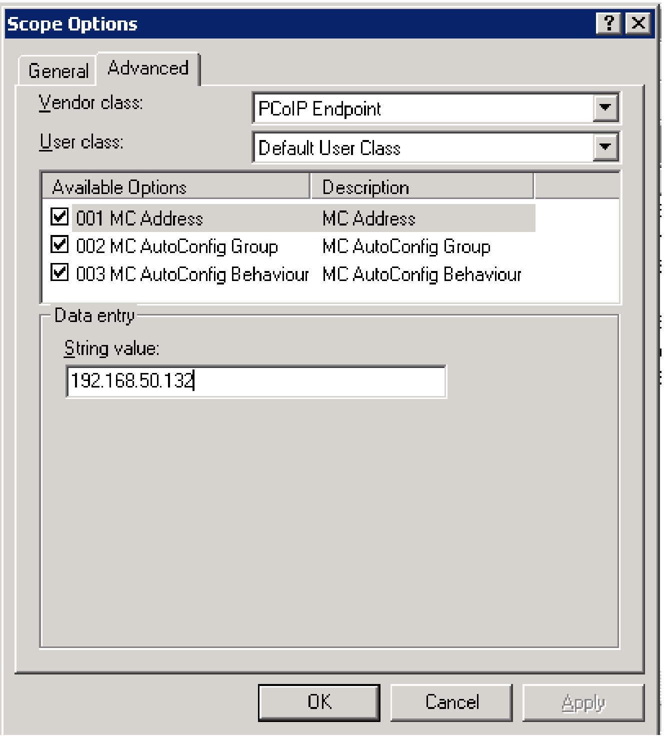
Data type: String ☐ Array

Code: 1

Description: MC Address

Figure 1-6: Add a DHCP Option Type Dialog Box

10. Click **OK** to save and close the dialog.
11. Expand the tree for the DHCP server, and expand the tree for the **Scope** to which you want to add options.
12. Right-click **Scope Options,** and then choose **Configure Options…**
13. Click the **Advanced** tab, and then select the **PCoIP Endpoint** Vendor class.
14. Enable the checkbox for the **MC Address,** and then enter a valid MC IP address in the **Data entry** field.
15. Click **OK** to save.



Vendor class: PCoIP Endpoint

User class: Default User Class

Available Options	Description
☑ 001 MC Address	MC Address
☑ 002 MC AutoConfig Group	MC AutoConfig Group
☑ 003 MC AutoConfig Behaviour	MC AutoConfig Behaviour

Data entry

String value: 192.168.50.132

Figure 1-7: DHCP Scope Options Dialog Box

Optionally, you can add **MC AutoConfig Group** and **MC AutoConfig Behavior** options in the **PCoIP Endpoint** vendor class. Add the options in the **Predefined Options and Values** dialog using the following values.

- **MC AutoConfig Group:** Enter the name **MC AutoConfig Group**, data type **String**, code **2**, and description **MC AutoConfig Group**.
- **MC AutoConfig Behavior:** Enter the name **MC AutoConfig Behavior**, data type **Byte**, code **3**, and description **MC AutoConfig Behavior**.

Then enter the data entry in the **Scope Options** dialog.

1. **MC AutoConfig Group**: String value of a group name
2. **MC AutoConfig Behavior**: Byte value representing one of the following options

   0. AutoConfig: All new devices
      Persistent AutoConfig: Only when device is in **MC AutoConfig Group**
   1. AutoConfig: All new devices
      Persistent AutoConfig: All grouped devices

2. AutoConfig: None
   Persistent AutoConfig: None

MC AutoConfig Behavior option is only used when **MC AutoConfig Group** option is configured. It is recommended to configure both options together.

See section 1.3.4 for details on using the DHCP options for AutoConfig.

1.3.3.3 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 not blank during startup, the device tries 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 (for example, 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 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. See RFC2132 for details on the DHCP options. If the DHCP server only supports DHCP options 12, the hostname string must contain the domain name.
- PCoIP devices managed by a specific MC must have the **PCoIP MC DNS-Based Discovery Prefix** setting equal to the MC's hostname prefix (for example, 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 gets 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 gets the hostname 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 creates many FQDN variations using the results from DHCP options 12 and 15. With each FQDN variation, the hostname prefix remains constant while the domain hierarchy level changes.

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

In detail, the algorithm works as follows:

1. 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.

2. If the transmission times out, the device creates the next FQDN variation by proceeding one level up the domain hierarchy. The last domain name attempted has a single dot in the string.
3. After exhausting the FQDN possibilities (based on the DHCP options 15 string), the device waits for five minutes and then uses hostname variations based on the DHCP options 12 string.
4. After failing to contact a MC using the DHCP options 12 string, the device waits for five minutes and then cycles back to using DHCP options 15.
5. The device repeats this process until a MC is contacted.

Example

In the following example, 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** setting 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.

1.3.3.4 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.

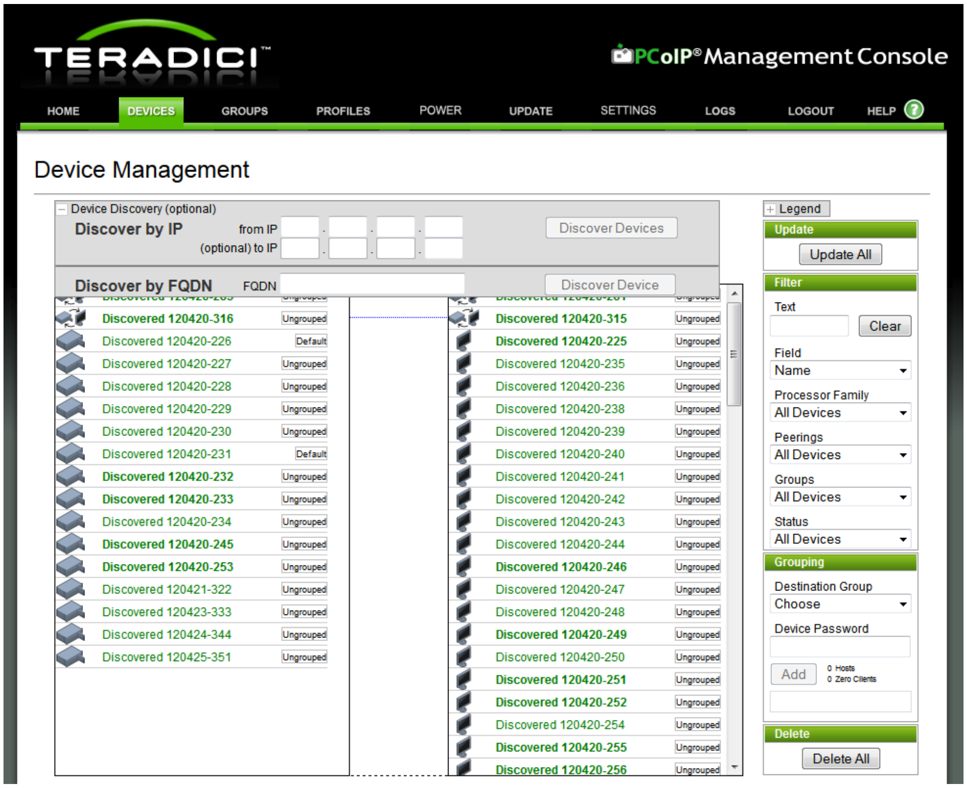
The MC supports manually discovering devices at a specific IP address, in a range of IP addresses or at an FQDN. This option is useful to quickly begin using the MC or when a deployment uses the **PCoIP MC DNS-Based Discovery Prefix** configuration setting described in section 1.3.3.2. In this situation, you 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** webpage 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 then select **Discover Devices**.
- When a device is on a specific subnet but its IP address is not known, you can command the MC to discover the devices in a range of IP addresses using both the **from IP** and (optional) **to IP** fields. After you specify the address range, select **Discover Devices**.

Note that this process can take a few minutes to complete depending on the number of addresses searched. A status bar appears while the tool discovers devices.

- When the FQDN of a device is known and the device is not discovered, enter the FQDN in the **FQDN** field and select **Discover Devices**.



Device Management

Device Discovery (optional)

Discover by IP — from IP . . . ; (optional) to IP . . .

Discover by FQDN — FQDN

Discovered 120420-316	Ungrouped
Discovered 120420-226	Default
Discovered 120420-227	Ungrouped
Discovered 120420-228	Ungrouped
Discovered 120420-229	Ungrouped
Discovered 120420-230	Ungrouped
Discovered 120420-231	Default
Discovered 120420-232	Ungrouped
Discovered 120420-233	Ungrouped
Discovered 120420-234	Ungrouped
Discovered 120420-245	Ungrouped
Discovered 120420-253	Ungrouped
Discovered 120421-322	Ungrouped
Discovered 120423-333	Ungrouped
Discovered 120424-344	Ungrouped
Discovered 120425-351	Ungrouped

Discovered 120420-315	Ungrouped
Discovered 120420-225	Ungrouped
Discovered 120420-235	Ungrouped
Discovered 120420-236	Ungrouped
Discovered 120420-238	Ungrouped
Discovered 120420-239	Ungrouped
Discovered 120420-240	Ungrouped
Discovered 120420-241	Ungrouped
Discovered 120420-242	Ungrouped
Discovered 120420-243	Ungrouped
Discovered 120420-244	Ungrouped
Discovered 120420-246	Ungrouped
Discovered 120420-247	Ungrouped
Discovered 120420-248	Ungrouped
Discovered 120420-249	Ungrouped
Discovered 120420-250	Ungrouped
Discovered 120420-251	Ungrouped
Discovered 120420-252	Ungrouped
Discovered 120420-254	Ungrouped
Discovered 120420-255	Ungrouped
Discovered 120420-256	Ungrouped

Text:
Field: Name
Processor Family: All Devices
Peerings: All Devices
Groups: All Devices
Status: All Devices
Destination Group: Choose
Device Password:
0 Hosts
0 Zero Clients

Figure 1-8: Management Console Manual Device Discovery Feature

1.3.4 AutoConfig

When the MC discovers new PCoIP zero clients, it automatically adds them to a group and applies the group’s profile. You can create AutoConfig rules to let one group 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:
  - **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 the criteria. Not specifying an IP address range adds zero clients that match the password criteria.
- **DHCP Option Matching:** Add discovered zero clients to this group if their PCoIP DHCP option values are configured so that the group name is set in the **MC AutoConfig Group** option and the **MC AutoConfig Behavior** option is not set to **2**.
  See section 1.3.3.2 for details on configuring DHCP Vendor Class Options.

When a zero client is discovered:

1. The device is listed in the AutoConfig status table with a status of **Not Started**.
2. The zero client IP address and password are compared against all AutoConfig rules.
3. If a match is found, the zero client is added to that group.
4. If the group‘s profile contains a firmware rule, the firmware is applied if it passes the criteria and the device is rebooted.
5. The rest of the profile‘s properties are now applied to the device.
6. After applying the profile‘s OSD logo and properties, the zero client is rebooted.

See section 4.3.3 for more details on configuring AutoConfig.

1.4 Management Console and Firmware Version Compatibility

Table 1-1: Management Console and Firmware Version Compatibility

MC Version	Supports FW Version	Fully Configures FW Versions
1.9.0	0.19-current	0.19-4.1.0 Added the ability to: • Configure Simple Certificate Enrollment Protocol (SCEP) • Configure zero client power down timeout • Disable Connection Management Interface (CMI) • Enable display cloning • Enable 802.1X support for legacy switches • Configure OneSign mode proximity reader beep control option: Use existing proximity card beep mode • Choose the Portuguese (Brazilian ABNT) and Slovak (QWERTY and QWERTZ) keyboard layouts • Enable host hot-plug delay • Configure PCoIP Connection Manager Session Connection Type • Configure custom session Server Name Indication (SNI) • Enable Differentiated Services Code Point (DSCP) • Enable transport congestion notification
1.8.1	0.19-current	0.19-4.0.3

MC Version	Supports FW Version	Fully Configures FW Versions
1.8.0	0.19-current	0.19-4.0.1 Added the ability to: • Configure certification check mode in View Connection Server mode • Enable certification check mode lockout in View Connection Server mode • Clear trusted View Connection Server address cache • Configure session negotiation security level • Configure SNMP community name • Configure Imprivata OneSign appliance verification • Configure Imprivata OneSign desktop name mode • Enable proximity reader beep • Configure session lost timeout • Enable session disconnect hotkey • Configure display topology • Enable monitor emulation on video port 3 and 4 • Enable Wake-on-USB • Enable Wake-on-LAN • Enable power on after power loss • Enable AES-256
1.7.1	0.19-current	0.19-3.5.1 Added the ability to: • Enable session login overlay: “Preparing Desktop…” • Choose the Turkish F keyboard layout

MC Version	Supports FW Version	Fully Configures FW Versions
1.7.0	0.19-current	0.19-3.5.0 Added the ability to: • Configure Imprivata OneSign authentication servers • Configure Self Help Link on VMware View login dialogs • Configure session connection type • Configure minimum image quality and maximum initial image quality on host devices • Enable/disable build to lossless • Configure maximum frame rate • Configure IPv6 • Configure 802.1x authentication • Configure Hotkey to reset Zero Clients to factory default • Configure disconnect message dialog filter • Configure enhanced logging mode • Configure audio-in mode • Configure USB 2.0
1.5.20, 1.5.30, 1.6.0	0.19-current	0.19-3.4.1 Added the ability to: • Configure syslog • Configure static IP address fallback • Choose the Czech, Romanian and Slovenian keyboard layouts • Configure the USB bridging override table
1.4.30, 1.4.40	0.19-current	0.19-3.3.0 Added the ability to: • 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 behavior and content • Choose the Estonian, Hungarian, Latvian and Serbian keyboard layouts • Configure VMware View auto-logon
1.3.30	0.19-current	0.19-3.2.0 Added the ability to: • 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

MC Version	Supports FW Version	Fully Configures FW Versions
1.2.20	0.19-current	0.19-3.1.0 Added the ability to: • Enable/disable SNMP server • Enable/disable host driver function • Configure session encryption modes • Choose the Korean keyboard layout
1.1.20	0.19-current	0.19-2.2 Added the ability to: • 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
1.0.26, 1.0.28	0.19-current	0.19-1.10

2 Installation and Setup

This section describes how to install and set up 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.

- The MC server machine must meet the requirements of the VMware Player 5. For a VMware Player installation, see the VMware Player documentation (http://www.vmware.com/pdf/desktop/vmware_player50.pdf) for the most up-to-date requirements. The current requirements are:
  - 64-bit x86 CPU with LAHF/SAHF support in long mode
  - Processor speed–1.3GHz or faster
  - Memory–1GB minimum, 2 GB recommended. You must have enough memory to run the host operating system, the virtual machine, and applications on the host and guest operating systems.
  - Hard disk–At least 1 GB of free disk space for each guest operating system. For installation, VMware Player requires approximately 250 MB (Windows) or 200 MB (Linux) of free disk space.
- 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 2 GHz 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.
- The MC virtual machine 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.
- The MC server machine must have 4 GB of available disk space to accommodate the virtual machine’s disk image.

2.2 Contents of the Management Console Package

The zip file contains the following files:

- Teradici_PCoIP_Management_Console_Agreement.pdf: Teradici PCoIP Management Console (“Software”) license file
- PCoIP_MC_relA-B-C_vDEF.vmx: Teradici PCoIP Management Console VMware configuration file for the virtual machine that hosts the management console
- PCoIP_MC_relA-B-C_vDEF.vmdk: Teradici PCoIP Management Console VMware virtual disk file containing the virtual machine's hard drive. The size of this file increases as the MC is used. The maximum size of the file is 4 GB.
- README.txt: file describing the contents of the zip file
- TER0812002_Issue_X-PCoIP_Management_Console_User_Manual.pdf: Teradici PCoIP Management Console User Manual, where X is the current issue number

- TER0904003_Issue_X-PCoIP_MC_Release_Notes.pdf: Teradici PCoIP Management Console Release Notes, where X is the current issue number

2.3 Installing the Management Console using VMware Player

1. Download the VMware Player application. 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 an application that you can download 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. 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. Double-click the file **PCoIP_MC_relA-B-C_vDEF.vmx** to launch VMware Player and have it load the MC VM.

   You can also start the MC from within VMware Player. Select **File->Open a Virtual Machine**, and then navigate to the PCoIP_MC_relA-B-C_vDEF.vmx file. Click **Open**. Once VMware Player has launched the MC at least once, you can restart the MC 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. Download and install this free tool from http://www.vmware.com/products/converter/.
2. Click the **Convert Machine** button to launch the **Conversion** wizard.
3. Select source type **VMware Workstation or other VMware virtual machine**.
4. Use the **Browse** button to locate the PCoIP MC's .vmx file. Click **Next**.
5. Select the destination type **VMware Infrastructure virtual machine**.
6. Enter the address, user name, and password of either the VMware vCenter or the VMware ESX host. Click **Next**.
7. Edit the virtual machine name (optional), and then click **Next**.
8. Review the options, and then click **Next**.
9. Click **Finish** to begin the conversion.
10. Once complete, start the VM through VMware vSphere client or your preferred mechanism.
11. See section 2.2 to learn about the contents of the MC virtual machine.

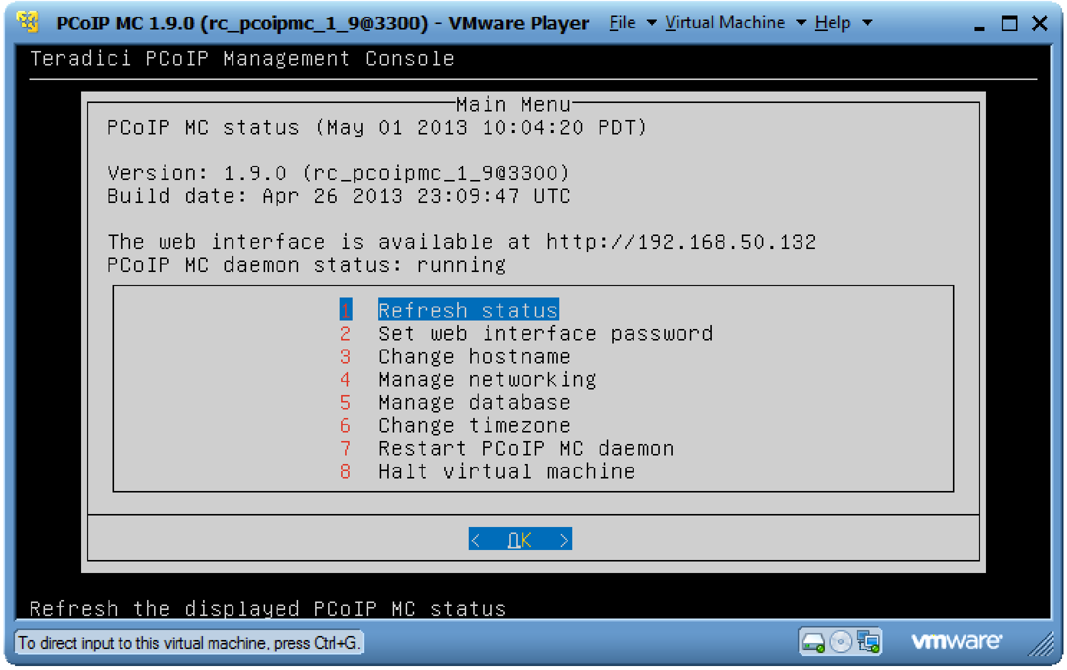
2.5 Running the Management Console

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 the MC console interface shown in Figure 2-1 appears.

Once the VM is started, the MC URL (web site address) appears. The URL is equal to http://192.168.50.132 as shown 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.



```
Teradici PCoIP Management Console

                              Main Menu
PCoIP MC status (May 01 2013 10:04:20 PDT)

Version: 1.9.0 (rc_pcoipmc_1_9@3300)
Build date: Apr 26 2013 23:09:47 UTC

The web interface is available at http://192.168.50.132
PCoIP MC daemon status: running

                    1   Refresh status
                    2   Set web interface password
                    3   Change hostname
                    4   Manage networking
                    5   Manage database
                    6   Change timezone
                    7   Restart PCoIP MC daemon
                    8   Halt virtual machine

Refresh the displayed PCoIP MC status
```

To direct input to this virtual machine, press Ctrl+G.

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 are released. These releases include support for new features and/or bugs fixes. This section describes:

- Potential problems that can occur when migrating to a new version of the MC along with recommendations on how to avoid them
- Information that is and is not imported from a backed up database
- Steps to 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 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.	Do not try to import databases created by a newer version of the MC into older versions of the MC.
When a deployment installs a new version of the MC the PCoIP host and zero client devices may loose contact with the MC.	This problem does not occur if the IP address of the new instance of the MC is the same as the old version of the MC. The best option is to assign a static IP address to the MC. If the MC IP address is assigned by a DHCP server and the deployment installed a MC DNS SRV record, the PCoIP devices eventually re-establish contact with the new version of the MC. The devices are 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. You can force the devices to contact the new MC by resetting the devices. You can also import the database of the old version of the MC. This makes the MC aware of the PCoIP devices in the deployment.

2.6.2 What Information is Imported

When a database is imported into the MC, the following information is 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 is 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 MC time zone settings are not imported.

Note: When migrating to a new version of the MC, you are responsible for reconfiguring the settings that were not imported.

2.6.3 Database Migration Procedure

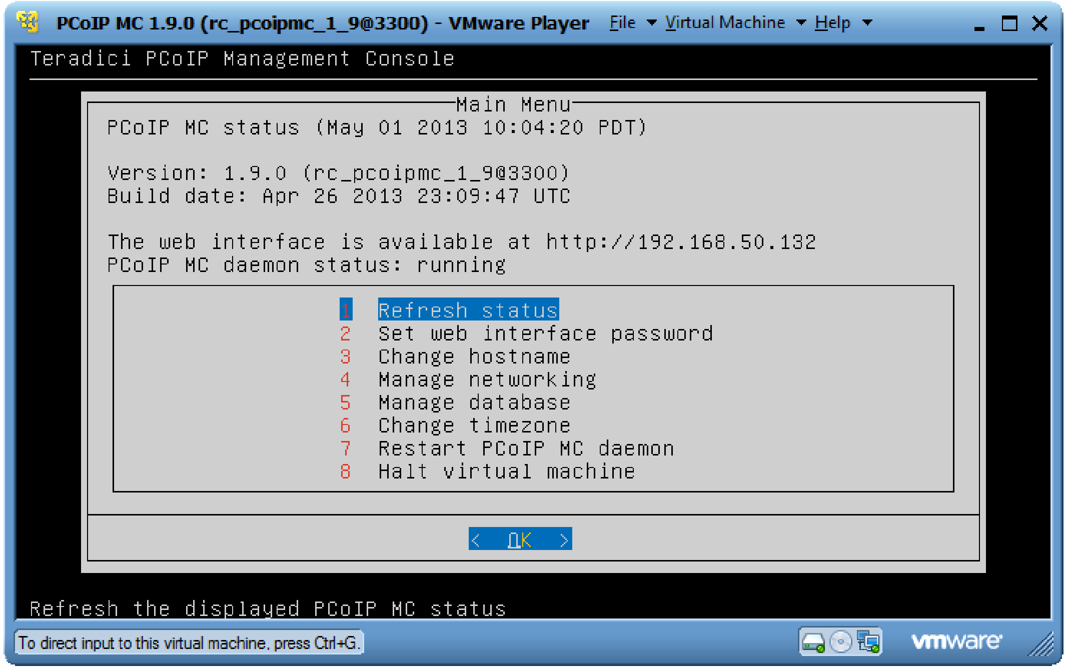
This section lists the process to migrate to a new version of the MC.

1. Use the old version of the MC to back up the current MC database. See section 3.5.1.
2. Download the backed up database to a host computer. See section 4.8.1.
3. See section 2.6.2 for a list of the settings that are and are not imported by the new version of the MC when a database is restored. Before you shut down the old version of the MC, write down the values of the settings that are not imported.
4. Shut down the old version of the MC. See 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. See section 4.8.1.
7. Restore the database from the imported database. See 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 management console is shown in Figure 3-1. This menu appears after you open the MC in the VMware Player. This section describes the features accessed and controlled through this interface (referred to as the “MC VM console” throughout this document).


PCoIP MC 1.9.0 (rc_pcoipmc_1_9@3300) - VMware Player
File
Virtual Machine
Help
To direct input to this virtual machine, press Ctrl+G.
vmware

```
Teradici PCoIP Management Console

                          Main Menu
PCoIP MC status (May 01 2013 10:04:20 PDT)

Version: 1.9.0 (rc_pcoipmc_1_9@3300)
Build date: Apr 26 2013 23:09:47 UTC

The web interface is available at http://192.168.50.132
PCoIP MC daemon status: running

                 1   Refresh status
                 2   Set web interface password
                 3   Change hostname
                 4   Manage networking
                 5   Manage database
                 6   Change timezone
                 7   Restart PCoIP MC daemon
                 8   Halt virtual machine

                       <  OK  >

Refresh the displayed PCoIP MC status
```

Figure 3-1: Management Console VM Console

3.1 Refresh Status

The **Refresh** status option lets you refresh the information that appears in 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, you are prompted to enter a password. To configure this password, select the **Set web interface password** option from the MC VM console.

3.3 Change hostname

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

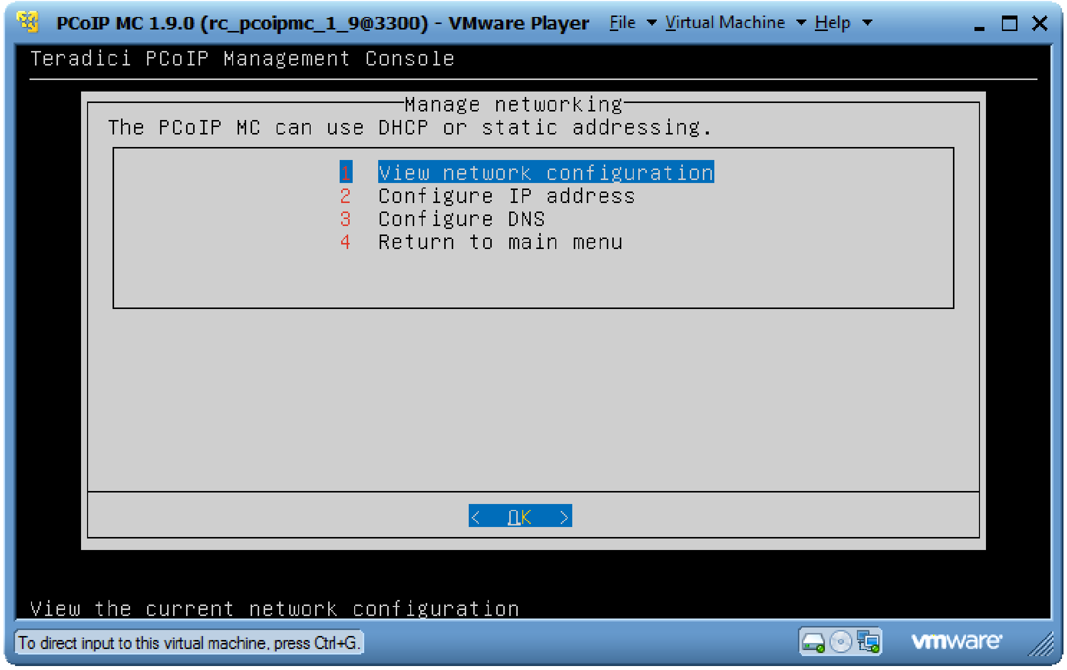
If a deployment installs more than one copy of the MC, makes sure each instance of the hostname is set to a unique value.

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

3.4 Manage Networking

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

The following network options appear:



```
Teradici PCoIP Management Console

                    Manage networking
 The PCoIP MC can use DHCP or static addressing.

                 1   View network configuration
                 2   Configure IP address
                 3   Configure DNS
                 4   Return to main menu

                        <  OK  >

View the current network configuration
```

To direct input to this virtual machine, press Ctrl+G.

Figure 3-2: Manage MC VM Console Network Settings

3.4.1 View Network Configuration

The **View network configuration** option lets you view the current network configuration settings of the MC.

3.4.2 Configure IP Address

The **Configure IP address option** lets you select:

- **DHCP**

- **Static IP addressing:** If you choose static IP addressing, you must configure the MC IP address and subnet mask. The gateway address, broadcast address and domain are optional and can be left blank. After you update the IP address settings, the MC restarts the network interface using the new settings.

3.4.3 Configure DNS

The **Configure DNS** option lets you 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 appears in the site status on the **Home** webpage. See section 4.9 for details.

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.

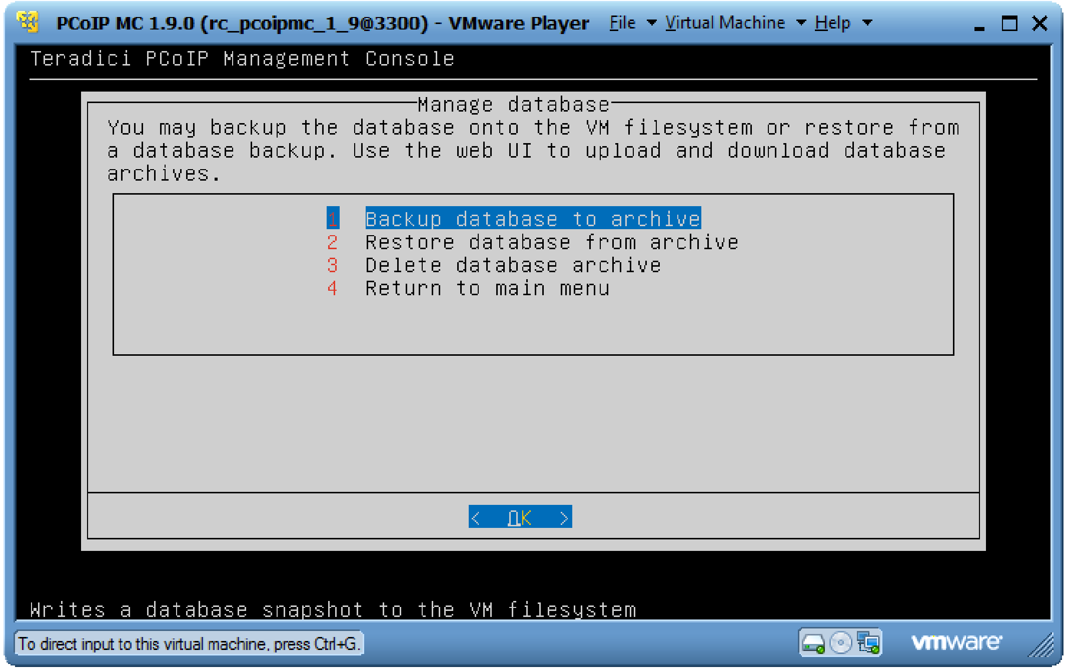
3.5 Database Management

The MC maintains a database containing information on the discovered PCoIP devices, configuration data, 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 let you back up and restore this database. You should use this feature when you upgrade the MC.

Before you install the new version of the MC:

1. Back up the MC database.
2. Export the database to an external PC.
3. Install the new version of the MC.
4. Import the backed up database.

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


PCoIP MC 1.9.0 (rc_pcoipmc_1_9@3300) - VMware Player
File
Virtual Machine
Help
To direct input to this virtual machine, press Ctrl+G.
vmware

```
Teradici PCoIP Management Console

                        Manage database
 You may backup the database onto the VM filesystem or restore from
 a database backup. Use the web UI to upload and download database
 archives.

                 1  Backup database to archive
                 2  Restore database from archive
                 3  Delete database archive
                 4  Return to main menu

                           <  OK  >

Writes a database snapshot to the VM filesystem
```

Figure 3-3: Manage MC VM Console Database

3.5.1 Back Up Database

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

You should use this command with the **Download database** command on the **Database Management** webpage to back up and store the contents of the database somewhere outside of the MC VM. See section 4.8.1 for details on downloading a backup file to the host PC from the MC VM.

3.5.2 Restore Database

The **Restore database** from archive command lets you update the active MC database from a previously stored archive. Note that the archive must already reside within the MC VM before you restore the database.

You should use this command with the **Upload** command on the Database Management webpage to restore the MC database from an archive located outside of the MC VM, possibly on the MC host machine. See section 4.8.1 for information on uploading a backup file to the MC VM from a host PC.

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

3.5.3 Delete Database

The Delete database archive command lets you 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. Because the host does not provide time zone information, you must configure the time zone.

To configure the time zone:

1. Select the **Change timezone** option on the MC VM console.
2. Select a geographic area that determines the time zone. For example, select America/New York if located in the same time zone as New York City.

Note: You can use the MC without configuring the time zone. If you do not configure the timezone, the time that appears at the top of the MC VM console is incorrect and the timestamps that appear on various screens in the MC web interface is incorrect.

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 appears on the MC VM console. This lets you know when the restart is complete.

You should execute this command:

- If the MC daemon status reported on the console interface shown in Figure 3-1 is stopped.
- 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. You can restart the MC VM 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 tool used to manage 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

To access the MC Web User Interface:

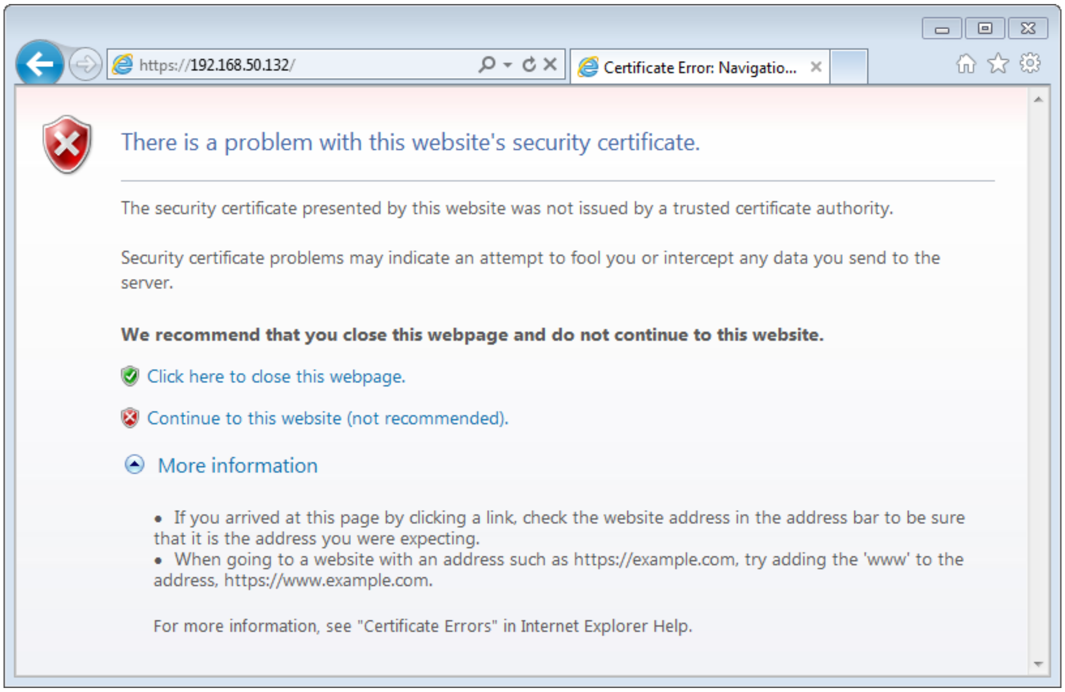
1. Connect a computer to the same network the MC server machine is connected to.

   Note: This computer can be the server machine itself.

2. Open a web browser, and then enter the webpage URL of the MC (shown on the VM console during bootup).

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

   When the web browser first connects to the MC, a security warning appears that is similar to the screen shown in Figure 4-1 for Internet Explorer (see section 4.1.1 for details on installing the certificate) or Figure 4-2 for Firefox (see section 4.1.2 for details on installing the certificate).



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

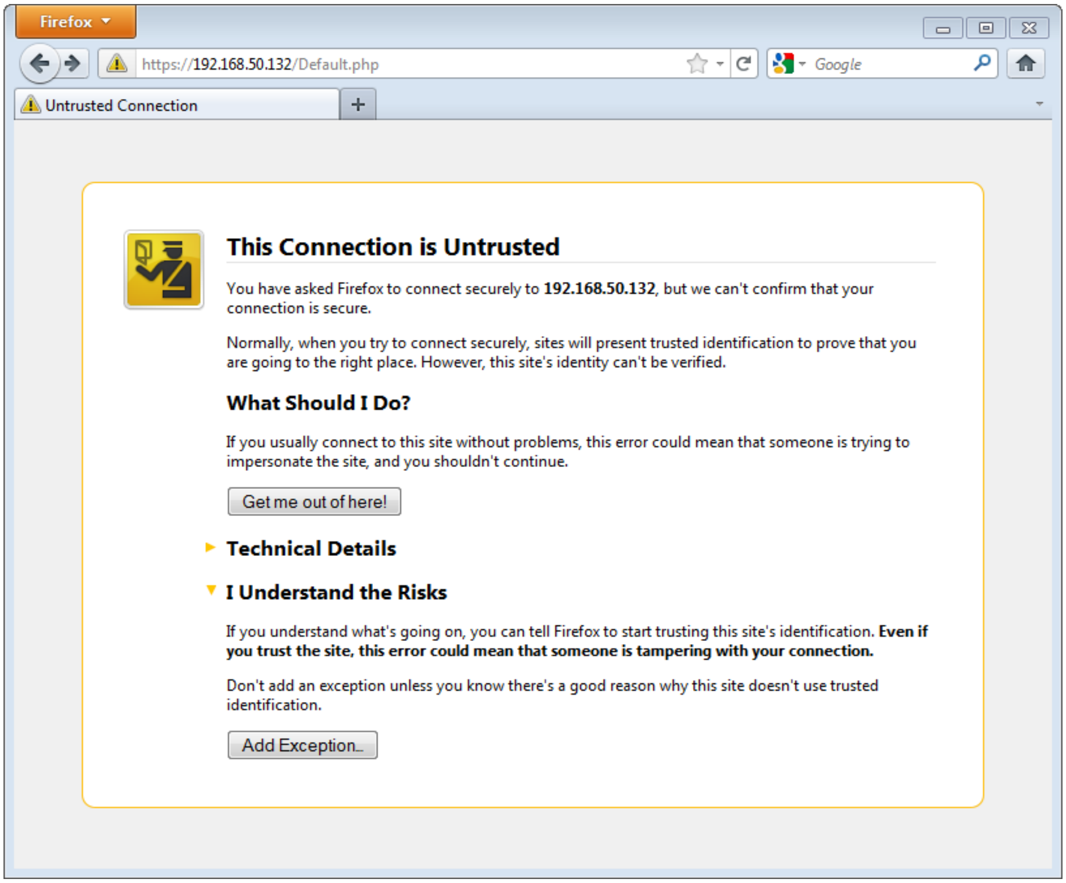
Continue to this website (not recommended).

More information

- If you arrived at this page by clicking a link, check the website address in the address bar to be sure that it is the address you were expecting.
- When going to a website with an address such as https://example.com, try adding the 'www' to the address, https://www.example.com.

For more information, see "Certificate Errors" in Internet Explorer Help.

Figure 4-1: Web Interface Security Warning in Internet Explorer



This Connection is Untrusted

You have asked Firefox to connect securely to **192.168.50.132**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

If you understand what's going on, you can tell Firefox to start trusting this site's identification. **Even if you trust the site, this error could mean that someone is tampering with your connection.**

Don't add an exception unless you know there's a good reason why this site doesn't use trusted identification.

Figure 4-2: Web Interface Security Warning in Firefox

4.1.1 Installing the MC Certificate in Internet Explorer

1. Right-click on **pcoipmc_cacert.p7b**, and then select **Install Certificate**.
2. When the **Certificate Import Wizard** appears click **Next**.
3. Select **Automatically select the certificate store based on the type of certificate**. Click **Next**.
4. Click **Finish** to complete the import. The PCoIP MC CA Root Certificate is now added the Windows' Trusted Root Certification Authorities certificate store.
5. Restart Internet Explorer so that it rescans the Windows' certificate store.

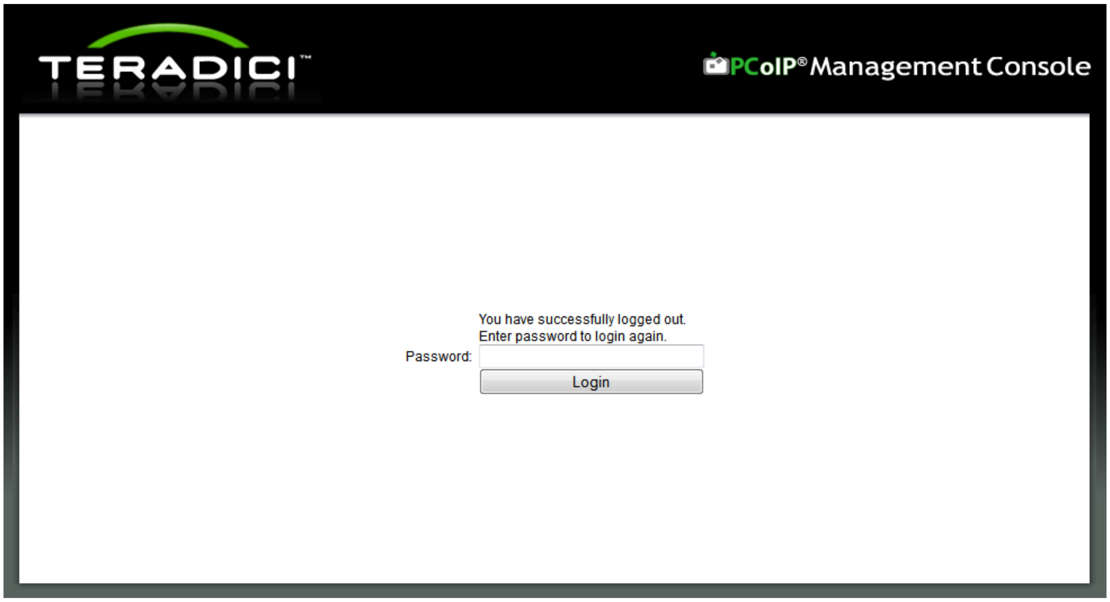
4.1.2 Installing the MC Certificate in Firefox

1. From the **Tools** menu, select **Options**.
2. Click the icon labeled **Advanced" at the top of the window**.
3. From the **Encryption** tab, click the **View Certificates** button.
4. From the **Authorities** tab, click the **Import** button.
5. From the **Select File** dialog, open **pcoipmc_cacert.pem**.
6. When the **Downloading Certificate** dialog appears, check the option labeled **Trust this CA to identify web sites** and then click **OK**. The **PCoIP Management Console Root CA** certificate appears 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 **I Understand the Risks on the This Connection is Untrusted** warning page and follow the directions given to add an exemption.

4.1.3 Logging into the MC Web User Interface

After adding the security exception in Firefox or installing the certificate in either browser, the web browser connects to the MC. You must enter a password as shown in Figure 4-3. The default password is blank. See section 3.2 for details on modifying the password.

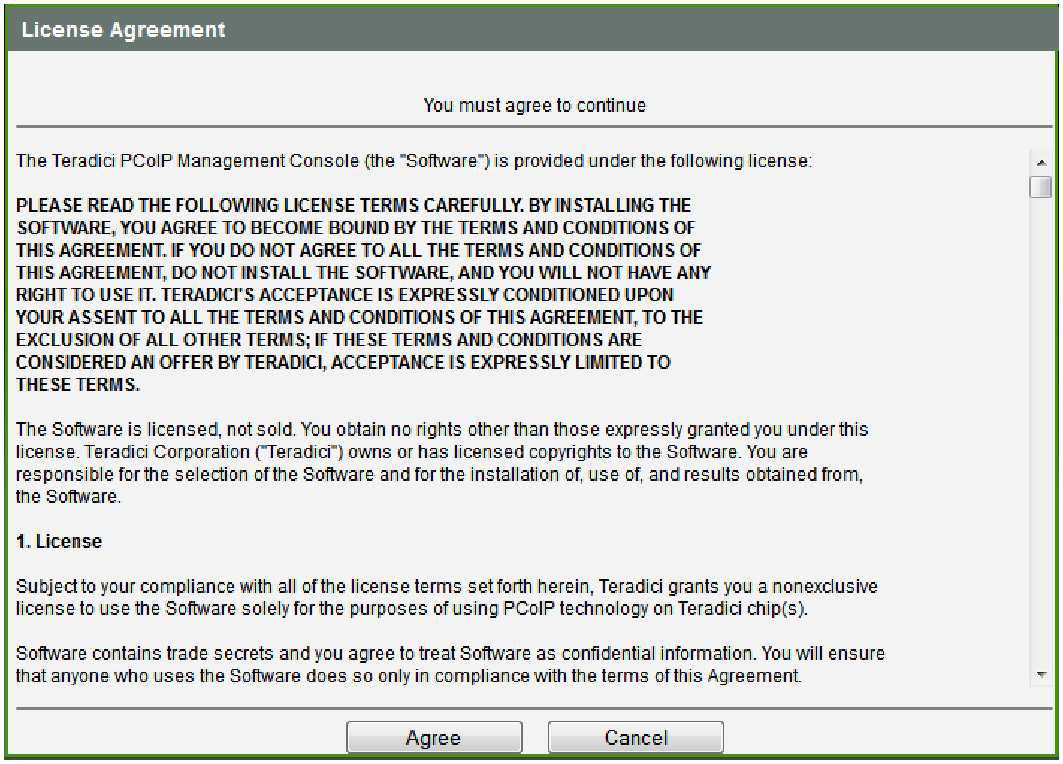


You have successfully logged out.
Enter password to login again.

Figure 4-3: Web Interface Login

4.1.4 Accepting the MC License Agreement

When you first log in to the MC, a prompt appears to accept the MC License Agreement shown in Figure 4-4. You must complete this process once. For subsequent logins to the MC, there is no prompt to accept this agreement. You can view the license agreement by clicking the **License Agreement** link near the bottom of the MC webpages. The MC License Agreement document is also included in the MC .zip file.



You must agree to continue

The Teradici PCoIP Management Console (the "Software") is provided under the following license:

PLEASE READ THE FOLLOWING LICENSE TERMS CAREFULLY. BY INSTALLING THE SOFTWARE, YOU AGREE TO BECOME BOUND BY THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT, DO NOT INSTALL THE SOFTWARE, AND YOU WILL NOT HAVE ANY RIGHT TO USE IT. TERADICI'S ACCEPTANCE IS EXPRESSLY CONDITIONED UPON YOUR ASSENT TO ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT, TO THE EXCLUSION OF ALL OTHER TERMS; IF THESE TERMS AND CONDITIONS ARE CONSIDERED AN OFFER BY TERADICI, ACCEPTANCE IS EXPRESSLY LIMITED TO THESE TERMS.

The Software is licensed, not sold. You obtain no rights other than those expressly granted you under this license. Teradici Corporation ("Teradici") owns or has licensed copyrights to the Software. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from, the Software.

1. License

Subject to your compliance with all of the license terms set forth herein, Teradici grants you a nonexclusive license to use the Software solely for the purposes of using PCoIP technology on Teradici chip(s).

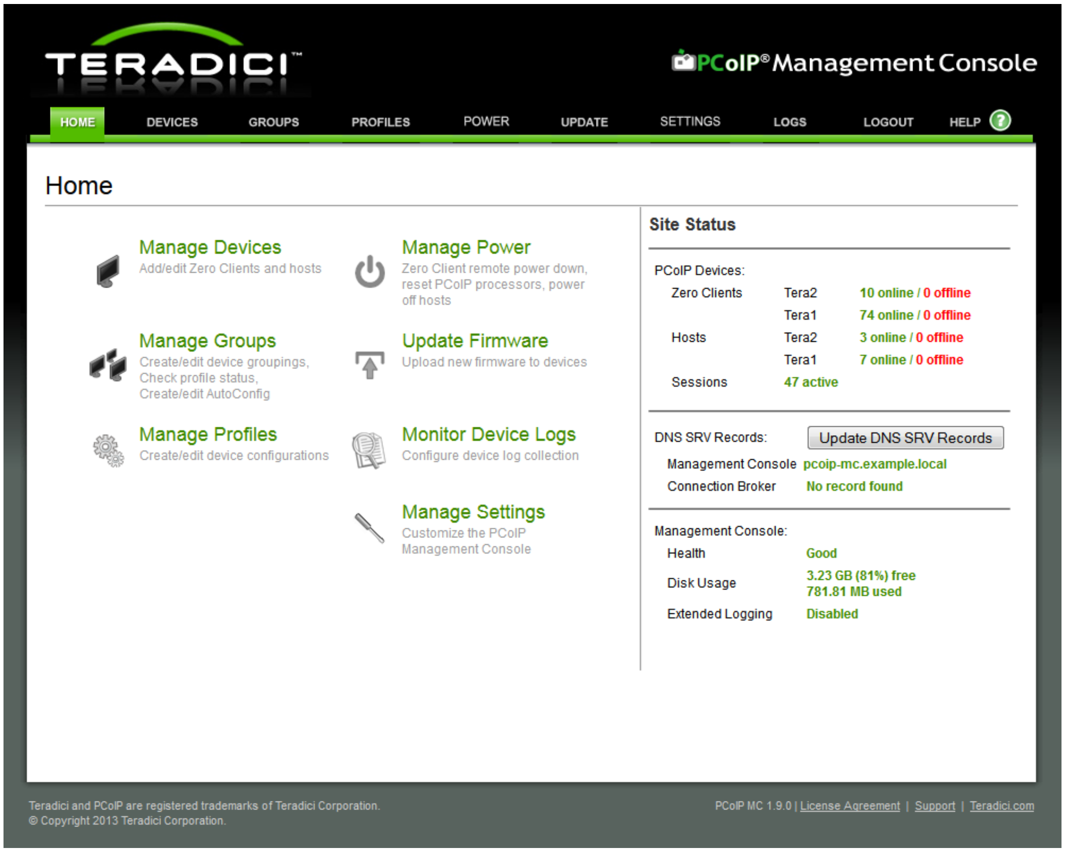
Software contains trade secrets and you agree to treat Software as confidential information. You will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement.

Figure 4-4: Management Console License Agreement

4.1.5 Using the MC Home Page

After you log in, the **MC Home** webpage, shown in Figure 4-5, appears. The **Home** page lets you:

- 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)
- Power off zero client 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)



Home

Manage Devices
Add/edit Zero Clients and hosts

Manage Power
Zero Client remote power down, reset PCoIP processors, power off hosts

Manage Groups
Create/edit device groupings, Check profile status, Create/edit AutoConfig

Update Firmware
Upload new firmware to devices

Manage Profiles
Create/edit device configurations

Monitor Device Logs
Configure device log collection

Manage Settings
Customize the PCoIP Management Console

Site Status

PCoIP Devices:

Zero Clients	Tera2	10 online / 0 offline
	Tera1	74 online / 0 offline
Hosts	Tera2	3 online / 0 offline
	Tera1	7 online / 0 offline
Sessions	47 active	

DNS SRV Records:

Management Console	pcoip-mc.example.local
Connection Broker	No record found

Management Console:

Health	Good
Disk Usage	3.23 GB (81%) free 781.81 MB used
Extended Logging	Disabled

Teradici and PCoIP are registered trademarks of Teradici Corporation.
© Copyright 2013 Teradici Corporation.

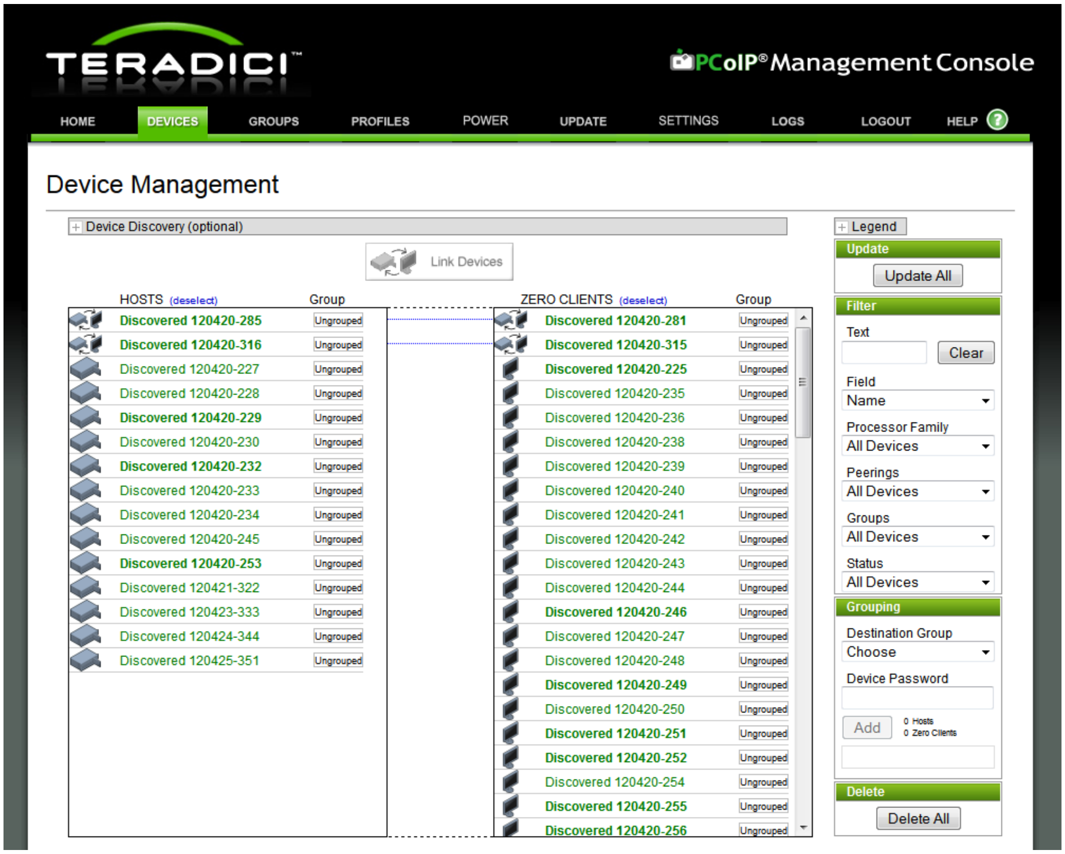
PCoIP MC 1.9.0 | License Agreement | Support | Teradici.com

Figure 4-5: Home Webpage

4.2 Device Management

The **Device Management** webpage, shown in Figure 4-6, lets you:

- 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 webpage
- 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



HOSTS (deselect)	Group
Discovered 120420-285	Ungrouped
Discovered 120420-316	Ungrouped
Discovered 120420-227	Ungrouped
Discovered 120420-228	Ungrouped
Discovered 120420-229	Ungrouped
Discovered 120420-230	Ungrouped
Discovered 120420-232	Ungrouped
Discovered 120420-233	Ungrouped
Discovered 120420-234	Ungrouped
Discovered 120420-245	Ungrouped
Discovered 120420-253	Ungrouped
Discovered 120421-322	Ungrouped
Discovered 120423-333	Ungrouped
Discovered 120424-344	Ungrouped
Discovered 120425-351	Ungrouped

ZERO CLIENTS (deselect)	Group
Discovered 120420-281	Ungrouped
Discovered 120420-315	Ungrouped
Discovered 120420-225	Ungrouped
Discovered 120420-235	Ungrouped
Discovered 120420-236	Ungrouped
Discovered 120420-238	Ungrouped
Discovered 120420-239	Ungrouped
Discovered 120420-240	Ungrouped
Discovered 120420-241	Ungrouped
Discovered 120420-242	Ungrouped
Discovered 120420-243	Ungrouped
Discovered 120420-244	Ungrouped
Discovered 120420-246	Ungrouped
Discovered 120420-247	Ungrouped
Discovered 120420-248	Ungrouped
Discovered 120420-249	Ungrouped
Discovered 120420-250	Ungrouped
Discovered 120420-251	Ungrouped
Discovered 120420-252	Ungrouped
Discovered 120420-254	Ungrouped
Discovered 120420-255	Ungrouped
Discovered 120420-256	Ungrouped

Text:
Field: Name
Processor Family: All Devices
Peerings: All Devices
Groups: All Devices
Status: All Devices
Destination Group: Choose
Device Password:
0 Hosts
0 Zero Clients

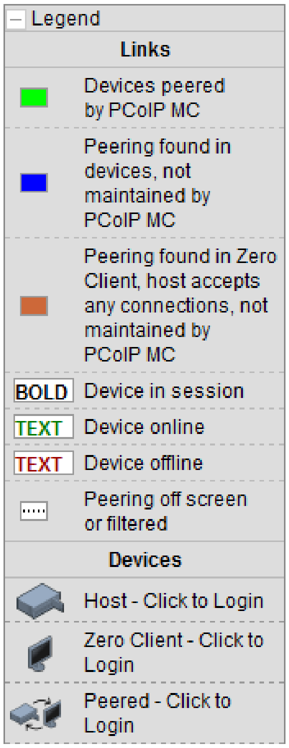
Figure 4-6: Device Management Webpage

4.2.1 Device Discovery (optional)

See section 1.3.3.3 for details about the **Device Discovery** (optional) feature.

4.2.2 Legend

The device management **Legend**, shown in Figure 4-7, describes the meaning of special symbols and line colors that appear on the **Device Management** page. To open the **Legend** box, select the "+" symbol next to the **Legend** text.



– 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

Figure 4-7: Device Management Legend Box

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 are peered by the MC. This means the MC database contains information about the device peering.
- A **blue** or **orange** line indicates the MC 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. The **orange** line indicates the host device is configured to accept connections from any zero client. To have the MC maintain this peering information, link the devices in the MC. See section 4.2.6 for further details.
- 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 indicates whether the device is currently in a session. If a session is active between a host and zero client, the device field name appears in bold characters.

The green/red color of the device field name indicates whether the device is currently online. If a device’s last known state was online, the device field name in green characters appears. Otherwise the device field name appears in red characters.

The following device symbols indicate 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 Querying 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. If you want to force the tool to refresh its internal copy of the device settings, you can use the **Update** box on the upper right hand side of the **Device Management** webpage. This feature lets you update one, multiple, or all devices discovered by the MC.

Note: 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.
- **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.
- **All devices**: Ensure no devices are selected by clicking the deselect links at the top of the HOSTS and ZERO CLIENTS columns. When all devices are de-selected, click the **Update All** button.

A future release of the MC will display a status bar that provides information to let you know when the update is complete. To view the update time using the current version of the tool, from the **Device Management** webpage, set the **Field** option in the **Filter** box to **Last Updated**.

4.2.4 Filtering Devices

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

- The **Field** dropdown menu: Select the device data field that appears in the HOSTS and ZERO CLIENTS columns. You can select from one of the following:
  - **Name**: 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. See section 4.2.10 for more details.
  - **Unique ID:** Read-only device configuration field provisioned at the factory.
  - **MAC Address:** Read-only device configuration field provisioned at the factory.
  - **IP Address:** Configured statically in the device or dynamically by a DHCP server.
  - **FW Version:** Determined by the firmware loaded on the device.
  - **FQDN:** The device FQDN if one is registered with the deployments DNS server. If the FQDN is not registered with the DNS server the MC displays the device IP address.
  - **Last Updated:** Displays the timestamp of when the MC last updated its internal database with the actual device configuration settings.
  - **Label - Name:** The PCoIP device name read from the device.
  - **Label - Description:** The PCoIP device description read from the device.
  - **Label - Generic Tag:** The generic tag read from the device.
  - **Description:** Displays the PCoIP device type description.

- **Text field:** Lets you 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 you enter the string **1.9** in the **Text** field, the tool displays all devices loaded with release 1.9.
- **Processor Family dropdown menu:** Lets you display all devices (Tera1 devices or Tera2).
- **Peerings dropdown menu:** Lets you display all devices (peered devices or unpeered).
- **Groups dropdown menu:** Lets you display all devices (grouped, ungrouped, and devices in individual groups).
- **Status dropdown menu:** Lets you display all devices (online, offline, with an active session and without an active session).

4.2.5 Configuring a Device Group

You should add all devices that are managed by the MC to a group. If a device is not in a group, you cannot perform the following actions:

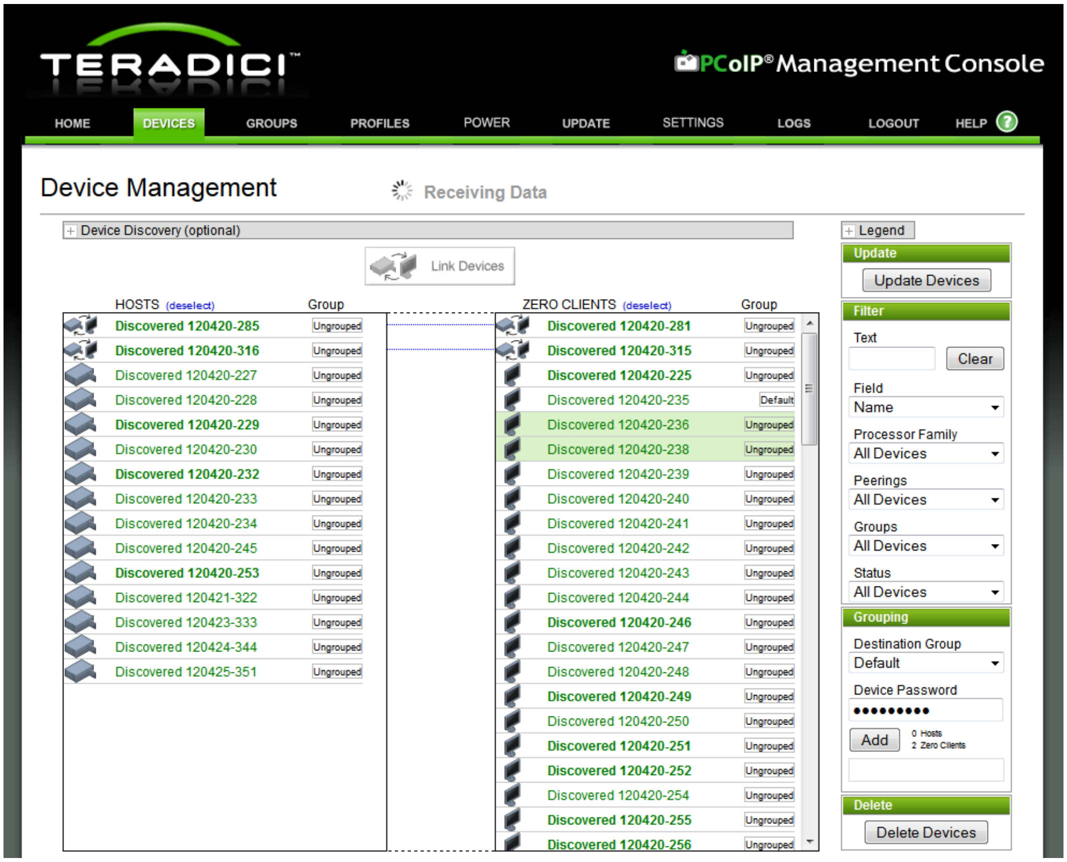
- Apply a profile to the device
- Peer the device
- Send power management commands to the device
- Update firmware on the device
- Edit the device name

See section 1.3.1 for details about MC groups.

To add or reassign one or more devices to a group:

1. Select the device or devices to be added to the group. To select multiple zero client or host devices, hold down the shift key while you select the devices.
2. Select the group to add the devices to using the **Destination Group** drop-down menu.
3. Enter the device password in the **Password** field.
4. Click **Add**. The selected devices are added to the specified group if the device password is correct. The **Group** field for each device successfully added to the group is updated to that of the new group.

Figure 4-8 shows the **Device Management** webpage when adding two zero clients (“Discovered 120420-236” and “Discovered 120420-238”) to the Default group.



Device Management

Receiving Data

Device Discovery (optional)

HOSTS (deselect)	Group
Discovered 120420-285	Ungrouped
Discovered 120420-316	Ungrouped
Discovered 120420-227	Ungrouped
Discovered 120420-228	Ungrouped
Discovered 120420-229	Ungrouped
Discovered 120420-230	Ungrouped
Discovered 120420-232	Ungrouped
Discovered 120420-233	Ungrouped
Discovered 120420-234	Ungrouped
Discovered 120420-245	Ungrouped
Discovered 120420-253	Ungrouped
Discovered 120421-322	Ungrouped
Discovered 120423-333	Ungrouped
Discovered 120424-344	Ungrouped
Discovered 120425-351	Ungrouped

ZERO CLIENTS (deselect)	Group
Discovered 120420-281	Ungrouped
Discovered 120420-315	Ungrouped
Discovered 120420-225	Ungrouped
Discovered 120420-235	Default
Discovered 120420-236	Ungrouped
Discovered 120420-238	Ungrouped
Discovered 120420-239	Ungrouped
Discovered 120420-240	Ungrouped
Discovered 120420-241	Ungrouped
Discovered 120420-242	Ungrouped
Discovered 120420-243	Ungrouped
Discovered 120420-244	Ungrouped
Discovered 120420-246	Ungrouped
Discovered 120420-247	Ungrouped
Discovered 120420-248	Ungrouped
Discovered 120420-249	Ungrouped
Discovered 120420-250	Ungrouped
Discovered 120420-251	Ungrouped
Discovered 120420-252	Ungrouped
Discovered 120420-254	Ungrouped
Discovered 120420-255	Ungrouped
Discovered 120420-256	Ungrouped

Text:
Field: Name
Processor Family: All Devices
Peerings: All Devices
Groups: All Devices
Status: All Devices
Destination Group: Default
Device Password: ●●●●●●●●●
0 Hosts
2 Zero Clients

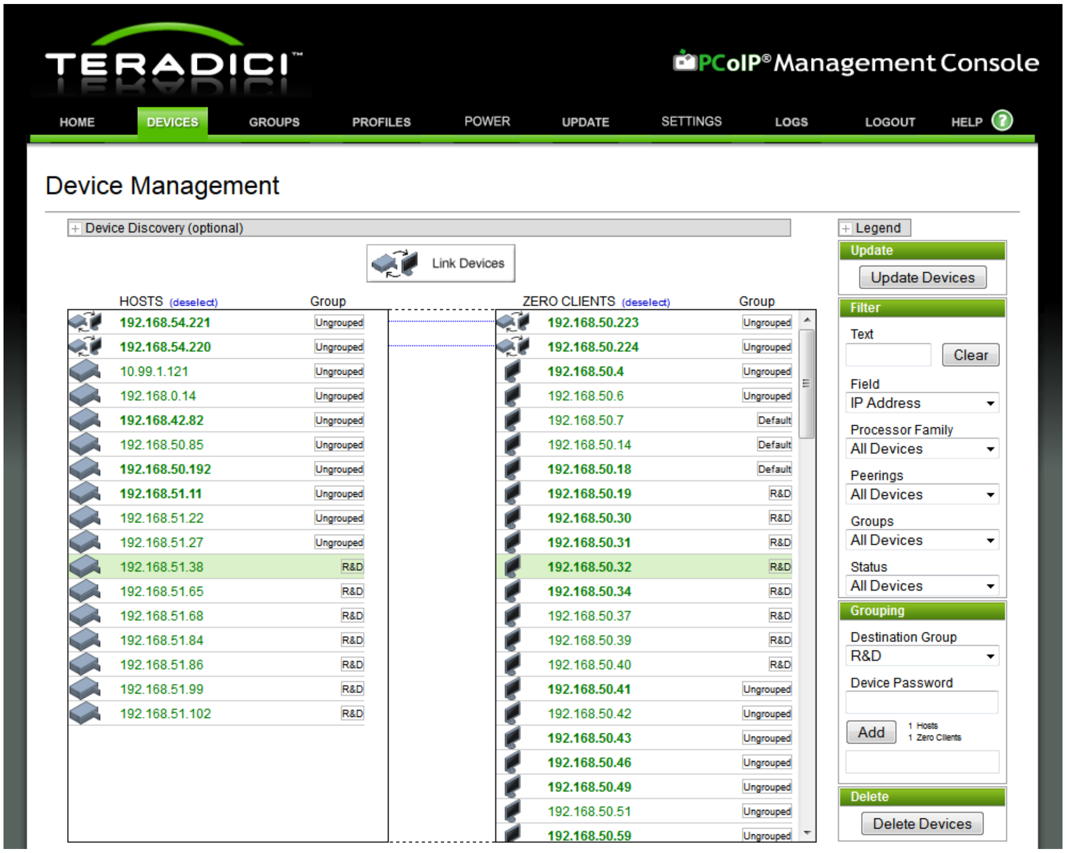
Figure 4-8: Adding Devices to a Group

4.2.6 Linking Devices

You can link together individual host and zero client devices. After two devices are linked, the zero client always establishes a PCoIP session with the linked host when you initiate a connection. The host only accepts connections from the linked zero client.

To link a host and zero client:

1. Select the host and zero client devices to be linked. Figure 4-9 shows the devices 192.168.51.38 and 192.168.50.32 selected.
2. Click the **Link Devices** button that appears below the **Device Discovery** command. After two devices are linked, a green line appears. This indicates the devices are linked in the MC database. The zero client now connects to the host 192.168.51.38 when you select **Connect** on the zero client OSD. See section 4.2.2 for the meaning of the lines that connect devices.



HOSTS (deselect)

HOSTS	Group
192.168.54.221	Ungrouped
192.168.54.220	Ungrouped
10.99.1.121	Ungrouped
192.168.0.14	Ungrouped
192.168.42.82	Ungrouped
192.168.50.85	Ungrouped
192.168.50.192	Ungrouped
192.168.51.11	Ungrouped
192.168.51.22	Ungrouped
192.168.51.27	Ungrouped
192.168.51.38	R&D
192.168.51.65	R&D
192.168.51.68	R&D
192.168.51.84	R&D
192.168.51.86	R&D
192.168.51.99	R&D
192.168.51.102	R&D

ZERO CLIENTS (deselect)

ZERO CLIENTS	Group
192.168.50.223	Ungrouped
192.168.50.224	Ungrouped
192.168.50.4	Ungrouped
192.168.50.6	Ungrouped
192.168.50.7	Default
192.168.50.14	Default
192.168.50.18	Default
192.168.50.19	R&D
192.168.50.30	R&D
192.168.50.31	R&D
192.168.50.32	R&D
192.168.50.34	R&D
192.168.50.37	R&D
192.168.50.39	R&D
192.168.50.40	R&D
192.168.50.41	Ungrouped
192.168.50.42	Ungrouped
192.168.50.43	Ungrouped
192.168.50.46	Ungrouped
192.168.50.49	Ungrouped
192.168.50.51	Ungrouped
192.168.50.59	Ungrouped

Text:
Field: IP Address
Processor Family: All Devices
Peerings: All Devices
Groups: All Devices
Status: All Devices
Destination Group: R&D
Device Password:
1 Hosts
1 Zero Clients

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 tries to write the new IP address into the zero client session settings. It keeps 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 set to the address of the MC managing the device.

Note: This feature is disabled when the **Brokered** setting is set to **Yes**. See section 4.8.2 for more details.

4.2.7 Access Device Webpage

All PCoIP devices have an embedded web server that provides you with access to device configuration settings and status. You can access this web server using a standard web browser. The MC provides multiple quick links that access the device's webpage. See the *PCoIP Zero Client and Host Administrator Guide* (TER1206003) for details.

To access a device's webpage from the **Device Management** webpage, 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 Deleting Devices

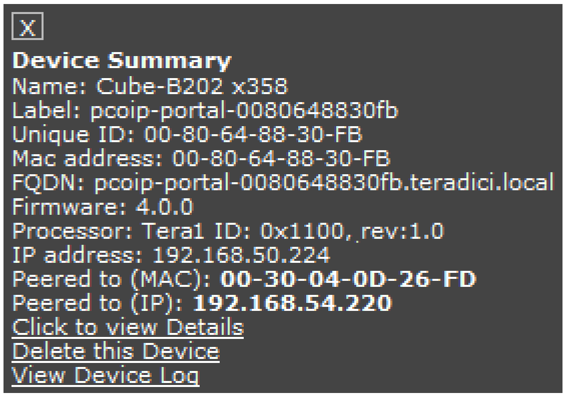
You can delete one, many, or all PCoIP devices by clicking the **Delete** button.

- **Single Device Delete:** Select a device from the list of HOSTS or ZERO CLIENTS, and then click the **Delete Device** button.
- **Multiple Devices Delete:** Select multiple devices by SHIFT-clicking from the list of HOSTS or ZERO CLIENTS, and then click the **Delete Devices** button.
- **All Devices Delete:** Deselect devices if already selected, and then click the **Delete All** button.

Once a device is deleted, its information no longer exists in the database. To manage the deleted device, it should be rediscovered by the MC. Rediscovered devices act same as newly discovered devices.

4.2.9 Summary Device Information

You can view summary information about each device by clicking on the **Device** field in the list of HOSTS or ZERO CLIENT devices. A dialog box appears that provides information about the device. Figure 4-10 displays a summary information dialog box.



Device Summary
Name: Cube-B202 x358
Label: pcoip-portal-0080648830fb
Unique ID: 00-80-64-88-30-FB
Mac address: 00-80-64-88-30-FB
FQDN: pcoip-portal-0080648830fb.teradici.local
Firmware: 4.0.0
Processor: Tera1 ID: 0x1100, rev:1.0
IP address: 192.168.50.224
Peered to (MAC): **00-30-04-0D-26-FD**
Peered to (IP): **192.168.54.220**
Click to view Details
Delete this Device
View Device Log

Figure 4-10: Summary Device Information Dialog Box

The dialog box also lets you configure the device name, view additional device details, delete the device from the MC database, and view the device event log.

4.2.10 Configure Device Name

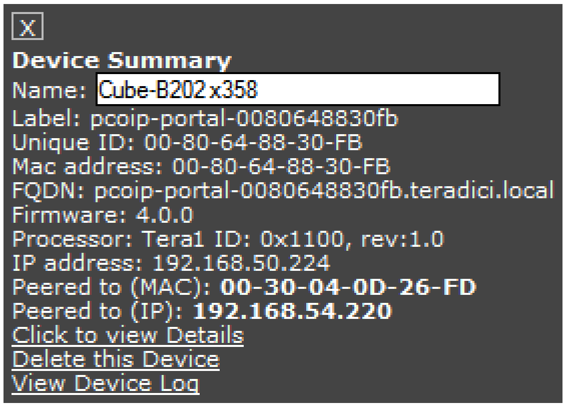
You should configure the name of each device in the system. The device names must be unique. The **Name** field is a string that you can set to whatever they want. Consider including location information in the name to simplify locating the device, but this is up to you to decide.

When a device is first discovered, the MC sets the **Name** to a string containing a timestamp and a unique number.

To modify the device name:

1. Click the device to display the **Summary Device Information** dialog box.
2. Click the **Summary Device** dialog box again. This opens a text editing field that shows the current device name.
3. Enter the new device name.

4. Click **Save** to update the device name. Figure 4-11 displays the summary information dialog box while the device name is being edited.



Device Summary
Name: Cube-B202x358
Label: pcoip-portal-0080648830fb
Unique ID: 00-80-64-88-30-FB
Mac address: 00-80-64-88-30-FB
FQDN: pcoip-portal-0080648830fb.teradici.local
Firmware: 4.0.0
Processor: Tera1 ID: 0x1100, rev:1.0
IP address: 192.168.50.224
Peered to (MAC): **00-30-04-0D-26-FD**
Peered to (IP): **192.168.54.220**
Click to view Details
Delete this Device
View Device Log

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

Note: The device must be part of a group before you can configure the name.

Note: The device name only supports English characters.

4.2.10.1 Access Device Details

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

1. Click the device to display the **Summary Device Information** dialog box.
2. Click the **Click to view Details** link. See section 4.2.9 for details on **Device Details** webpage features.

4.2.10.2 Delete Device from Management Console Database

To delete a PCoIP device from the MC database:

1. Click the device to display the **Summary Device Information** dialog box.
2. Click the **Delete this Device** link in the **Summary Device** window.

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

4.2.10.3 View Device Event Log

PCoIP devices maintain a persistent event log containing messages that may be useful in diagnosing problems. To view a device’s event log:

1. Click the device to display the **Summary Device Information** dialog box.
2. Click the **View Device Log** link in the **Summary Device** window.

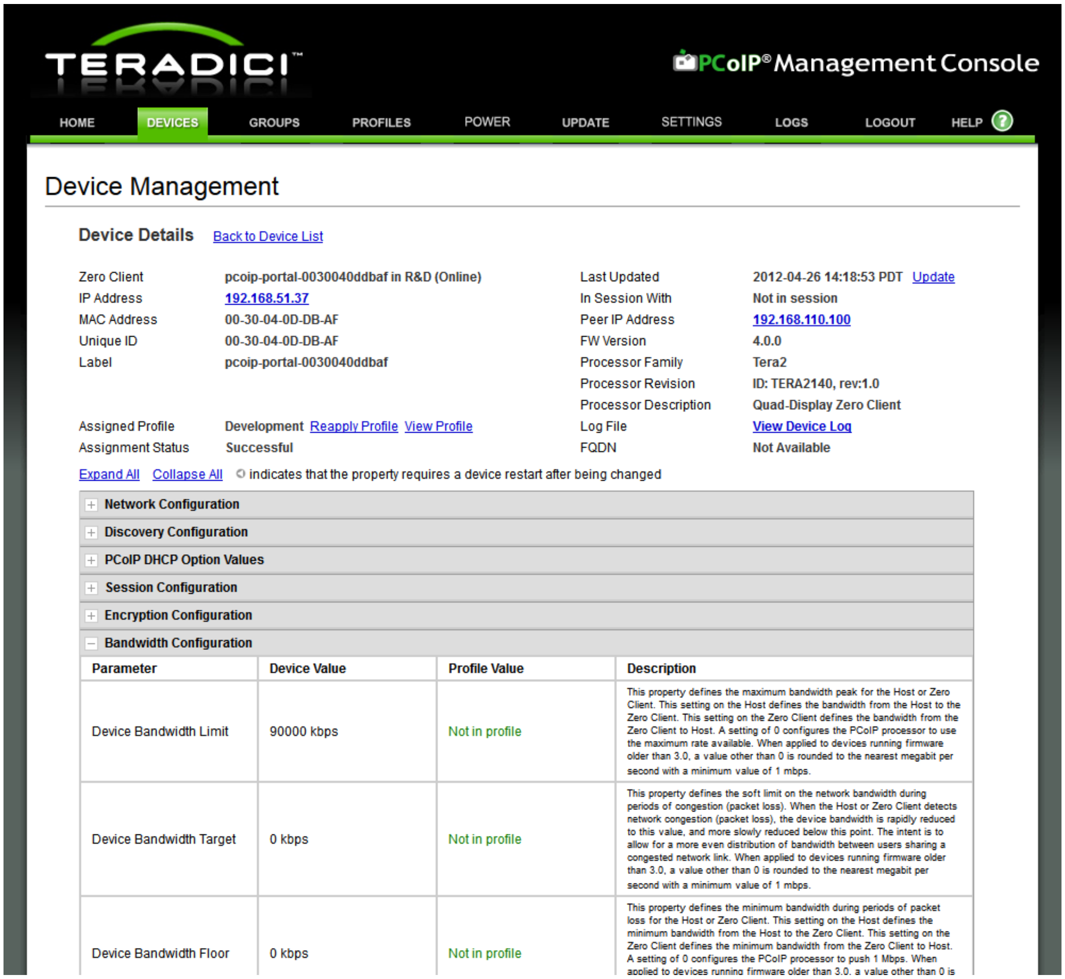
4.2.11 Device Details

Section 4.2.10.1 describes how to access the device details webpage. Figure 4-12 shows the **Device Details** webpage for a zero client.

The **Device Details** webpage lets you:

- 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 webpage
- Open a web browser connected to device’s peer webpage
- View the device’s event log



Device Management

Device Details Back to Device List

Zero Client	pcoip-portal-0030040ddbaf in R&D (Online)	Last Updated	2012-04-26 14:18:53 PDT Update
IP Address	192.168.51.37	In Session With	Not in session
MAC Address	00-30-04-0D-DB-AF	Peer IP Address	192.168.110.100
Unique ID	00-30-04-0D-DB-AF	FW Version	4.0.0
Label	pcoip-portal-0030040ddbaf	Processor Family	Tera2
		Processor Revision	ID: TERA2140, rev:1.0
		Processor Description	Quad-Display Zero Client
Assigned Profile	Development Reapply Profile View Profile	Log File	View Device Log
Assignment Status	Successful	FQDN	Not Available

Expand All Collapse All ○ indicates that the property requires a device restart after being changed

+ Network Configuration
+ Discovery Configuration
+ PCoIP DHCP Option Values
+ Session Configuration
+ Encryption Configuration
− Bandwidth Configuration

Parameter	Device Value	Profile Value	Description
Device Bandwidth Limit	90000 kbps	Not in profile	This property defines the maximum bandwidth peak for the Host or Zero Client. This setting on the Host defines the bandwidth from the Host to the Zero Client. This setting on the Zero Client defines the bandwidth from the Zero Client to Host. A setting of 0 configures the PCoIP processor to use the maximum rate available. When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest megabit per second with a minimum value of 1 mbps.
Device Bandwidth Target	0 kbps	Not in profile	This property defines the soft limit on the network bandwidth during periods of congestion (packet loss). When the Host or Zero Client detects network congestion (packet loss), the device bandwidth is rapidly reduced to this value, and more slowly reduced below this point. The intent is to allow for a more even distribution of bandwidth between users sharing a congested network link. When applied to devices running firmware older than 3.0, a value other than 0 is rounded to the nearest megabit per second with a minimum value of 1 mbps.
Device Bandwidth Floor	0 kbps	Not in profile	This property defines the minimum bandwidth during periods of packet loss for the Host or Zero Client. This setting on the Host defines the minimum bandwidth from the Host to the Zero Client. This setting on the Zero Client defines the minimum bandwidth from the Zero Client to Host. A setting of 0 configures the PCoIP processor to push 1 Mbps. When applied to devices running firmware older than 3.0, a value other than 0 is

Figure 4-12: Device Details Webpage for a Zero Client

4.2.11.1 Device Configuration and Status

The Device Details webpage displays device configuration and status data as well as device profile data. When the webpage first appears, the device categories are collapsed.

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

The following list is 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.
- **Not valid for current session configuration:** The parameter is not specified in the profile because the currently selected session connection type does not support this parameter.

The following 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 are sset to this when the device is not configured to use a CMS.
- **Not supported:** Certain device parameters only apply to specific devices or device models. This value appears for device parameters that are not supported by a device.
- **Not valid for current session configuration:** The parameter is not specified in the profile because the currently selected session connection type does not support this parameter.

4.2.11.2 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 tracks the last time it updated its internal copy of the device data. The **Last Updated** field on the **Device Details** webpage displays this timestamp.

To force the MC to refresh its internal copy of the device values, click the **Update** link.

4.2.11.3 Write Profile Settings to Device

The **Reapply Profile** link lets you write the device profile settings to the device. This can be useful in situations when you want to write the profile settings to a single device in a group.

4.2.11.4 Open Device Profile

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

4.2.11.5 Access Device & Peer Webpages

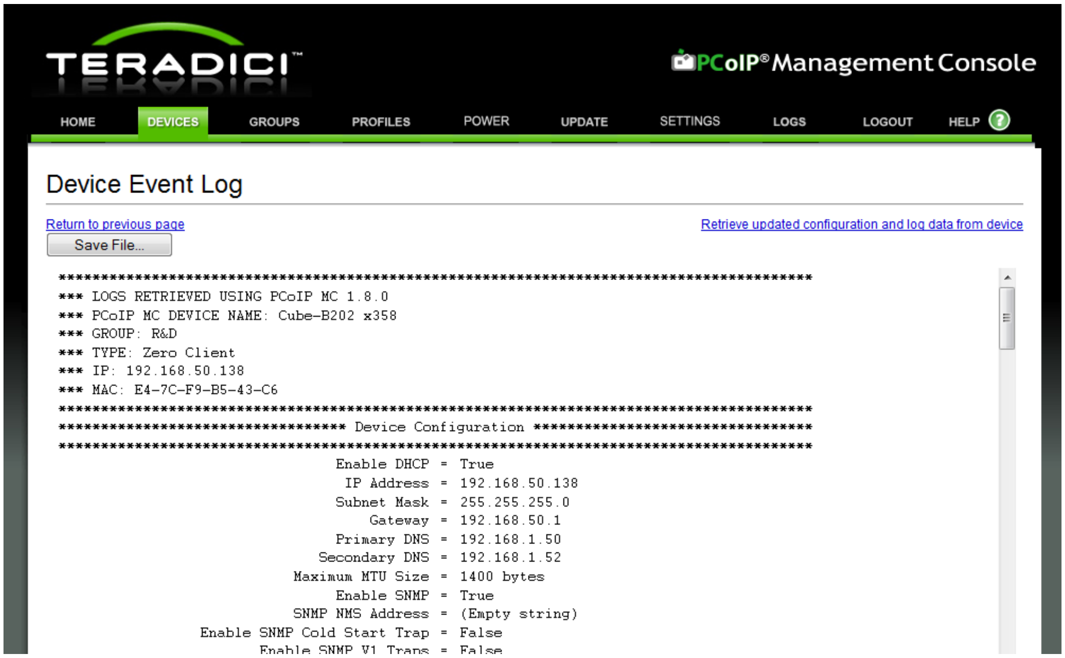
PCoIP devices have an embedded web server that provides you with access to device configuration settings and status. You can access this web server using a standard web browser. The MC provides multiple quick links that you can click to access the webpage:

- Device’s webpage from the **Device Details** webpage: Click the **IP Address** link.
- Peer device’s webpage from the **Device Details** webpage: Click the **Peer IP Address** link.

4.2.11.6 View Device Log

PCoIP devices maintain a persistent event log containing messages that may be useful in diagnosing problems. To access this event log, click the **View Device Log** link. Figure 4-13 shows a **Device Event Log** webpage.

To save the event log to a file, click the **Save File** button. You can retrieve the most recent event log data from the device using the **Retrieve updated log data from device** link.



```
*****************************************************************************************
*** LOGS RETRIEVED USING PCoIP MC 1.8.0
*** PCoIP MC DEVICE NAME: Cube-B202 x358
*** GROUP: R&D
*** TYPE: Zero Client
*** IP: 192.168.50.138
*** MAC: E4-7C-F9-B5-43-C6
*****************************************************************************************
********************************** Device Configuration *********************************
*****************************************************************************************
                                 Enable DHCP = True
                                  IP Address = 192.168.50.138
                                 Subnet Mask = 255.255.255.0
                                     Gateway = 192.168.50.1
                                 Primary DNS = 192.168.1.50
                               Secondary DNS = 192.168.1.52
                            Maximum MTU Size = 1400 bytes
                                 Enable SNMP = True
                            SNMP NMS Address = (Empty string)
                 Enable SNMP Cold Start Trap = False
                        Enable SNMP V1 Traps = False
```

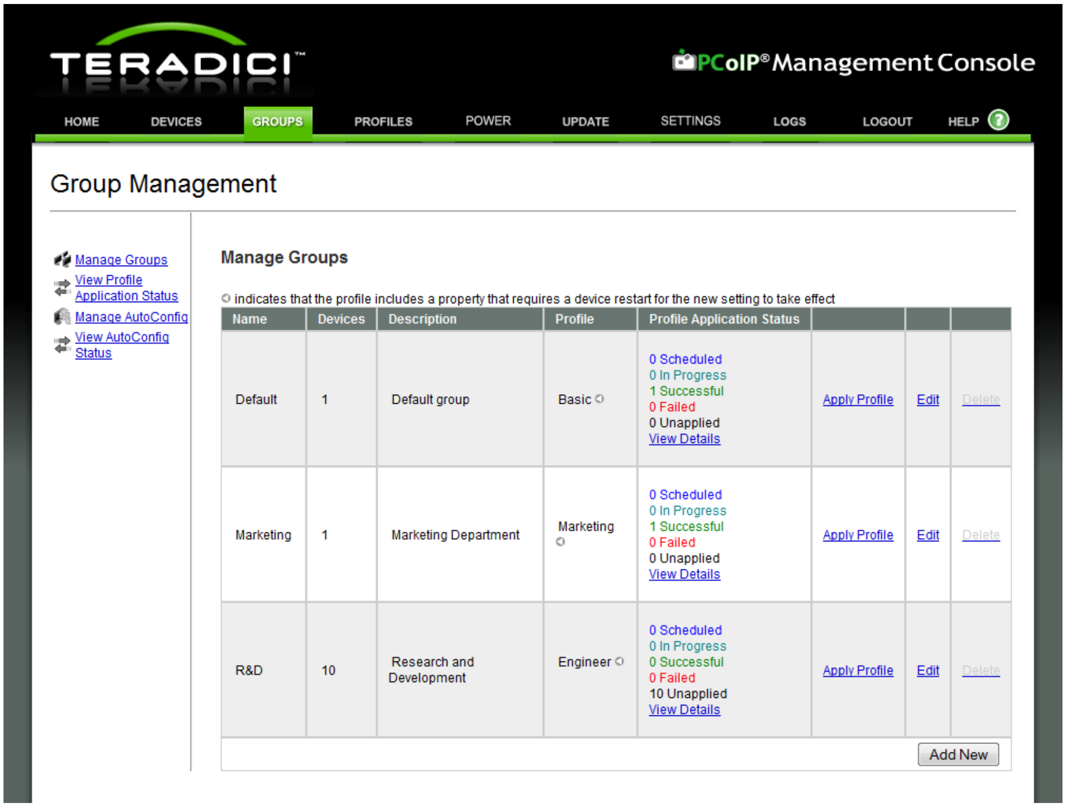
Figure 4-13: Device Event Log Webpage

4.3 Group Management

The **Group Management** webpage, shown in Figure 4-14, lets you view the currently defined groups, view the number of devices in each group, manage AutoConfig rules, and view profile application status information.

The Group Management web page lets you:

- 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



Manage Groups

○ indicates that the profile includes a property that requires a device restart for the new setting to take effect

Name	Devices	Description	Profile	Profile Application Status			
Default	1	Default group	Basic ○	0 Scheduled 0 In Progress 1 Successful 0 Failed 0 Unapplied View Details	Apply Profile	Edit	Delete
Marketing	1	Marketing Department	Marketing ○	0 Scheduled 0 In Progress 1 Successful 0 Failed 0 Unapplied View Details	Apply Profile	Edit	Delete
R&D	10	Research and Development	Engineer ○	0 Scheduled 0 In Progress 0 Successful 0 Failed 10 Unapplied View Details	Apply Profile	Edit	Delete

Figure 4-14: Group Management Webpage

4.3.1 Manage Groups

The **Manage Groups** subcategory lets you view, create, edit, 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 way to apply the profile settings to the entire group.

4.3.1.1 Create a Group

Click **Add New** to create a group. Enter the group name, description, and profile.

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. You can use this group or delete it.

4.3.1.2 Modify a Group

Click the **Edit** link to modify the group name, description, or profile.

4.3.1.3 Delete a Group

Click the **Delete** link to delete a group. You can only delete a group can 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 you click the **Details** link, 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.

The following 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. This problem typically occurs when devices are offline.
- **Unapplied:** The profile was modified since it was last written to the device. This lets you know when you need to reapply a profile to one or more devices in a group.

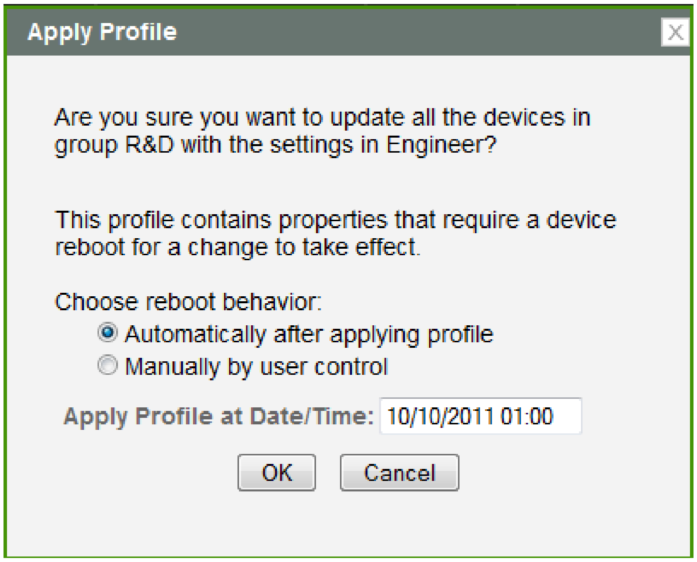
4.3.1.5 Apply a Profile to a Group

Click the **Apply Profile** link 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. Click in the **Apply Profile at Date/Time** field to display a graphical date/time picker. Figure 4-16 shows the date/time picker.

To determine when the profile was written to devices in the group, watch the **Group Management** webpage until the number of **Scheduled updates** is 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 tried to write the profile the status is marked as **Failed**. To see the **View Profile Application** status with the filter set to this group, click **View Details**.



Apply Profile

Are you sure you want to update all the devices in group R&D with the settings in Engineer?

This profile contains properties that require a device reboot for a change to take effect.

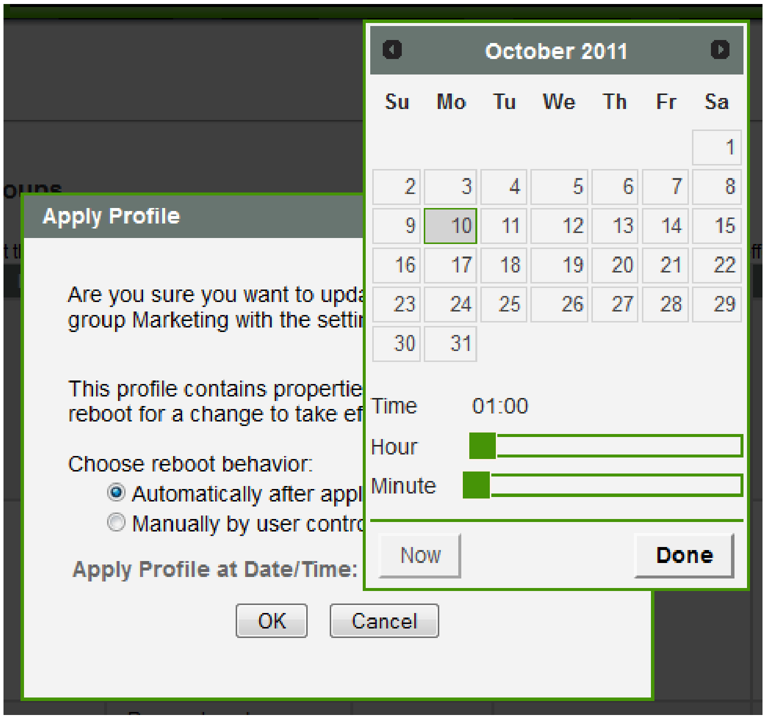
Choose reboot behavior:

● Automatically after applying profile

○ Manually by user control

Apply Profile at Date/Time: 10/10/2011 01:00

Figure 4-15: Apply Profile Reboot Behavior Options



Apply Profile

Are you sure you want to upda
group Marketing with the settir

This profile contains propertie
reboot for a change to take ef

Choose reboot behavior:

● Automatically after appl

○ Manually by user contro

Apply Profile at Date/Time:

October 2011

Su	Mo	Tu	We	Th	Fr	Sa
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Time 01:00

Hour

Minute

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 that represent the expected reboot behavior of devices when the profile is applied.

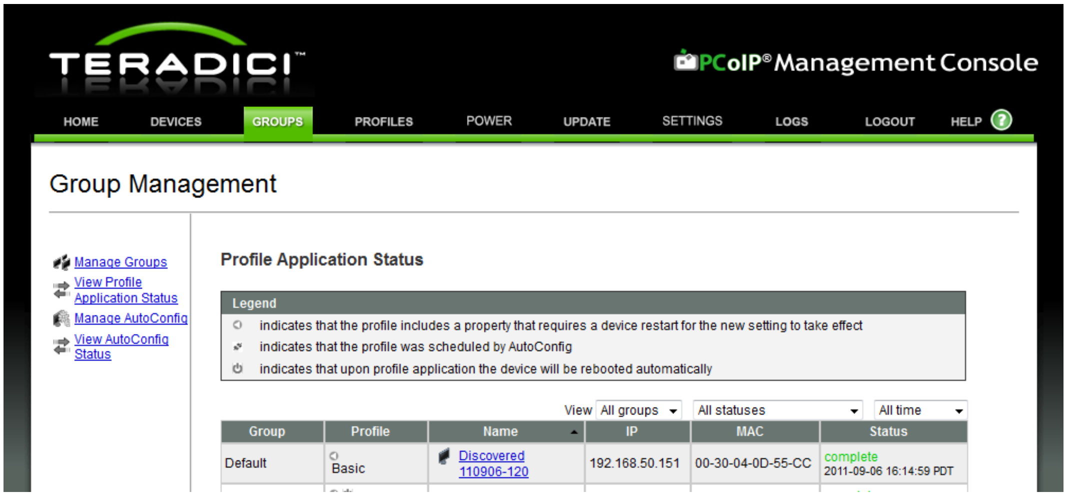
The following legend contains the description of each reboot icon:

◀	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 on profile application, the device is automatically rebooted

The following describes 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 completed writing the OSD logo to the device.
- **firmware pending reboot:** The MC completed writing the profile’s selected firmware to the device and requires a reboot before the profile properties are written.
- **firmware done:** The MC has completed writing the profile’s selected firmware to the device which was also rebooted.
- **SCEP pending:** The MC has completed writing the profile to the device and requires the SCEP certificate installation to finish before completing the profile application.
- **unapplied:** The profile was modified since it was last written to the device. This lets you know when you must reapply a profile to one or more devices in a group.



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
Default	Basic	Discovered 110906-120	192.168.50.151	00-30-04-0D-55-CC	complete 2011-09-06 16:14:59 PDT

Figure 4-17: View Profile Application Status Webpage

4.3.3 Manage AutoConfig

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

You can optionally create an AutoConfig rule 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 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.

  OR

  The DHCP Option Matching is on. The **MC AutoConfig Group** option is set to the identical group name, and the **MC AutoConfig Behavior** option is not set to **2**.

  See section 1.3.3.2 for details on configuring DHCP Vendor Class Options.

- **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 show 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	[ ] Add device with no password PASSWORD	DHCP Option Matching OFF <Empty>
Group B	[x] Add device with no password	DHCP Option Matching ON 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		DHCP Vendor Options		Group A Rule		Group B Rule		AutoConfig Result
IP	Password	MC AutoConfig Group	MC AutoConfig Behavior	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			2	True	False	True	True	Added to Group B
192.168.60.30	PASSWORD	Group A	0	False	True	False	False	Not added to any group
192.168.60.30		Group B	0	False	False	True	True	Added to Group B
192.168.50.30		Group B	2	False	False	False	True	Not added to any group

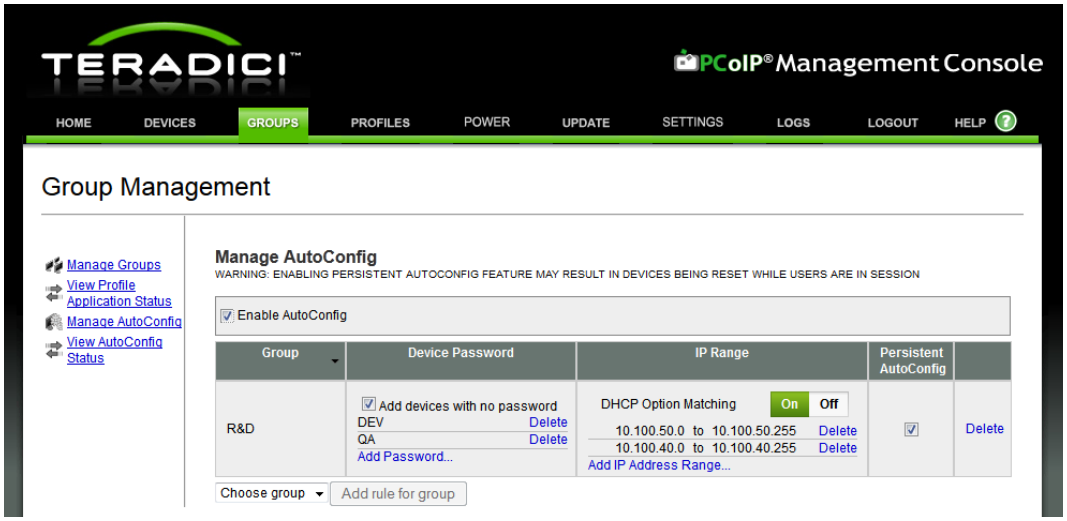
Note: When the **MC AutoConfig Group** is empty the **MC AutoConfig Behavior** is ignored. When the **MC AutoConfig Group** is not empty the MC looks for the group with the identical name and checks if the **DHCP Option Matching** is swiched on. AutoConfig fails if the group does not exist or the group's **DHCP Option Matching** is swiched off. Do not configure the **MC AutoConfig Group** option if you want to use the IP address matching.

To create an 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 then click **Add rule** for group. When a rule is created, it has no IP ranges, **DHCP Option Matching** is off, no specific passwords are set, and **Add device with no passwor**d is checked. If AutoConfig is enabled, this rule matches all zero clients with no password.
3. To restrict the rule's password matching, click **Add** Password, and then add one or more specific passwords to the rule. Once the rule contains one or more specific passwords, you can clear the **Add devices with no password checkbox** 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**, and then add one or more IP address ranges. A rule can have an unlimited number of IP address ranges.
5. To enable DHCP option matching, enable the **DHCP Option Matching** button. DHCP option matching only works if the **PCoIP DHCP Vendor Class Option** is configured.
6. If AutoConfig was disabled in step 1, enable it now to make the current rule configuration active.

When two rules conflict, a warning appears on the **Manage AutoConfig** screen. Leaving rule conflicts unresolved results 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, you can edit AutoConfig rules by adding and removing specific passwords and IP address ranges and changing **the Add devices with no password** checkbox. (Make sure you disable AutoConfig before editing the rules and to re-enable it when done.)



Group Management

Manage Groups
View Profile Application Status
Manage AutoConfig
View AutoConfig Status

Manage AutoConfig

WARNING: ENABLING PERSISTENT AUTOCONFIG FEATURE MAY RESULT IN DEVICES BEING RESET WHILE USERS ARE IN SESSION

☑ Enable AutoConfig

Group	Device Password	IP Range	Persistent AutoConfig	
R&D	☑ Add devices with no password DEV Delete QA Delete Add Password...	DHCP Option Matching On Off 10.100.50.0 to 10.100.50.255 Delete 10.100.40.0 to 10.100.40.255 Delete Add IP Address Range...	☑	Delete

Choose group ▾ Add rule for group

Figure 4-18: Manage AutoConfig Webpage

4.3.4 Persistent AutoConfig

WARNING: ENABLING THIS FEATURE MAY RESULT IN DEVICES BEING RESET WHILE USERS ARE IN SESSION.

The **Manage AutoConfig** subcategory, shown in Figure 4-18, also lets you enable or disable the **Persistent AutoConfig** feature. By default, **Persistent AutoConfig** is disabled. You can enable it for each group by clicking the checkbox. When **Persistent AutoConfig** is enabled, devices that qualify to be in the group periodically get the group's profile applied if one or more settings are different. Conditions 1, 2 and 3 must be true for Persistent AutoConfig to work. The MC checks these conditions every hour to determine the action of **Persistent AutoConfig**.

- **Condition 1**

The **AutoConfig** feature is enabled.

- **Condition 2**

The **Persistent AutoConfig** is enabled.

- **Condition 3**

The **MC AutoConfig Group** option is empty and the zero client is already in the same group.

OR

The DHCP Option Matching is on, the **MC AutoConfig Group** option is set to the identical group, the **MC AutoConfig Behavior** option is set to **0**, and the zero client is in the same group.

OR

The DHCP Option Matching is on, the **MC AutoConfig Group** option is set to the identical group, the **MC AutoConfig Behavior** option is set to **1**, and the zero client is in any group.

Note: Passwords and IP addresses are not compared during the Persistent AutoConfig process.

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

Table 4-3: Example AutoConfig Rules

Group	IP Range Cdn3	Persistent AutoConfig Cdn2
Group A	DHCP Option Matching OFF <Empty>	[ ]
Group B	DHCP Option Matching OFF <Empty>	[x]
Group C	DHCP Option Matching ON <Empty>	[x]

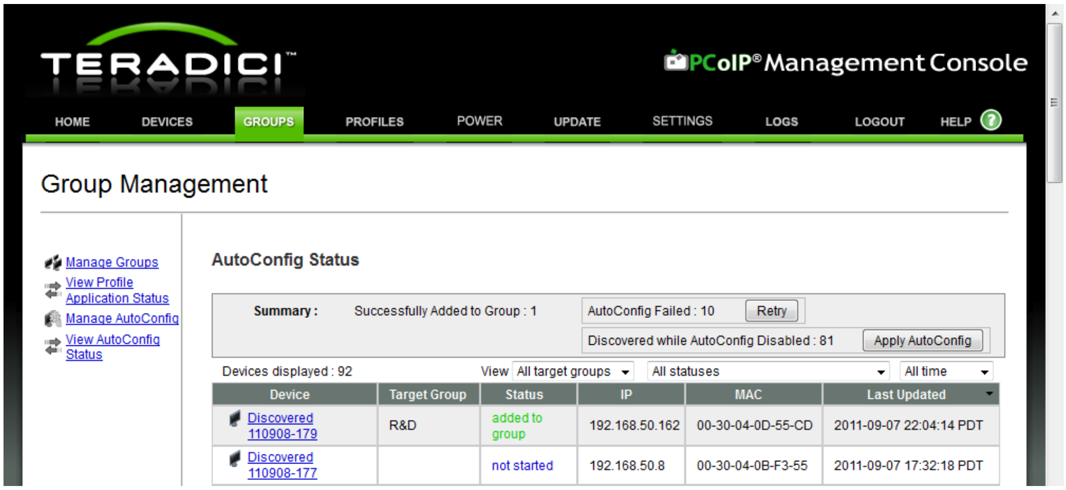
Table 4-4: Example AutoConfig Rule Application

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

Zero Client	DHCP Vendor Options		Group A Rule		Group B Rule		Group C Rule		Persistent AutoConfig Result
Current Group	**MC AutoConfig Group**	**MC AutoConfig Behavior**	**Cdn 2**	**Cdn 3**	**Cdn 2**	**Cdn 3**	**Cdn 2**	**Cdn 3**	
Group A			False	True	True	False	True	False	Profile not applied
Group B			False	False	True	True	True	False	Group B profile applied
Group B	Group B	1	False	False	True	False	True	False	Profile not applied
Group B	Group C	0	False	False	True	False	True	False	Profile not applied
Group B	Group C	1	False	False	True	False	True	True	Moved to Group C and Group C profile applied
Group B	Group C	2	False	False	True	False	True	False	Profile not applied

4.3.5 View AutoConfig Status

The **View AutoConfig Status** subcategory, shown in Figure 4 19, lets administrators view status information, retry AutoConfig to failed devices, and apply AutoConfig to devices that were discovered while AutoConfig was disabled.



Group Management

AutoConfig Status

Summary : Successfully Added to Group : 1 | AutoConfig Failed : 10 | Discovered while AutoConfig Disabled : 81

Devices displayed : 92 View

Device	Target Group	Status	IP	MAC	Last Updated
Discovered 110908-179	R&D	added to group	192.168.50.162	00-30-04-0D-55-CD	2011-09-07 22:04:14 PDT
Discovered 110908-177		not started	192.168.50.8	00-30-04-0B-F3-55	2011-09-07 17:32:18 PDT

Figure 4-19: View AutoConfig Status Webpage

4.3.5.1 View Status Information

The status information shows if devices were discovered and matched the criteria of existing AutoConfig rules along with the profile application status.

The following describes each status category:

- not started: The MC has not yet checked this device for AutoConfig rule compatibility.
- failed error: 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 the rules that matched the device's IP address.
- failed password check (no match): The device does not match the password criteria for the rules that matched the device's IP address.
- added to group: The MC finished adding the device to this group and applies the profile.
- AutoConfig disabled: The device was discovered while AutoConfig was disabled on the **Manage AutoConfig** webpage.
- failed DHCP option group name check: The device failed to be added to a group because the group specified in the **MC AutoConfig Group** could not be found.
- failed AutoConfig (DHCP option matching off): The device failed to be added to this group because the **DHCP Option Matching** was disabled.
- failed AutoConfig (disabled by DHCP option): The device failed to be added to this group because the **MC AutoConfig Behavior** option was set to **2 - Do not AutoConfig**.
- Persistent AutoConfig Pending: The MC has not yet checked this device for Persistent AutoConfig rule compatibility.
- Persistent AutoConfig Success: The MC finished checking the compatibility and moved the device to this group if needed. The profile is applied.
- Persistent AutoConfig disabled: The device was found to have the settings different from the group's profile, but Persistent AutoConfig was disabled on the **Manage AutoConfig** webpage.

Note: A device with a status of **not started** shows an **AC Pending** label in the **Device Management** page. While a device is in this state, you cannot manually add it to a group. Once the device is completed with AutoConfig, its assigned group name is shown.

4.3.5.2 Retry AutoConfig

Click **Retry** to re-apply AutoConfig to devices that had previously failed AutoConfig. The total number of failed devices is displayed in the same box.

4.3.5.3 Apply AutoConfig

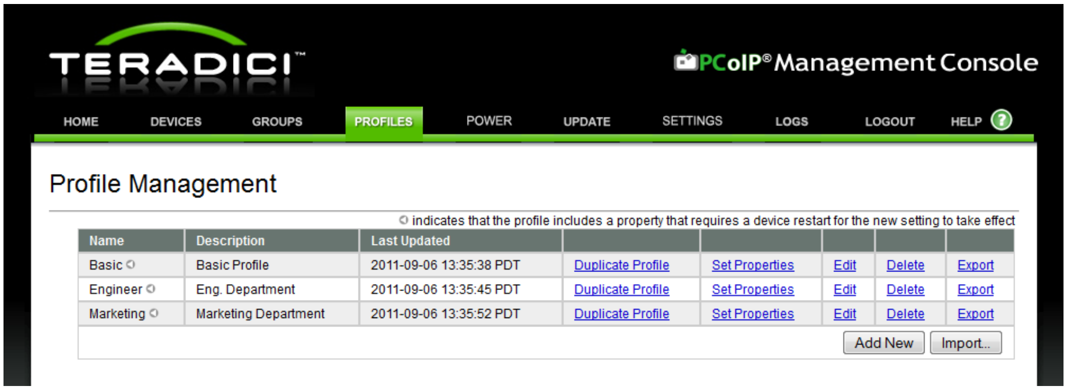
Click **Apply AutoConfig** to apply AutoConfig to ungrouped devices that were discovered while AutoConfig was turned off. The total number of devices being applied appears in the same box.

4.4 Profile Management

The **Profile Management** webpage, shown in Figure 4-20, lets you view the currently defined profiles along with the time each profile was last modified/updated.

The **Profile Management** webpage lets you:

- Create new profiles
- Duplicate profiles
- Delete profiles
- Modify the profile name and description
- Modify the profile properties (device configuration settings)
- Import profiles
- Export profiles



Profile Management

○ indicates that the profile includes a property that requires a device restart for the new setting to take effect

Name	Description	Last Updated					
Basic ○	Basic Profile	2011-09-06 13:35:38 PDT	Duplicate Profile	Set Properties	Edit	Delete	Export
Engineer ○	Eng. Department	2011-09-06 13:35:45 PDT	Duplicate Profile	Set Properties	Edit	Delete	Export
Marketing ○	Marketing Department	2011-09-06 13:35:52 PDT	Duplicate Profile	Set Properties	Edit	Delete	Export

Figure 4-20: Profile Management Webpage

4.4.1 Create a Profile

The **Add New** button lets you create a new profile. After you click **Add New**, enter the profile name and description.

4.4.2 Duplicate a Profile

Click the **Duplicate Profile** link to create a new profile with the same profile properties as the selected profile. Click the **Edit** link to configure the profile name and description after you copy a profile.

Note: You 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 set up, you can copy the profile and then configure the unique profile settings.

4.4.3 Delete a Profile

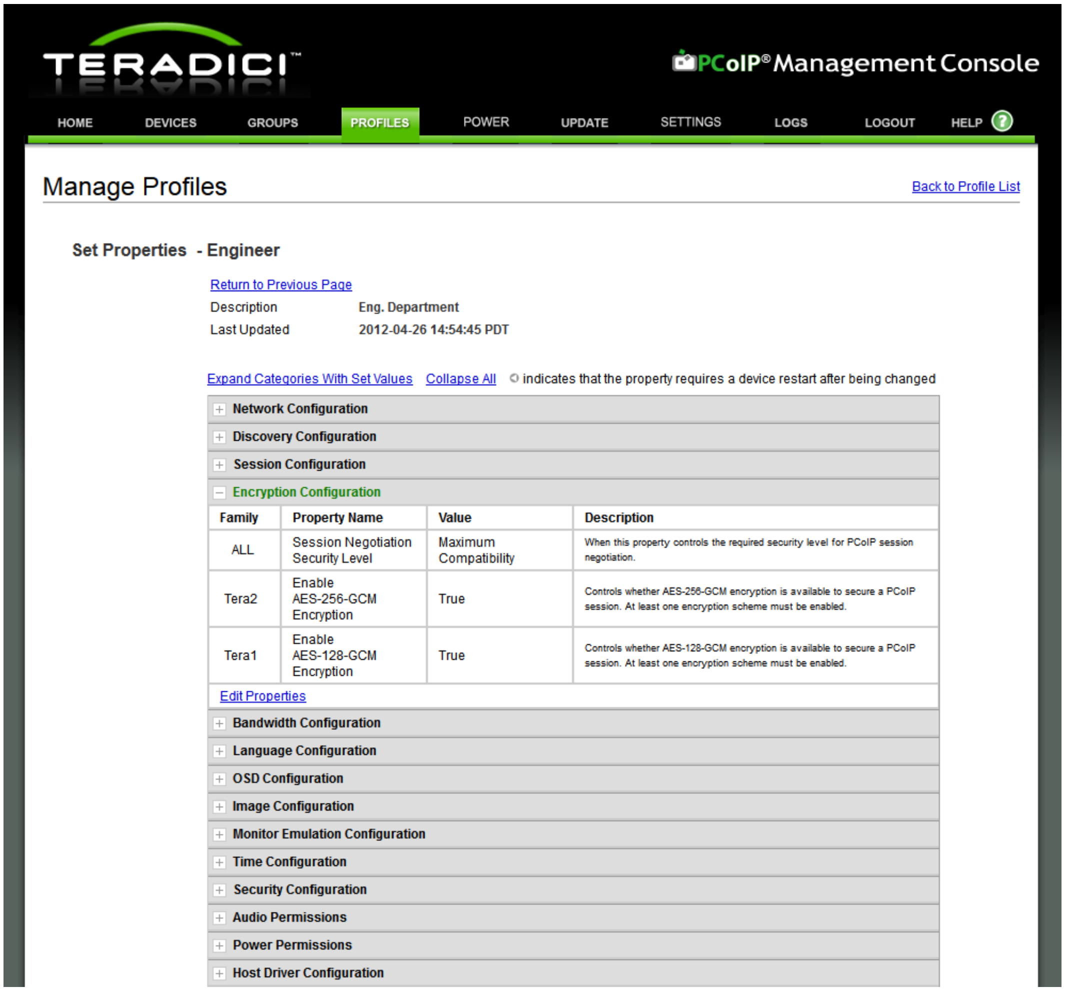
Click the **Delete** link to delete a profile. The **Delete** link does not work if a profile is associated with one or more groups. To delete a profile assigned to one or more groups, use the **Group Management** webpage to first assign a different profile to the group(s) currently using the profile.

4.4.4 Modify Profile Name & Description

Click **Edit** to configure the profile name and description.

4.4.5 Modify Profile Properties

Click the **Set Properties** link to configure the properties of a profile. Figure 4-21 shows the **Profile Management Set Properties** webpage.



Manage Profiles

Back to Profile List

Set Properties - Engineer

Return to Previous Page

Description Eng. Department

Last Updated 2012-04-26 14:54:45 PDT

Expand Categories With Set Values Collapse All ○ indicates that the property requires a device restart after being changed

- ⊞ Network Configuration
- ⊞ Discovery Configuration
- ⊞ Session Configuration
- ⊟ Encryption Configuration

Family	Property Name	Value	Description
ALL	Session Negotiation Security Level	Maximum Compatibility	When this property controls the required security level for PCoIP session negotiation.
Tera2	Enable AES-256-GCM Encryption	True	Controls whether AES-256-GCM encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled.
Tera1	Enable AES-128-GCM Encryption	True	Controls whether AES-128-GCM encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled.

Edit Properties

- ⊞ Bandwidth Configuration
- ⊞ Language Configuration
- ⊞ OSD Configuration
- ⊞ Image Configuration
- ⊞ Monitor Emulation Configuration
- ⊞ Time Configuration
- ⊞ Security Configuration
- ⊞ Audio Permissions
- ⊞ Power Permissions
- ⊞ Host Driver Configuration

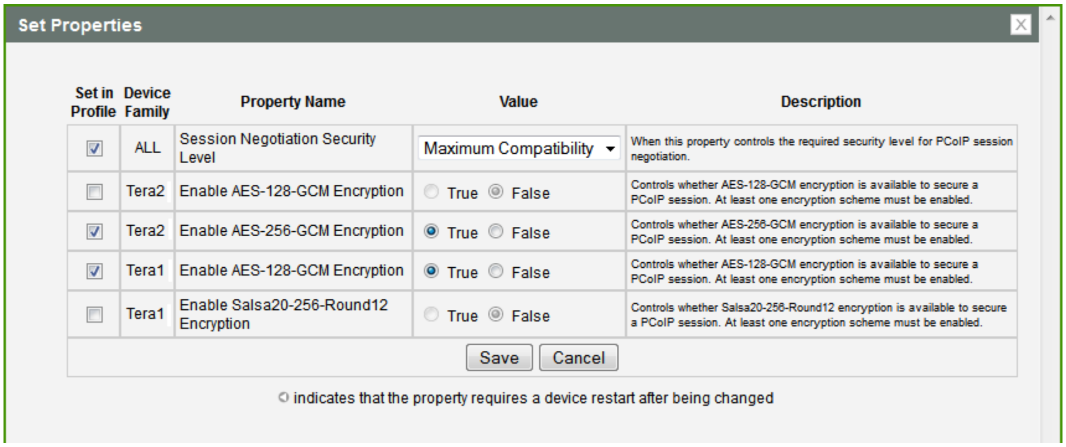
Figure 4-21: Profile Management – Set Properties Webpage

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.

To define individual profile settings, expand the profile property category. The **Encryption Configuration** category is expanded in the previous figure. When a category is expanded, you can access the **Edit Properties** link. Click this link to open a dialog box that specifies the category property settings. Figure 4-22 shows the **Encryption Configuration Settings** dialog box. There are five columns in the configuration settings dialog box.

- **Set in Profile**: Each checkbox in this column determines if a setting is included in the profile. Profile application skips the settings that are not included in the profile and does not change the device settings.

- **Device Family**: This column shows the device family type to which each property setting applies. Figure 4-22 shows one encryption property for all devices, two for Tera1 device family and two for Tera2 device family. Setting Tera1 property values has no effect on the Tera2 devices and vice versa.
- **Property Name**
- **Value**: The fields in this column determine the value of each profile setting.
- **Description**



Set Properties

Set in Profile	Device Family	Property Name	Value	Description
☑	ALL	Session Negotiation Security Level	Maximum Compatibility	When this property controls the required security level for PCoIP session negotiation.
□	Tera2	Enable AES-128-GCM Encryption	○ True ● False	Controls whether AES-128-GCM encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled.
☑	Tera2	Enable AES-256-GCM Encryption	● True ○ False	Controls whether AES-256-GCM encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled.
☑	Tera1	Enable AES-128-GCM Encryption	● True ○ False	Controls whether AES-128-GCM encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled.
□	Tera1	Enable Salsa20-256-Round12 Encryption	○ True ● False	Controls whether Salsa20-256-Round12 encryption is available to secure a PCoIP session. At least one encryption scheme must be enabled.

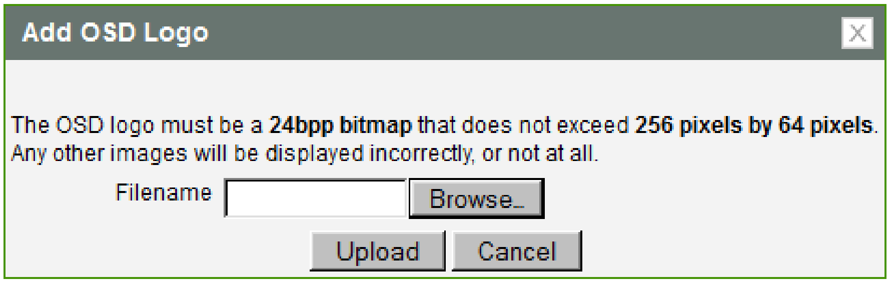
○ indicates that the property requires a device restart after being changed

Figure 4-22: Encryption Configuration Settings Dialog Box

4.4.5.1 OSD Logo in a Profile

To upload a logo for the OSD into a profile (the logo is then applied to the devices groups with that profile):

1. Prepare an image file that is a 24bpp bitmap that does not exceed 256 pixels by 64 pixels.
2. Choose **Profile OSD Logo**, and then **Set OSD Logo**.
3. Click **Browse** to locate your image file.
4. Click **Upload** to import the file to the MC.



Add OSD Logo

The OSD logo must be a **24bpp bitmap** that does not exceed **256 pixels by 64 pixels**. Any other images will be displayed incorrectly, or not at all.

Filename

Figure 4-23: Add OSD Logo Property

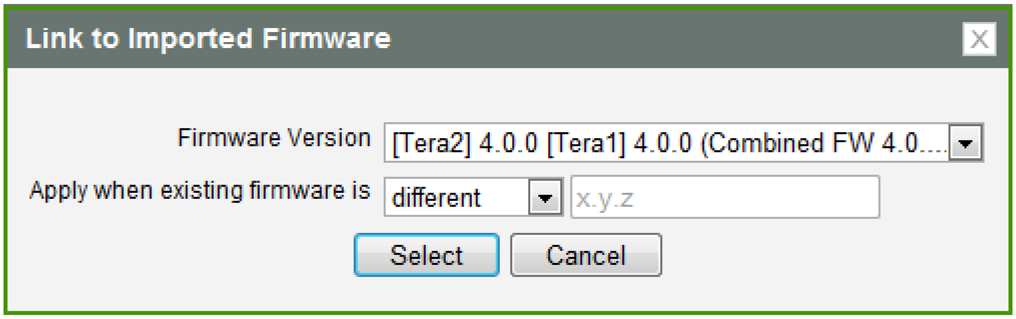
4.4.5.2 Firmware in a Profile

You can assign a firmware file 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:

1. Make sure the firmware file is imported into the MC (see section 4.6.1).
2. Choose **Profile Firmware**, and then **Set Firmware** in the profile properties.

3. Choose the firmware version from the existing firmware versions in the select box. Figure 4-24 shows the **Link to Imported Firmware** dialog.
4. Choose the firmware replacement criteria from these options:
    - **Different:** Firmware is overwritten on the device if its version is different from the firmware version listed in the select box.
    - **Less than:** Firmware is overwritten on the device if its version is less than the x.y.z firmware version you enter in the text entry field.


Link to Imported Firmware

Firmware Version: [Tera2] 4.0.0 [Tera1] 4.0.0 (Combined FW 4.0....

Apply when existing firmware is: different, x.y.z

Figure 4-24: Link to Imported Firmware Property

Note: All supported device family types are indicated in the sqaure brackets. Devices that do not match the device family type are ignored during the profile application.

4.4.5.3 Certificates in a Profile

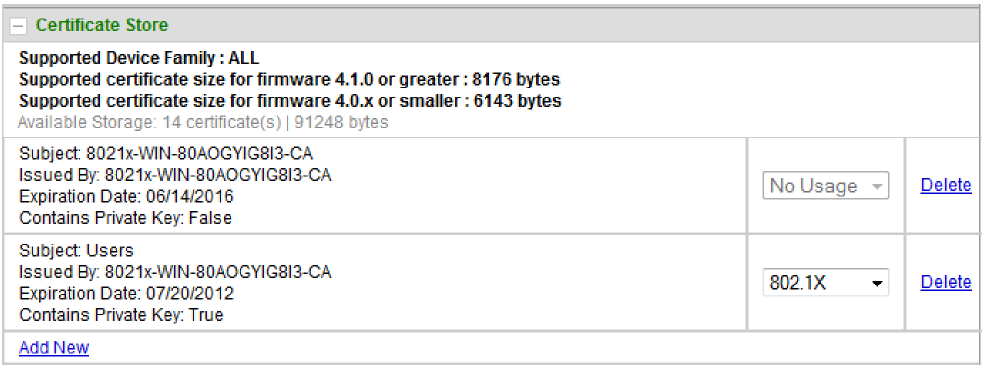
You can upload up to 16 certificate files into a profile and set their usages. The available storage indicates the remaining number of certificates and how much space is left in the certificate store.

Note: When the Simple Certificate Enrollment Protocol (SCEP) setting is configured, only 14 additional certificate files can be uploaded since two slots are reserved for SCEP server certificates.

To upload a certificate file into a profile:

1. Prepare a valid certificate file
2. Choose **Certificate Store**, and then **Add New**
3. Click **Browse** to locate your certificate file
4. Click **Upload**

Once you upload the certificate file you can assign an usage using the dropdown menu in the **Certificate Store** tab.



Certificate Store

Supported Device Family : ALL
Supported certificate size for firmware 4.1.0 or greater : 8176 bytes
Supported certificate size for firmware 4.0.x or smaller : 6143 bytes
Available Storage: 14 certificate(s) | 91248 bytes

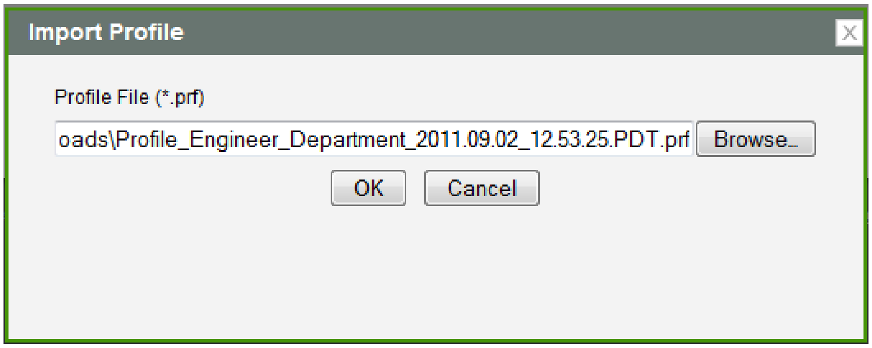
Subject: 8021x-WIN-80AOGYIG8I3-CA Issued By: 8021x-WIN-80AOGYIG8I3-CA Expiration Date: 06/14/2016 Contains Private Key: False	No Usage	Delete
Subject: Users Issued By: 8021x-WIN-80AOGYIG8I3-CA Expiration Date: 07/20/2012 Contains Private Key: True	802.1X	Delete

Add New

Figure 4-25: Profile Management – Certificate Store

4.4.6 Import a Profile

Click **Import** to create a new profile by importing a profile from a file. You must then locate the file in the file system. Figure 4 25 shows the **Import Profile** dialog.



Import Profile

Profile File (*.prf)

oads\Profile_Engineer_Department_2011.09.02_12.53.25.PDT.prf

Figure 4-26: Import Profile Dialog

If the imported profile contains a firmware file, the import process adds a new firmware file to the **Update Devices** webpage.

4.4.7 Export a Profile

Click **Export** to export a selected profile into a file. You must then confirm the download to start the export process.

Note: You may find it useful to export a profile and share it with other MCs if multiple instances of MCs are deployed.

4.5 Power Management

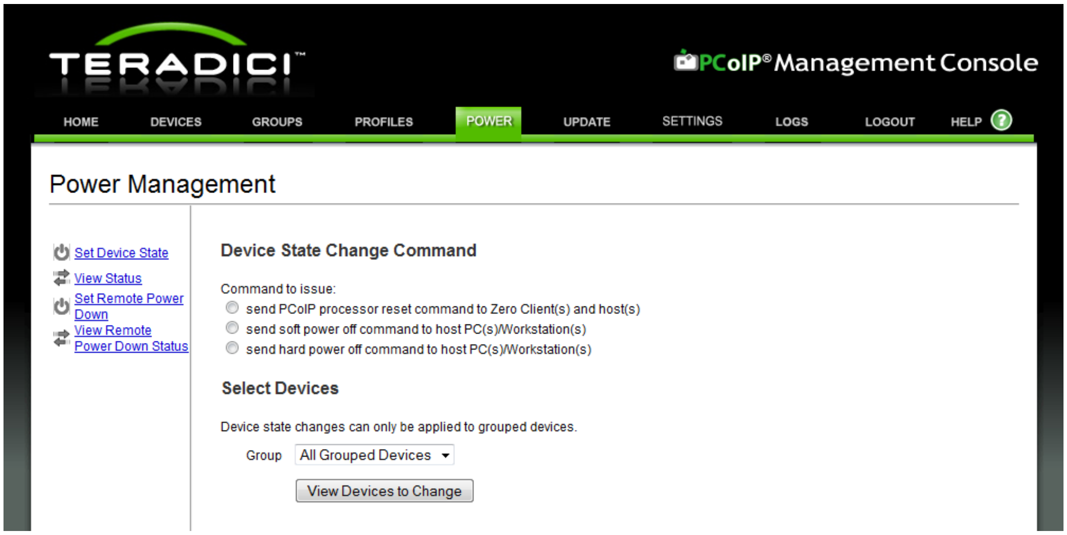
The **Power Management** webpage lets you :

- 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
- Display the current power state of host PCs/workstations
- Display status information on the last or next scheduled reset and power off commands for each PCoIP device

- Schedule remote power down for zero client devices
- Display status information on the device that received the remote powerdown

4.5.1 Sending Reset and Power off Commands

Click the **Set Device State** link on the **Power Management** webpage to schedule reset and power off commands to be sent to PCoIP devices. The webpage shown in Figure 4-26 appears.



Power Management

Device State Change Command

Command to issue:

○ send PCoIP processor reset command to Zero Client(s) and host(s)
○ send soft power off command to host PC(s)/Workstation(s)
○ send hard power off command to host PC(s)/Workstation(s)

Select Devices

Device state changes can only be applied to grouped devices.

Group: All Grouped Devices

Figure 4-27: Send Device State Change Command Webpage

In the **Set Device State** webpage, reset commands can be sent to both host and zero client devices, while power off commands can only be sent to host devices. To power off zero client devices, see the **Set Remote Power Down** webpage (section 4.5.3).

Reset Commands

- A PCoIP zero client resets immediately when it receives a reset command.
- A PCoIP host device schedules 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.

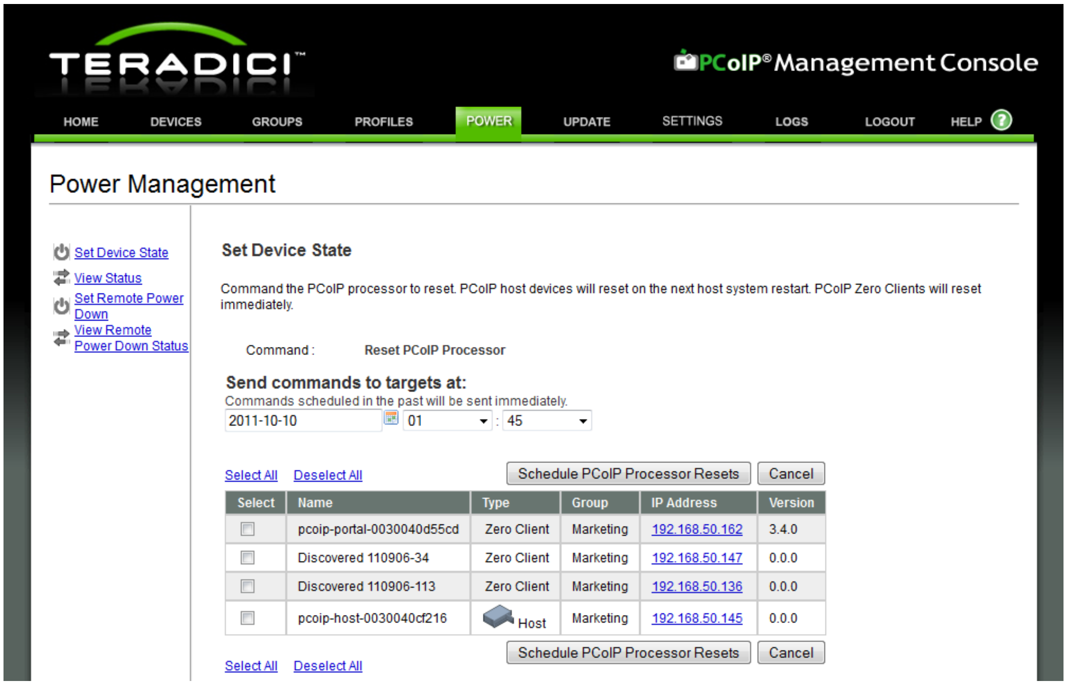
Power Off Commands

- Soft power off commands sent to host PCoIP devices trigger the same action that occurs when you click the host PC/workstation **Power** button for less than four seconds. The action taken by the host depends 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 you press the host PC/workstation **Power** button for more than four seconds. This immediately shuts down the PC/workstation by turning off its power.

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

To send a reset or power off command to a device:

1. Select the command type by selecting one of the radio buttons shown in Figure 4-26.
2. Filter the devices the command may be sent to using the **Group** dropdown menu.
3. Click the **View Devices to Change** button to display a new webpage. Figure 4-27 shows the webpage that supports sending the **PCoIP Processor Reset** command.



Power Management

Set Device State

Command the PCoIP processor to reset. PCoIP host devices will reset on the next host system restart. PCoIP Zero Clients will reset immediately.

Command : Reset PCoIP Processor

Send commands to targets at:

Commands scheduled in the past will be sent immediately.

2011-10-10 01 : 45

Select	Name	Type	Group	IP Address	Version
□	pcoip-portal-0030040d55cd	Zero Client	Marketing	192.168.50.162	3.4.0
□	Discovered 110906-34	Zero Client	Marketing	192.168.50.147	0.0.0
□	Discovered 110906-113	Zero Client	Marketing	192.168.50.136	0.0.0
□	pcoip-host-0030040cf216	Host	Marketing	192.168.50.145	0.0.0

Figure 4-28: Schedule Device State Change Command Webpage

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

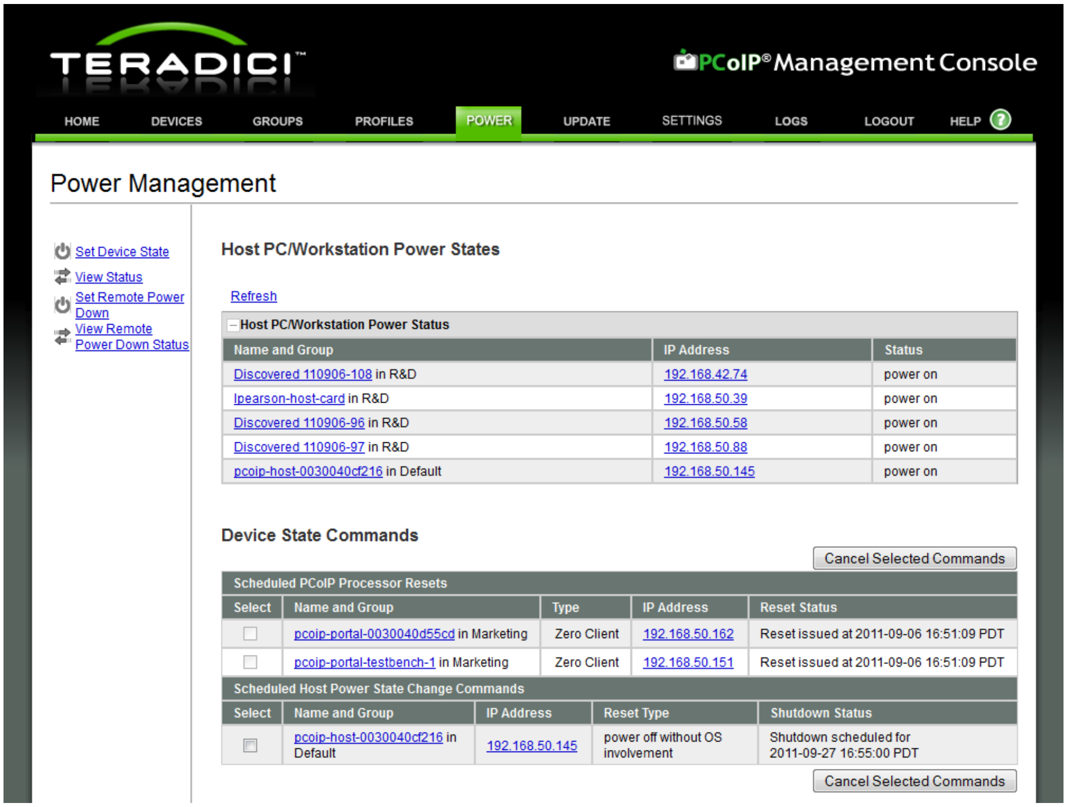
You must choose which devices the command is sent to by selecting the checkbox next to each target.

To schedule the command(s), 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), click the **View Status** link on the left side of the screen to view the status of the command(s).

4.5.2 Power Management Status

Click the **View Status link** on the **Power Management** webpage toview 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. Figure 4-28 shows an example of the Power Management Status webpage.



Power Management

Host PC/Workstation Power States

Host PC/Workstation Power Status

Name and Group	IP Address	Status
Discovered 110906-108 in R&D	192.168.42.74	power on
lpearson-host-card in R&D	192.168.50.39	power on
Discovered 110906-96 in R&D	192.168.50.58	power on
Discovered 110906-97 in R&D	192.168.50.88	power on
pcoip-host-0030040cf216 in Default	192.168.50.145	power on

Device State Commands

Scheduled PCoIP Processor Resets

Select	Name and Group	Type	IP Address	Reset Status
□	pcoip-portal-0030040d55cd in Marketing	Zero Client	192.168.50.162	Reset issued at 2011-09-06 16:51:09 PDT
□	pcoip-portal-testbench-1 in Marketing	Zero Client	192.168.50.151	Reset issued at 2011-09-06 16:51:09 PDT

Scheduled Host Power State Change Commands

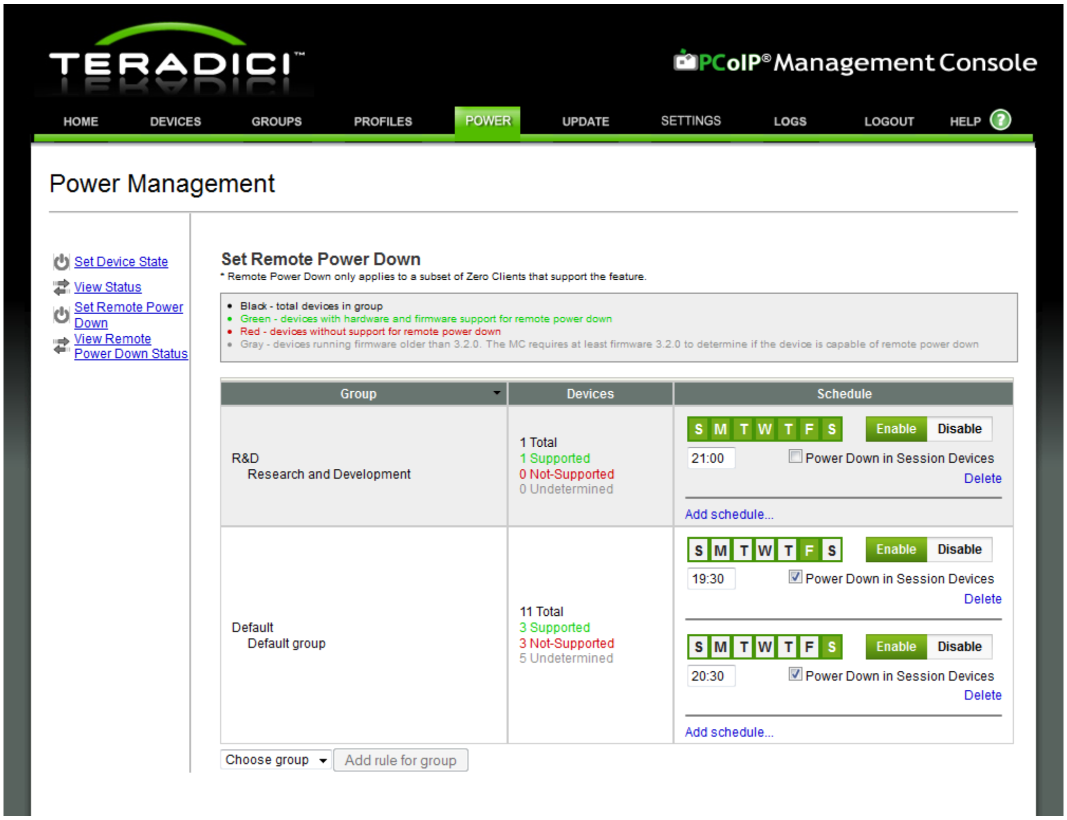
Select	Name and Group	IP Address	Reset Type	Shutdown Status
□	pcoip-host-0030040cf216 in Default	192.168.50.145	power off without OS involvement	Shutdown scheduled for 2011-09-27 16:55:00 PDT

Figure 4-29: Power Management Status Webpage

In addition to providing status information, you can cancel commands scheduled to be sent in the future from this webpage.

4.5.3 Schedule Remote Power Down

Click the **Set Remote Power Down** link on the **Power Management** webpage to schedule remote power down commands to be sent to zero client devices. When you click this link, the webpage shown in Figure 4-29 appears.



Power Management

Set Remote Power Down

* Remote Power Down only applies to a subset of Zero Clients that support the feature.

- Black - total devices in group
- Green - devices with hardware and firmware support for remote power down
- Red - devices without support for remote power down
- Gray - devices running firmware older than 3.2.0. The MC requires at least firmware 3.2.0 to determine if the device is capable of remote power down

Group	Devices	Schedule
R&D Research and Development	1 Total 1 Supported 0 Not-Supported 0 Undetermined	S M T W T F S Enable Disable 21:00 □ Power Down in Session Devices Delete Add schedule...
Default Default group	11 Total 3 Supported 3 Not-Supported 5 Undetermined	S M T W T F S Enable Disable 19:30 ☑ Power Down in Session Devices Delete S M T W T F S Enable Disable 20:30 ☑ Power Down in Session Devices Delete Add schedule...

Choose group ▾ Add rule for group

Figure 4-30: Set Remote Power Down Webpage

You can schedule remote powerdown by specifying day(s) of a week and time of a day. Ctrl-click on the day-selector to select multiple days in a single schedule. You can schedule different times for each day by adding more schedules.

Select the **Power Down in Session Devices** checkbox to set the schedule to force power down devices that are in session.

To enable the schedule, click the **Enable** button after configuring the day(s) and time.

Remote power down only applies to zero client devices with both hardware and firmware support. Hardware support for remote power down is available with firmware 3.2.0 or higher version.

The four device counters include:

- Black: The total number of devices
- **Green**: The number of devices with both hardware and firmware support
- **Red:** The number of devices without hardware support
- **Gray:** The number of devices without firmware support. The MC requires firmware 3.2.0 or higher to determine if the device can perform a remote power down.

After scheduling the power down, click the **View Remote Power Down** link on the left side of the screen to view the status of power down commands sent to zero client devices.

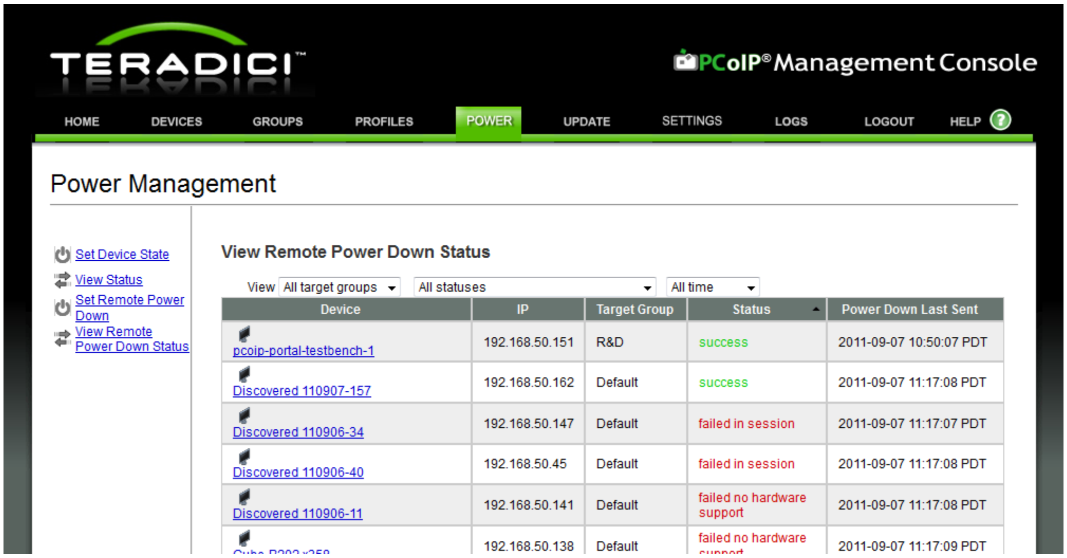
Note: The MC cannot power on the zero clients. Once the MC successfully powers off the zero clients, you (or your users) should manually power on the devices to respond to the MC again.

4.5.4 View Remote Power Down Status

The **View Remote Power Down Status** subcategory, shown in Figure 4-30, provides status information that shows if devices have been powered down.

The status categories include:

- **success**:The device was successfully powered down by MC.
- **failed error**: The device failed for a reason other than listed next.
- **failed offline**: The device could not be reached for power down.
- **failed no hardware support** – The device did not have hardware support.
- **failed no firmware support**: The device did not have firmware support.
- **failed in session**: The device was in session and the **Power Down in Session Devices** checkbox was turned off.



Power Management

View Remote Power Down Status

View All target groups All statuses All time

Device	IP	Target Group	Status	Power Down Last Sent
pcoip-portal-testbench-1	192.168.50.151	R&D	success	2011-09-07 10:50:07 PDT
Discovered 110907-157	192.168.50.162	Default	success	2011-09-07 11:17:08 PDT
Discovered 110906-34	192.168.50.147	Default	failed in session	2011-09-07 11:17:07 PDT
Discovered 110906-40	192.168.50.45	Default	failed in session	2011-09-07 11:17:08 PDT
Discovered 110906-11	192.168.50.141	Default	failed no hardware support	2011-09-07 11:17:08 PDT
Cube-R202-x258	192.168.50.138	Default	failed no hardware support	2011-09-07 11:17:09 PDT

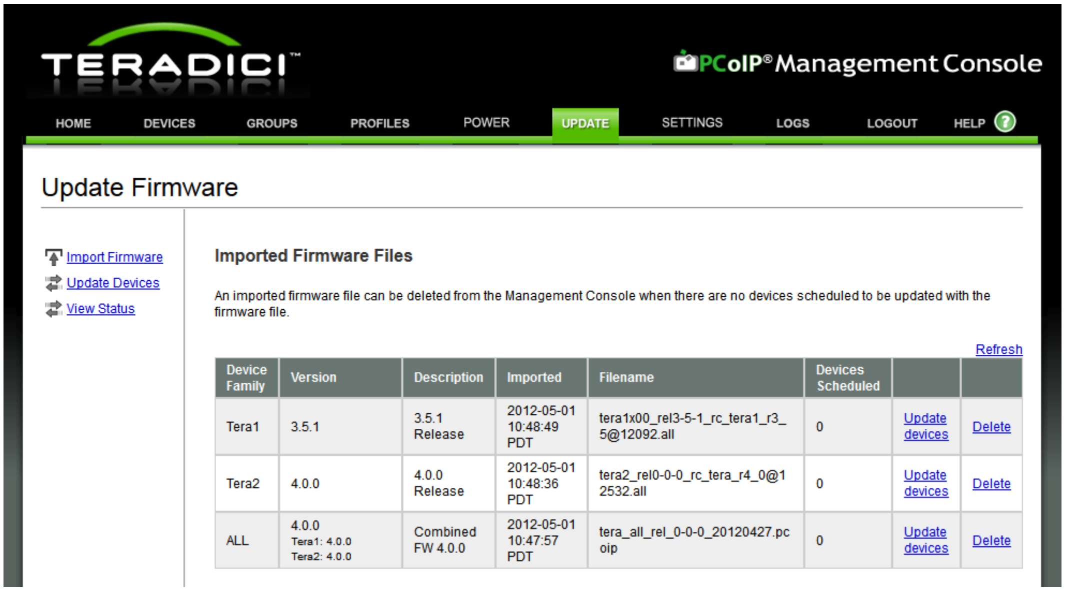
Figure 4-31: View Remote Power Down Status Webpage

4.6 Update Firmware

The **Update Firmware** webpage, shown in Figure 4-32, lets you update the firmware running on PCoIP devices.

The **Update Firmware** webpage lets you:

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



Update Firmware

Imported Firmware Files

An imported firmware file can be deleted from the Management Console when there are no devices scheduled to be updated with the firmware file.

Device Family	Version	Description	Imported	Filename	Devices Scheduled		
Tera1	3.5.1	3.5.1 Release	2012-05-01 10:48:49 PDT	tera1x00_rel3-5-1_rc_tera1_r3_5@12092.all	0	Update devices	Delete
Tera2	4.0.0	4.0.0 Release	2012-05-01 10:48:36 PDT	tera2_rel0-0-0_rc_tera_r4_0@12532.all	0	Update devices	Delete
ALL	4.0.0 Tera1: 4.0.0 Tera2: 4.0.0	Combined FW 4.0.0	2012-05-01 10:47:57 PDT	tera_all_rel_0-0-0_20120427.pcoip	0	Update devices	Delete

Figure 4-32: Update Firmware Webpage

4.6.1 Import Firmware

Click the **Import Firmware** link to transfer a firmware release file from the host machine to the MC VM. When prompted, 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. Delete old firmware releases if this limit is reached and you need to import additional firmware releases.

The MC supports following firmware file types:

- .all file: Firmware file
- .pcoip file: Firmware file containing both Tera1 and Tera2 firmware

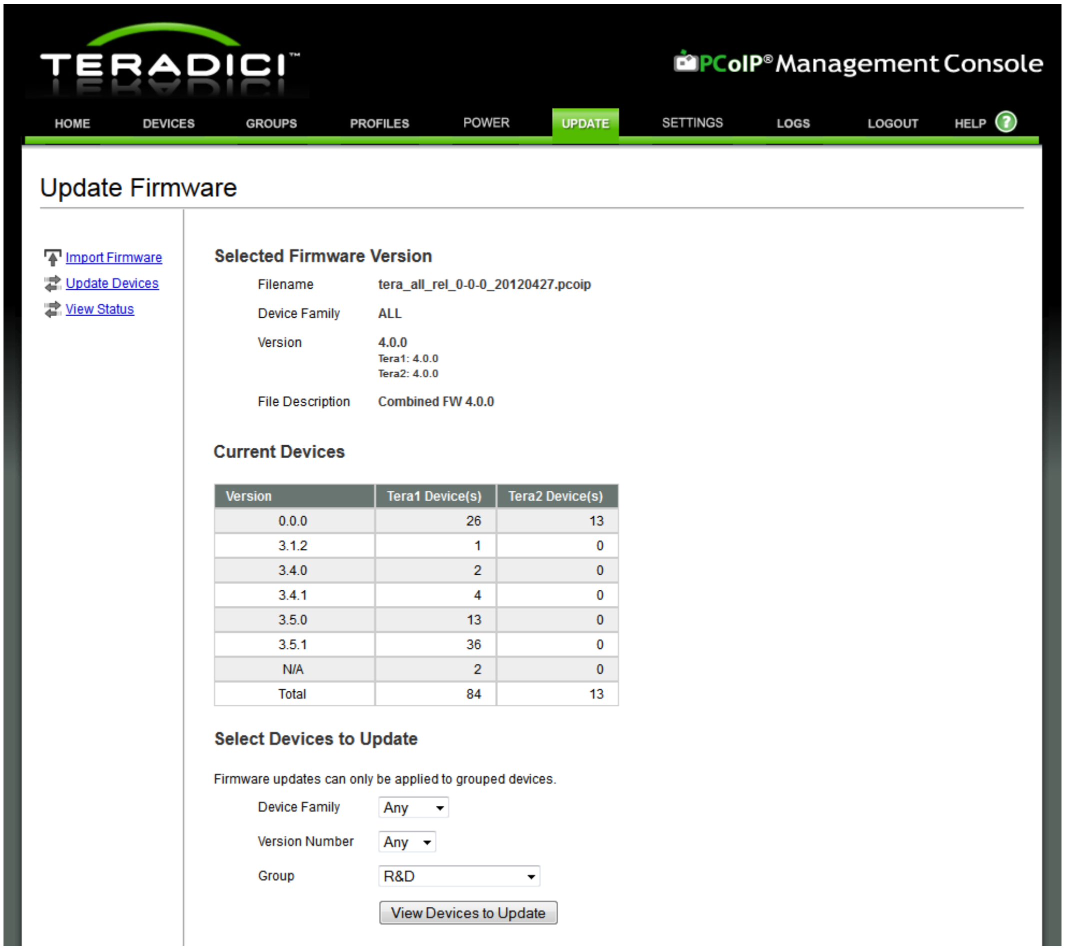
4.6.2 Update Device Firmware

Click the **Update Devices** link next to an imported firmware release to specify the devices to update and the time the update takes place. This lets you schedule firmware updates to take place at night. Figure 4-33 shows the **Update Devices** webpage.

This webpage displays:

- the firmware version and the device family type to download, shown under the **Selected Firmware Version** text
- a table with summary information about the firmware versions running on the **Current Devices** managed by the MC

Use the **Version Number** and **Group Name** dropdown menus to update specific groups of devices and/or devices loaded with specific versions of firmware.



Update Firmware

Selected Firmware Version

Filename	tera_all_rel_0-0-0_20120427.pcoip
Device Family	ALL
Version	4.0.0 Tera1: 4.0.0 Tera2: 4.0.0
File Description	Combined FW 4.0.0

Current Devices

Version	Tera1 Device(s)	Tera2 Device(s)
0.0.0	26	13
3.1.2	1	0
3.4.0	2	0
3.4.1	4	0
3.5.0	13	0
3.5.1	36	0
N/A	2	0
Total	84	13

Select Devices to Update

Firmware updates can only be applied to grouped devices.

Device Family	Any
Version Number	Any
Group	R&D

Figure 4-33: Initial Update Devices Webpage

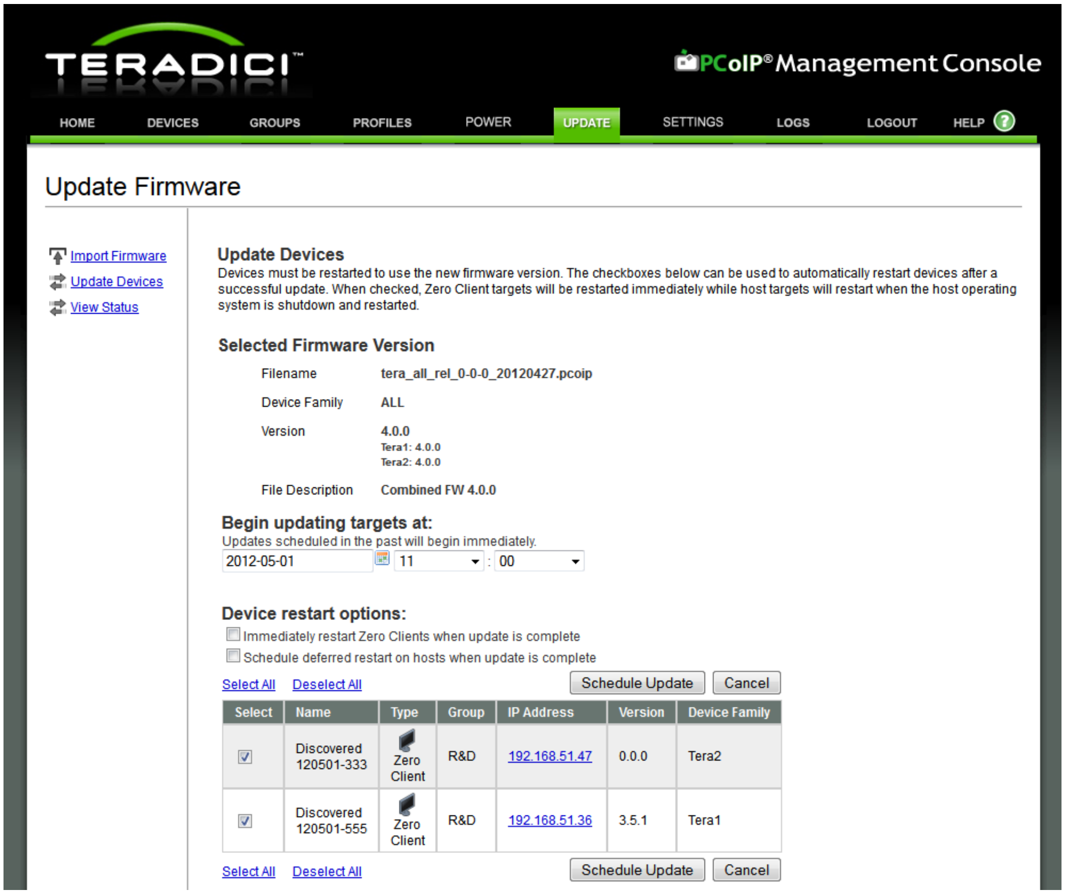
Click the **View Devices to Update** button to display the second update devices webpage that lists the devices that match the specified version number and group name. This new page is shown in Figure 4-33.

This webpage lets you specify the time the update occurs with the fields under the **Begin updating targets at** text.

You can specify the reset options you want 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 triggers a reset the next time the host operating systems shuts down

You must also specify the devices to update by checking the boxes next to the devices you want to update. After the options are configured, click the **Schedule Update** link to initiate the firmware update.



Update Firmware

Update Devices

Devices must be restarted to use the new firmware version. The checkboxes below can be used to automatically restart devices after a successful update. When checked, Zero Client targets will be restarted immediately while host targets will restart when the host operating system is shutdown and restarted.

Selected Firmware Version

Filename	tera_all_rel_0-0-0_20120427.pcoip
Device Family	ALL
Version	4.0.0 Tera1: 4.0.0 Tera2: 4.0.0
File Description	Combined FW 4.0.0

Begin updating targets at:

Updates scheduled in the past will begin immediately.

2012-05-01 11 : 00

Device restart options:

□ Immediately restart Zero Clients when update is complete

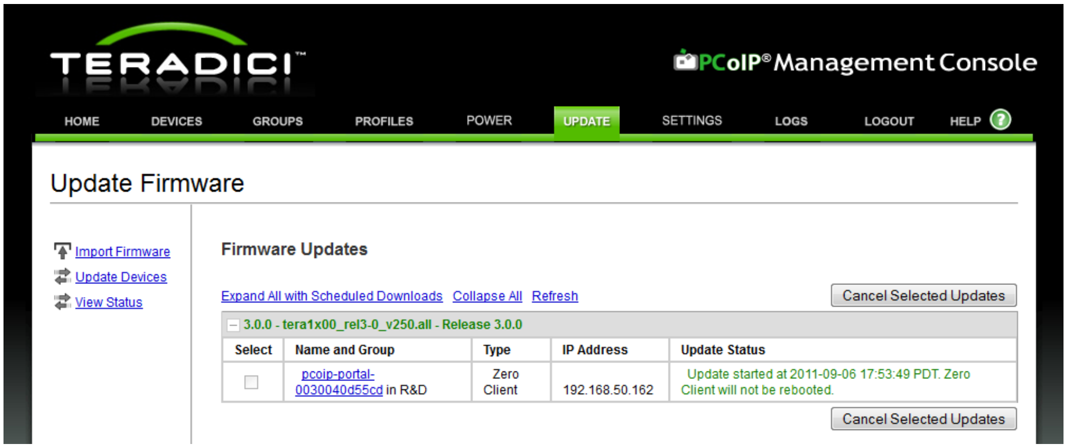
□ Schedule deferred restart on hosts when update is complete

Select	Name	Type	Group	IP Address	Version	Device Family
☑	Discovered 120501-333	Zero Client	R&D	192.168.51.47	0.0.0	Tera2
☑	Discovered 120501-555	Zero Client	R&D	192.168.51.36	3.5.1	Tera1

Figure 4-34: Second Update Devices Webpage

4.6.3 View Status

Click the **View Status** link to view the current status of all scheduled and completed firmware updates. Figure 4-34 shows the **Firmware Update Status** webpage.



Update Firmware

Firmware Updates

3.0.0 - tera1x00_rel3-0_v250.all - Release 3.0.0

Select	Name and Group	Type	IP Address	Update Status
□	pcoip-portal-0030040d55cd in R&D	Zero Client	192.168.50.162	Update started at 2011-09-06 17:53:49 PDT. Zero Client will not be rebooted.

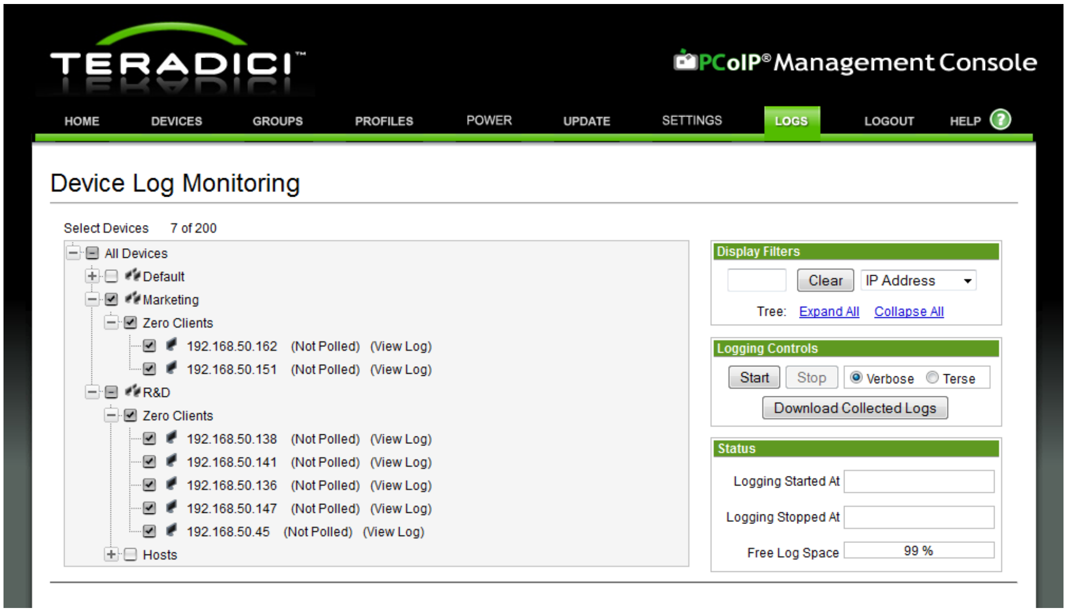
Figure 4-35: Firmware Update Status Webpage

4.7 Device Log Monitoring

The **Device Log Monitoring** webpage, shown in Figure 4-35, lets you collect logs over time from a selection of PCoIP devices.

The **Device Log Monitoring** webpage lets you:

- 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



Device Log Monitoring

Select Devices 7 of 200

- ⊟ All Devices
  - ⊞ □ Default
  - ⊟ ☑ Marketing
    - ⊟ ☑ Zero Clients
      - ☑ 192.168.50.162 (Not Polled) (View Log)
      - ☑ 192.168.50.151 (Not Polled) (View Log)
  - ⊟ ⊟ R&D
    - ⊟ ☑ Zero Clients
      - ☑ 192.168.50.138 (Not Polled) (View Log)
      - ☑ 192.168.50.141 (Not Polled) (View Log)
      - ☑ 192.168.50.136 (Not Polled) (View Log)
      - ☑ 192.168.50.147 (Not Polled) (View Log)
      - ☑ 192.168.50.45 (Not Polled) (View Log)
    - ⊞ □ Hosts

● Verbose ○ Terse

Logging Started At

Logging Stopped At

Free Log Space 99 %

Figure 4-36: Device Log Monitoring Webpage

4.7.1 Device Tree

The device tree displays grouped devices and lets you select which devices are monitored. When you use the checkboxes for individual devices, you can select all zero clients or hosts within a group, an entire group, or all grouped devices for monitoring. Once log monitoring is started, you cannot change the selection until it is stopped. The same display filters that appear in the **Devices** page are included here.

You can enable up to 200 devices for log monitoring at a time.

4.7.2 Logging Controls

After you select the devices using the device tree, you can set the event log filter mode to verbose or terse. This setting overrides 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 is overwritten to the setting made here the next time logs are retrieved by the log monitoring process.

To begin monitoring logs, click **Start**. This empties the MC’s storage of any previously collected logs and starts the log monitoring process. You cannot change the selection of devices being monitored and the event log filter mode until log monitoring is stopped. An attempt to collect logs is made every 300 seconds.

Click the **Download Collected Logs** button to format the logs collected into individual .txt files per device, archive the logs into .tar.gz format, and present them as a downloadable file.

When log monitoring is no longer needed, click **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 clicked remain available for download until you click **Start** again.

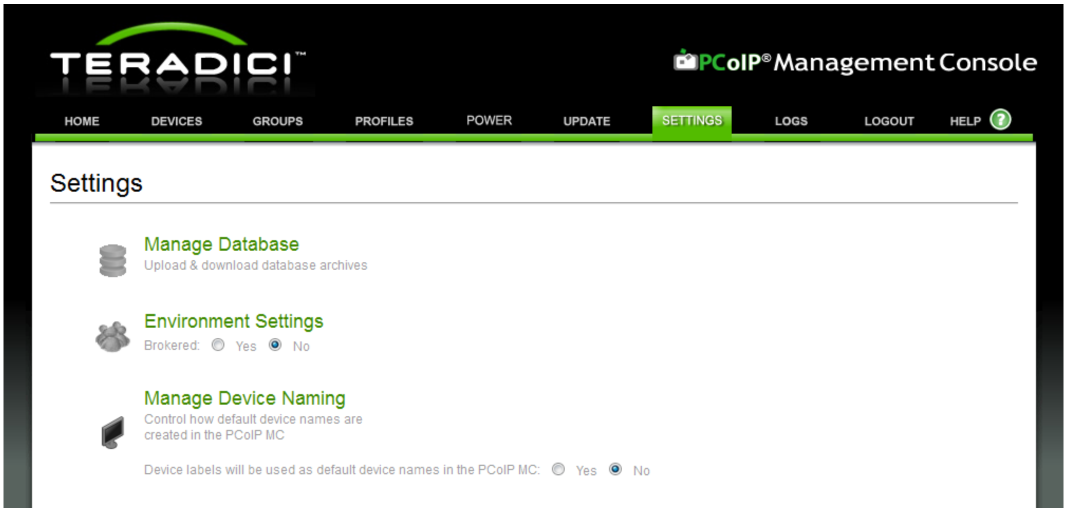
4.7.3 Status

Localized date/time stamps appear when log monitoring was started and stopped. Log monitoring in the MC has a finite storage limit which appears 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 is overwritten with new log data. It's a good idea to check this display periodically.

4.8 Manage Settings

The **Settings** webpage, shown in Figure 4-36, lets you:

- Upload and download MC database archive files
- Configure MC environment settings
- Manage device naming



Settings

Manage Database
Upload & download database archives

Environment Settings
Brokered: ○ Yes ● No

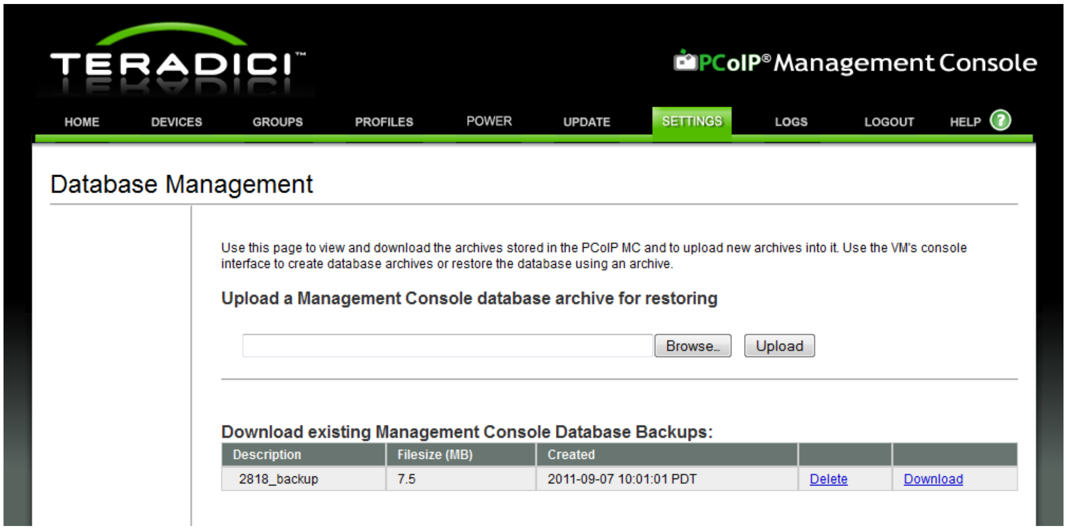
Manage Device Naming
Control how default device names are created in the PCoIP MC

Device labels will be used as default device names in the PCoIP MC: ○ Yes ● No

Figure 4-37: Settings Webpage

4.8.1 Database Management

Click the **Manage Database** link on the **Settings** webpage to upload and download database files from the MC VM. When you click this link, the webpage shown in Figure 4-37 appears.



Database Management

Use this page to view and download the archives stored in the PCoIP MC and to upload new archives into it. Use the VM's console interface to create database archives or restore the database using an archive.

Upload a Management Console database archive for restoring

Download existing Management Console Database Backups:

Description	Filesize (MB)	Created		
2818_backup	7.5	2011-09-07 10:01:01 PDT	Delete	Download

Figure 4-38: Database Management Webpage

Uploading a Database

Click **Browse** and **Upload** to transfer a database archive from the host PC running the web browser to the MC VM. Click **Browse**, and then select the database archive to upload. Click **Upload** to start the transfer of the database file into the VM.

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

Downloading a Database

Click the **Download** link to transfer a database archive from the MC VM to the host PC running the web browser. When you click this link, you must select the destination directory to download the archive to.

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

4.8.2 Environment Settings

Set the **Brokered configuration** setting shown in Figure 4-36 to:

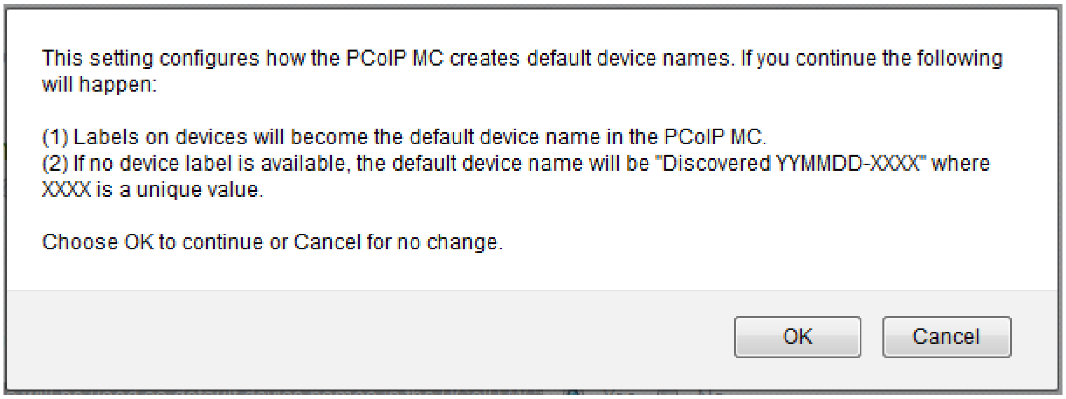
- **Yes:** If the deployment is using a connection broker to manage host and zero client peerings.
- **No:** If the deployment uses the MC to manage the host and zero client peerings.

Note: The **Link devices** button on the **Device Management** page is disabled when this setting is set to **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 configuration** setting is changed from **No** to **Yes,** the MC deletes peering information from its database. If you later change the setting to **No,** you must link the host and zero clients again. When re-enabling the old peerings, back up the database before you change the setting to **Yes**.

4.8.3 Manage Device Naming

The device labels used as default device names in the PCoIP MC configuration setting, lets you name newly discovered devices with their labels. By default this setting is disabled and devices are named as “Discovered YYMMDD-XXXX” where XXXX is a unique value. Figure 4-38 shows the confirmation dialog that appears once the setting is enabled.



This setting configures how the PCoIP MC creates default device names. If you continue the following will happen:

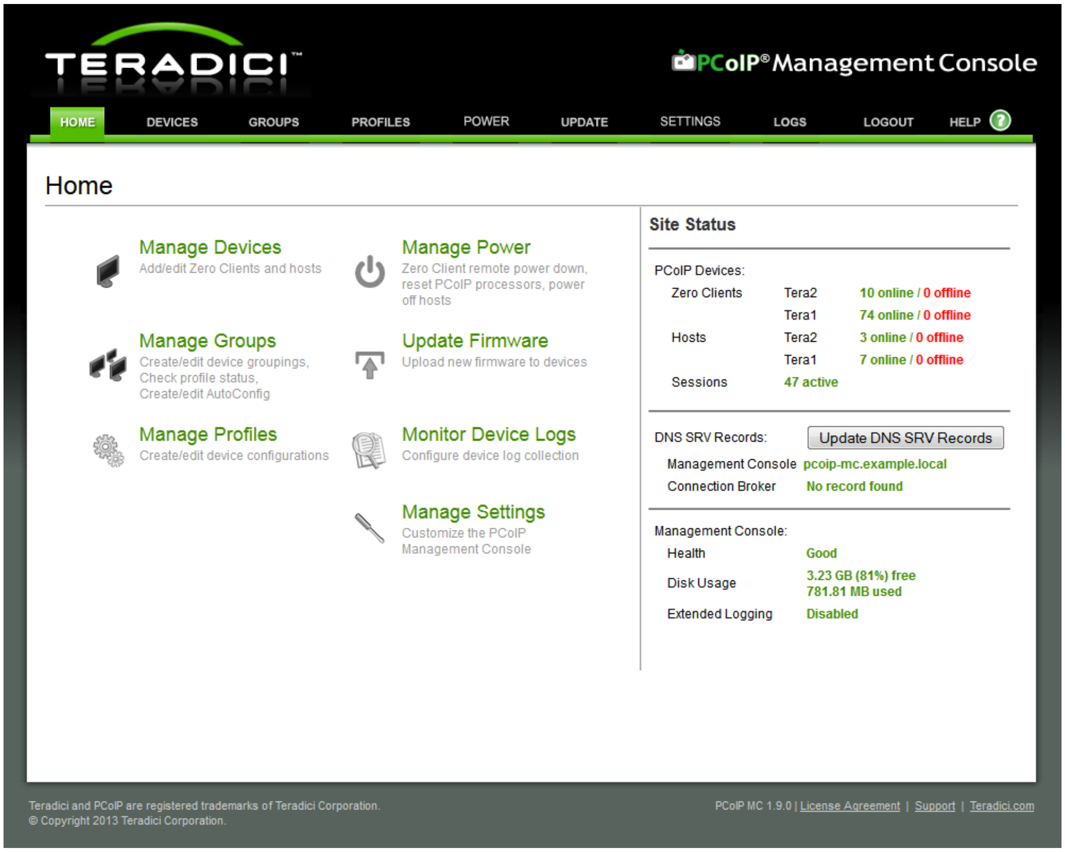
(1) Labels on devices will become the default device name in the PCoIP MC.
(2) If no device label is available, the default device name will be "Discovered YYMMDD-XXXX" where XXXX is a unique value.

Choose OK to continue or Cancel for no change.

Figure 4-39: Manage Device Naming Dialog

4.9 Site Status

The right side of the **Home** webpage displays summary information on the PCoIP devices discovered by the MC.



Home

Manage Devices
Add/edit Zero Clients and hosts

Manage Power
Zero Client remote power down, reset PCoIP processors, power off hosts

Manage Groups
Create/edit device groupings, Check profile status, Create/edit AutoConfig

Update Firmware
Upload new firmware to devices

Manage Profiles
Create/edit device configurations

Monitor Device Logs
Configure device log collection

Manage Settings
Customize the PCoIP Management Console

Site Status

PCoIP Devices:

Zero Clients	Tera2	10 online / 0 offline
	Tera1	74 online / 0 offline
Hosts	Tera2	3 online / 0 offline
	Tera1	7 online / 0 offline
Sessions	47 active	

DNS SRV Records:

Management Console	pcoip-mc.example.local
Connection Broker	No record found

Management Console:

Health	Good
Disk Usage	3.23 GB (81%) free 781.81 MB used
Extended Logging	Disabled

Teradici and PCoIP are registered trademarks of Teradici Corporation.
© Copyright 2013 Teradici Corporation.

PCoIP MC 1.9.0 | License Agreement | Support | Teradici.com

Figure 4-40: Home Webpage

The following status information appears:

- 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 4 GB of disk space. When the usage begins to approach this limit, the status turns red indicating that you 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 when:

- You click **Update** on the **Device Details** webpage
- Once an hour if the device is online
- Once every 15 minutes if the device if offline
- After a firmware update if the deployment has a MC DNS SRV record. If the record does not exist, the device is 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.

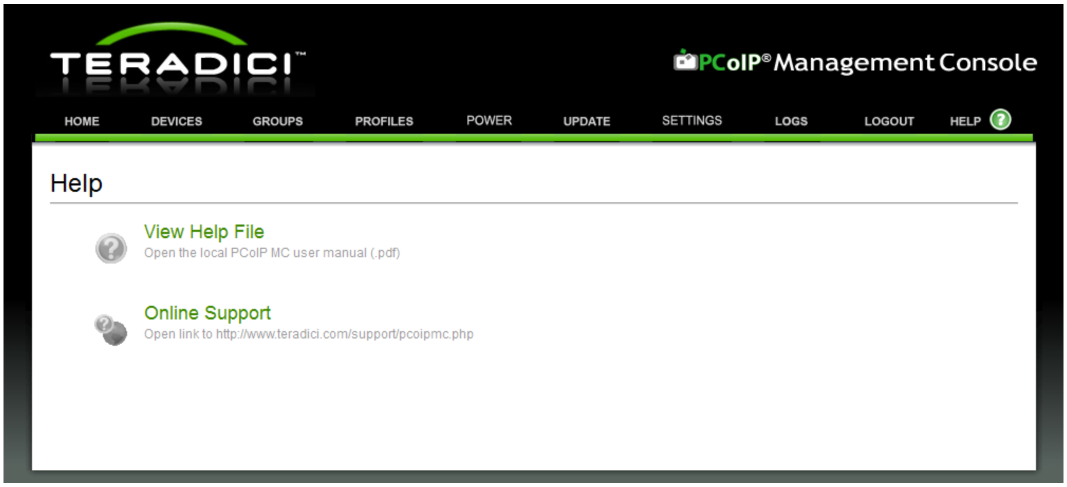
Note: Site status information is updated when you reload the **Home** webpage. The MC checks the DNS SRV records every five minutes or when you click the **Update DNS SRV Records** button on the **Home** webpage.

4.10 Online Help

MC webpages include a **HELP** link in the upper right-hand corner. When you click this link, a help screen (as shown in Figure 4-40) appears. This webpage has two links that 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 web-site. The URL for this site is http://www.teradici.com/support/pcoipmc.php.

Note: You can also access the online support link by clicking the **Support** link at the bottom of any of the MC webpages.



Help

View Help File

Open the local PCoIP MC user manual (.pdf)

Online Support

Open link to http://www.teradici.com/support/pcoipmc.php

Figure 4-41: Help Webpage

5 Getting Started

This section provides instructions on how to begin using the MC. After completing the following steps, you can 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 2.3 or 2.4 to install the MC, and then read section 2.5 to start using it. Doing these steps activate the MC VM on the MC host machine.

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

5.2 Discover Devices

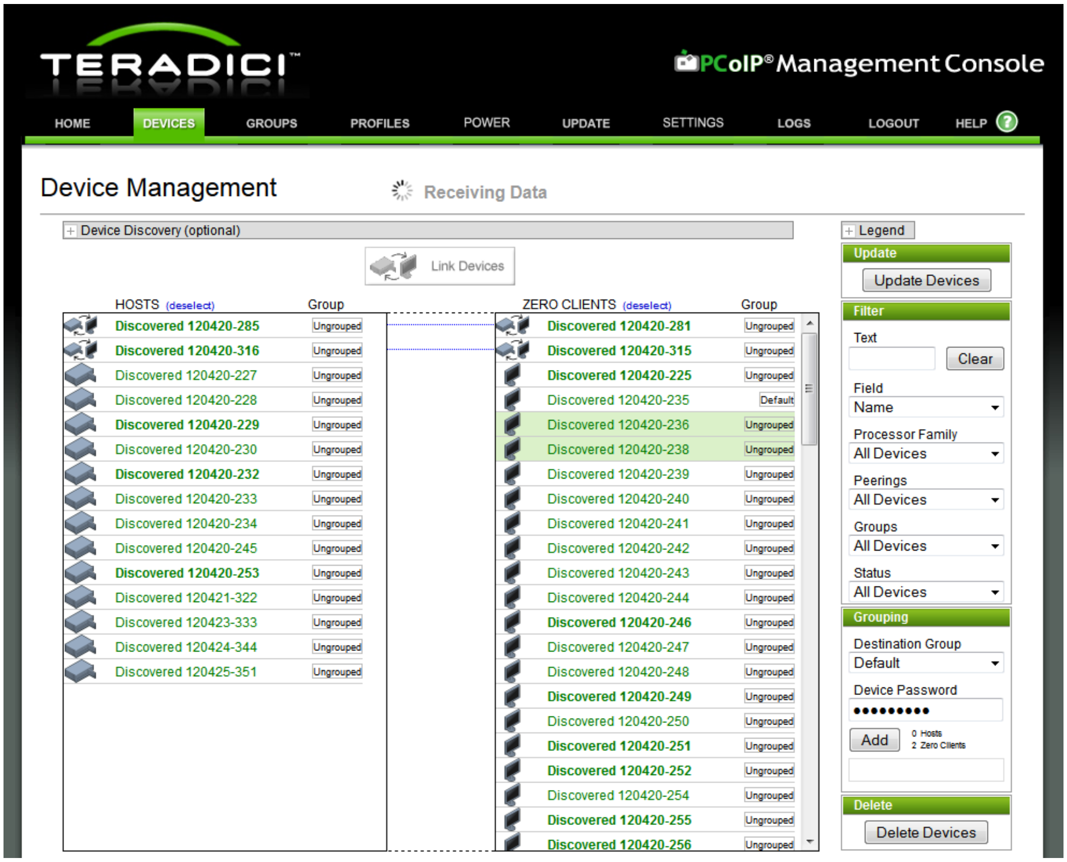
Open the **MC Device Management** webpage. Verify the MC has discovered the devices you want to link (peer). If the devices are not discovered, use the **Manual Device Discovery** feature to discover the devices. The **Manual Device Discovery** feature is described in section 1.3.3.3.

5.3 Adding Devices to a Group

Once the PCoIP devices are discovered, you must add them to a group through the **Device Management** webpage, see Figure 5-1. The following process is an example of the steps you would take to add two zero clients to the **Default** group.

To add two zero clients to the **Default** group:

1. Open the **MC Device Management** webpage.
2. While pressing the “Shift” key, click the devices you want to add to a group. The selected devices are highlighted.
3. From the **Destination Group** dropdown menu on the right-hand side of the screen, select the group you want to add the devices to. In this example, 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, the devices are assigned the same password. It’s a good idea to assign the same password to all devices in your deployment.
5. Click **Add**. The MC adds the selected devices to the R&D group.



Device Management

Device Discovery (optional)

HOSTS (deselect)	Group
Discovered 120420-285	Ungrouped
Discovered 120420-316	Ungrouped
Discovered 120420-227	Ungrouped
Discovered 120420-228	Ungrouped
Discovered 120420-229	Ungrouped
Discovered 120420-230	Ungrouped
Discovered 120420-232	Ungrouped
Discovered 120420-233	Ungrouped
Discovered 120420-234	Ungrouped
Discovered 120420-245	Ungrouped
Discovered 120420-253	Ungrouped
Discovered 120421-322	Ungrouped
Discovered 120423-333	Ungrouped
Discovered 120424-344	Ungrouped
Discovered 120425-351	Ungrouped

ZERO CLIENTS (deselect)	Group
Discovered 120420-281	Ungrouped
Discovered 120420-315	Ungrouped
Discovered 120420-225	Ungrouped
Discovered 120420-235	Default
Discovered 120420-236	Ungrouped
Discovered 120420-238	Ungrouped
Discovered 120420-239	Ungrouped
Discovered 120420-240	Ungrouped
Discovered 120420-241	Ungrouped
Discovered 120420-242	Ungrouped
Discovered 120420-243	Ungrouped
Discovered 120420-244	Ungrouped
Discovered 120420-246	Ungrouped
Discovered 120420-247	Ungrouped
Discovered 120420-248	Ungrouped
Discovered 120420-249	Ungrouped
Discovered 120420-250	Ungrouped
Discovered 120420-251	Ungrouped
Discovered 120420-252	Ungrouped
Discovered 120420-254	Ungrouped
Discovered 120420-255	Ungrouped
Discovered 120420-256	Ungrouped

Update

Filter
Text:
Field: Name
Processor Family: All Devices
Peerings: All Devices
Groups: All Devices
Status: All Devices

Grouping
Destination Group: Default
Device Password: ●●●●●●●●●
0 Hosts
2 Zero Clients

Delete

Figure 5-1: Adding Devices to a Group

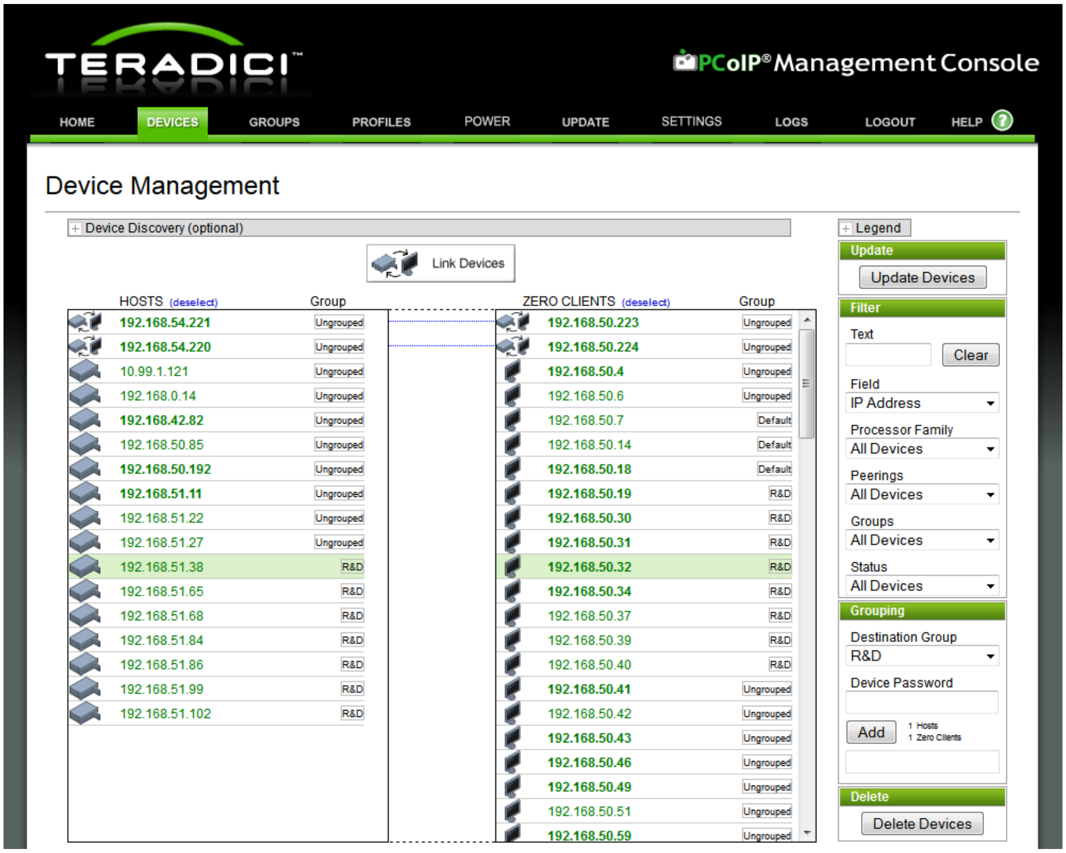
Note: After a device is successfully added to a group, the group name appears in the **Group** column for each device. In Figure 5-1, the first zero client device is part of the **Default** group and the third zero client device is not part of a group.

5.4 Peering Devices

You can peer (or link together) each pair of host and zero client devices. After a host and zero client are peered, a PCoIP session can be started from the zero client. To start a PCoIP session, the end user must click the **Connect** button on the zero client OSD.

To peer (link) pairs of host and zero client devices:

1. Open the **MC Device Management** webpage.
2. Select the host and zero client devices to be peered. In Figure 5-2 the devices 192.168.51.38 and 192.168.50.32 are selected.
3. Click the **Link Devices** button to peer the devices. The zero client connects to the host 192.168.51.38 when the end user clicks **Connect** on the zero client OSD.



Device Management

HOSTS (deselect)	Group
192.168.54.221	Ungrouped
192.168.54.220	Ungrouped
10.99.1.121	Ungrouped
192.168.0.14	Ungrouped
192.168.42.82	Ungrouped
192.168.50.85	Ungrouped
192.168.50.192	Ungrouped
192.168.51.11	Ungrouped
192.168.51.22	Ungrouped
192.168.51.27	Ungrouped
192.168.51.38	R&D
192.168.51.65	R&D
192.168.51.68	R&D
192.168.51.84	R&D
192.168.51.86	R&D
192.168.51.99	R&D
192.168.51.102	R&D

ZERO CLIENTS (deselect)	Group
192.168.50.223	Ungrouped
192.168.50.224	Ungrouped
192.168.50.4	Ungrouped
192.168.50.6	Ungrouped
192.168.50.7	Default
192.168.50.14	Default
192.168.50.18	Default
192.168.50.19	R&D
192.168.50.30	R&D
192.168.50.31	R&D
192.168.50.32	R&D
192.168.50.34	R&D
192.168.50.37	R&D
192.168.50.39	R&D
192.168.50.40	R&D
192.168.50.41	Ungrouped
192.168.50.42	Ungrouped
192.168.50.43	Ungrouped
192.168.50.46	Ungrouped
192.168.50.49	Ungrouped
192.168.50.51	Ungrouped
192.168.50.59	Ungrouped

Text

Field: IP Address

Processor Family: All Devices

Peerings: All Devices

Groups: All Devices

Status: All Devices

Destination Group: R&D

Device Password

1 Hosts
1 Zero Clients

Figure 5-2: Peering a Pair of Devices

5.5 Configuring Zero Clients for VMware View

You can configure zero clients for VMware View. After a zero client is configured, a PCoIP session can be started from the zero client. To start a PCoIP session, the end user must click the **Connect** button on the zero client OSD.

To configure zero clients for VMware View:

1. Open the **MC Profile Management** webpage.
2. Click the **Add New** button to create a new profile.
3. After creating a new profile click the **Set Properties** link to configure the properties.
4. Click on the **Session Configuration** tab to expand it and click on the **Edit Properties** to bring up the **Set Properties** dialog.
5. Click and enable the **Set in Profile** checkbox for **Session Connection Type**.
6. Select **View Connection Server** in the **Session Connection Type** dropdown menu. Now you will see all the settings for the VMware View connection server.
7. Click and enable the **Set in Profile** checkbox for **View Connection Server Address** and type in the server address in the value field.
8. Optionally you can also set the **Certification Check Mode.**
9. Scroll to the bottom of the dialog and click the **Save** button

10. Depending on the **Certification Check Mode** and the server configuration a valid certificate must be presented by the zero client. Click **Add New** button in the **Certificate Store** tab to upload and assign a certificate file to the profile.
    Note: See Knowledge Base 15134-1020 for details on downloading the View Connection Server trusted root certificate.
11. Go to the **Group Management** webpage by clicking the **GROUPS** tab.
12. Click the **Edit** link for the **Default** group and select the profile in the dropdown menu.
13. Once you assign the profile to the **Default** group click the **Apply Profile** link to change settings on all devices in the **Default** group.

5.6 Familiarizing Yourself with the MC

To become more familiar with the MC:

1. Review section 1of this document to become familiar with the different components in a PCoIP deployment. This section also describes some fundamental concepts to be aware of to use the MC.
2. Update the time zone of the MC using the VM Console interface. See section 3.6.
3. Create a profile and set one or more properties within the profile. A good parameter to use to try this out on is the **Language** field in the **Language Configuration** settings. See section 4.4 for details.
4. Create a group and assign the profile created in the previous step to the new group. See section 4.3.
5. Assign some devices to the new group. See section 4.2.5.
6. Write the profile settings to the devices in the group and verify the settings were written to the devices. See sections 4.3.1.5 and 4.3.2.
7. 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 simple parameter. See sections 4.3.3 and 4.3.4.
8. Query and view the current device settings. See section 4.2.9.
9. Query and view the data stored in the device event log. Sections 4.2.9 and 4.2.10.6 describe two different ways of doing this.
10. Download new firmware to a device. See section 4.6.
11. Send reset commands to a device, and then view power management status information. See section 4.5.
12. Back up the MC database, and then download it from the MC VM to an external server. See sections 3.5.1 and 4.8.1.
13. Upload a backed up copy of the MC database to the MC VM, and then restore the active database from the uploaded file. See sections 3.5.2 and 4.8.1.