



# Service Managed Gateway™

## Polycom Phone Provisioning on a Teleware Platform

Issue 0.3  
Date 10 December 2008

|            |  |           |
|------------|--|-----------|
| <b>1</b>   | <b>About this document .....</b>             | <b>3</b>  |
| <b>1.1</b> | <b>Scope .....</b>                           | <b>3</b>  |
| <b>1.2</b> | <b>Readership .....</b>                      | <b>3</b>  |
| <b>1.3</b> | <b>Terminology .....</b>                     | <b>3</b>  |
| <b>2</b>   | <b>Configuring the SMG.....</b>              | <b>4</b>  |
| <b>2.1</b> | <b>DHCP option 66 .....</b>                  | <b>4</b>  |
| <b>2.2</b> | <b>Event filter .....</b>                    | <b>5</b>  |
| 2.2.1      | Create an event filter .....                 | 5         |
| 2.2.2      | Configure the IP address for Activator ..... | 7         |
| 2.2.3      | Configure log Activator events .....         | 8         |
| 2.2.4      | Configure MAC alerts .....                   | 9         |
| <b>3</b>   | <b>Polycom phone provisioning.....</b>       | <b>12</b> |
| <b>3.1</b> | <b>Creating a phone account.....</b>         | <b>12</b> |
| <b>3.2</b> | <b>Linking to DHCP .....</b>                 | <b>12</b> |
| <b>3.3</b> | <b>HTTP operation .....</b>                  | <b>12</b> |

Copyright 2008 Virtual Access (Irl) Ltd. This material is protected by copyright. No part of this material may be reproduced, distributed, or altered without the written consent of Virtual Access. All rights reserved. Third party trademarks are the property of the third parties.

# 1 About this document

## 1.1 Scope

This document describes:

- how to automatically provision a Polycom handset on a Teleware platform
- the applicable form fields and their CLI commands

## 1.2 Readership

This document is for Virtual Access' operation and support teams deploying Polycom handsets on a Teleware platform.

## 1.3 Terminology

|      |                                     |
|------|-------------------------------------|
| DHCP | Dynamic Host Configuration Protocol |
| HTTP | Hypertext Transfer Protocol         |
| SMG  | Service Managed Gateway             |

## 2 Configuring the SMG

To enable Polycom IP handsets to provision against a Teleware platform, you must set four router configuration parameters: a DHCP option 66, an event filter, a MAC alert, and an HTTP client pointing to Teleware Activator.

### 2.1 DHCP option 66

Polycom phones have DHCP enabled as their default factory setting. When each phone initially boots up it receives an IP address from the Service Managed Gateway (SMG).

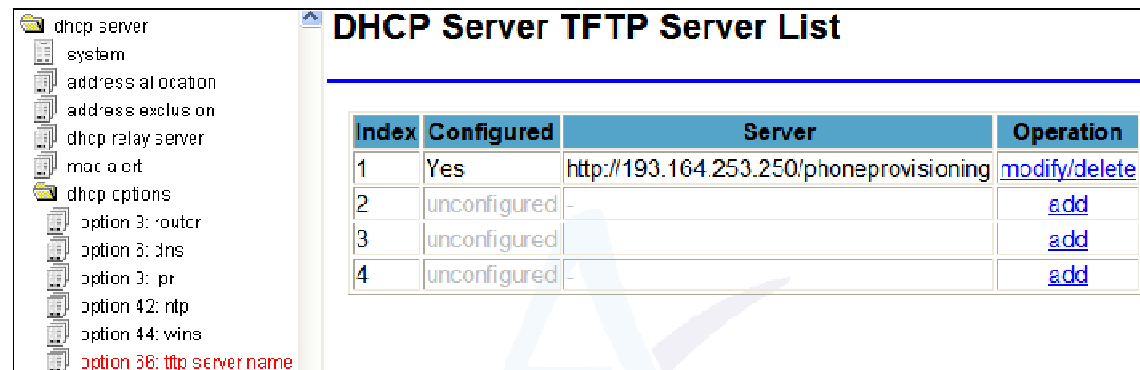
As part of the DHCP parameters passed down by the SMG, the phone receives option 66. This tells the phone which server to contact to download its files to and also which protocol to use.

Option 66 is a string that contains the IP address of the server the phones need to access.

The DHCP TFTP Server Name is used to enable or disable the offering of DHCP option 66 TFTP Server Name. This can be a domain name or IP address, as part of a DHCP offer. You can configure one or more DHCP TFTP Server Names.

To configure option 66, from the SMG homepage, click **Advanced**.

In the Advanced menu, click **Expert View -> system -> local servers -> dhcp server -> dhcp options -> option 66: tftp server name**. The DHCP Server List appears.



| Index | Configured   | Server                                   | Operation                     |
|-------|--------------|--|-------------------------------|
| 1     | Yes          | http://193.164.253.250/phoneprovisioning | <a href="#">modify/delete</a> |
| 2     | unconfigured | -  | <a href="#">add</a>           |
| 3     | unconfigured | -  | <a href="#">add</a>           |
| 4     | unconfigured | -  | <a href="#">add</a>           |

Figure 1: The DHCP server TFTP server list

In the Operation column, click **add** in the row of the entry you want to configure option 66. The DHCP Server TFTP Server Entry page appears.

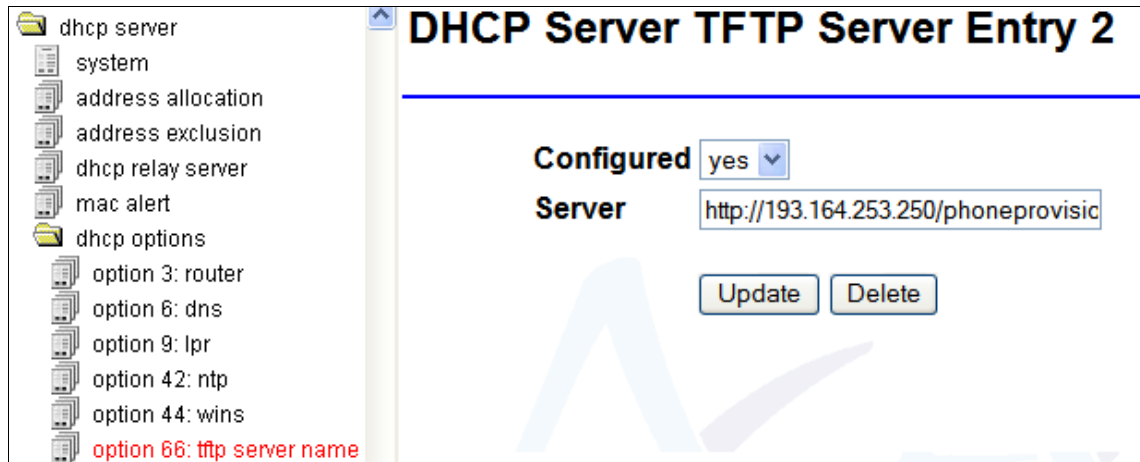


Figure 2: The DHCP server TFTP server entry page

| Field             | Description   | CLI command  |
|-------------------|---|--|
| <b>Configured</b> | Enables or disables a configured TFTP Server Name.<br><b>Option</b> <b>Description</b><br><b>yes</b> Enables the TFTP Sever Name Option<br><b>no</b> Disables the TFTP Sever Name Option                              | Dhcp Server Tftp Server Configured                                     |
| <b>Server</b>     | Specifies the Domain Name or IP Address of the TFTP Server<br><b>Option</b> <b>Description</b><br><b>Minimum length</b> 0<br><b>Default value</b> Unspecified<br><b>Maximum length</b> 63<br><b>Units</b> Unspecified | Set DHCP server TFTP server 1,http://193.164.253.250/phoneprovisioning |

Table 1: The DHCP server entry page and their descriptions and CLI commands

## 2.2 Event filter

The Event Filtering form is used to specify the filtering criteria and, when the event matches the filtering criteria, you can selectively log the event to the router, an SNMP manager, or both. The definitions of Severity Criterion, Event Class, and Severity create the filtering criteria.

### 2.2.1 Create an event filter

You must create an event filter to send an event to Activator.

To create an event filter, click **Advanced**. In the Advanced menu, click **Expert View -> system -> events -> event filter**. The Events Filtering List appears.

| Index | Event Class  | Event Subclass | Target    | Operation                     |
|-------|--------------|----------------|-----------|-------------------------------|
| 1     | Script       | 9999           | Manager 1 | <a href="#">modify/delete</a> |
| 2     | DHCP         | 67             | Activator | <a href="#">modify/delete</a> |
| 3     | unconfigured | -              | -         | <a href="#">add</a>           |
| 4     | unconfigured | -              | -         | <a href="#">add</a>           |
| 5     | unconfigured | -              | -         | <a href="#">add</a>           |
| 6     | unconfigured | -              | -         | <a href="#">add</a>           |
| 7     | unconfigured | -              | -         | <a href="#">add</a>           |
| 8     | unconfigured | -              | -         | <a href="#">add</a>           |
| 9     | unconfigured | -              | -         | <a href="#">add</a>           |
| 10    | unconfigured | -              | -         | <a href="#">add</a>           |

Figure 3: The Events filtering list

In the Operation column, click **add** in the row of the entry you want to create an event filter for. The Event Filtering Entry page appears.

**Event Filtering Entry 3**

Event Class:

Event Subclass:

Target:

Severity Criterion:

Severity:

Figure 4: The event filtering entry page

In the Event Filtering Entry page, click **Advanced** to view all fields.

| Field                     | Description  | CLI command                                       |
|---------------------------|--|---|
| <b>Event Class</b>        | Defines the event class to filter. Select <b>DHCP</b> from the drop-down menu.   | Event Forwarding Discriminator Entry Class        |
| <b>Event Subclass</b>     | Forwards the event only if the event subclass matches the event subclass configured here.<br>The value is normally left the same as the default value. | Event Forwarding Discriminator Entry Subclass     |
| <b>Target</b>             | Defines the destination of the event. If the event meets the filtering criteria, select the destination of the event.                                  | Event Forwarding Discriminator Entry Target       |
| <b>Severity Criterion</b> | Defines options to filter the event based on the event severity.   | Set Event Forwarding Discriminator Entry Criteria |

|                 |   |   |
|-----------------|---|---|
| <b>Severity</b> | Defines the severity to use as the filtering criteria.<br>Severity levels are listed in order. Emergency is the highest severity and Debug-Level Messages is the lowest severity. | Set Event Forwarding Discriminator Entry Severity |
|-----------------|---|---|

**Table 2: The event filtering entry page fields, their descriptions and CLI commands**

Click **Update** to save the new event filter.

## 2.2.2 Configure the IP address for Activator

The HTTP Client is used to download files from a web server over HTTP and HTTPS. The HTTP client is primarily used to receive updates from Activator. The HTTP client can also send events to Activator over HTTP or HTTPS. You must set the IP address for Activator so the HTTP client can send events to the correct IP address.

To configure the IP address for Activator, click **Advanced**. In the Advanced menu, click **Expert View -> system -> local clients -> http client**. The HTTP Client page appears.

**Figure 5: The HTTP client page**

| Field                         | Description   | CLI command                            |
|-------------------------------|---|--|
| <b>Enabled</b>                | Enables or disables the HTTP client.  | Set Http Client Enabled                |
| <b>File Server IP Address</b> | The file server IP address is the address of the web server from which the client will retrieve files and to which it will send events. | Set Http Client File Server Ip Address |
| <b>Download Path</b>          | The download path is pre-pended to the filename entered in hdl. This is not carried   | Set Http Client Download Path          |

|                                | out if the filename contains \$\$ or if begins with a /.   |   |             |            |                      |           |                     |                                 |
|--------------------------------|--|---|-------------|------------|----------------------|-----------|---------------------|---------------------------------|
| <b>Events Path</b>             | Specifies the full URL to which events are to be sent, such as:<br>/activator/eventHandler.asp.  | Set Http Client Events Path             |             |            |                      |           |                     |                                 |
| <b>Activator Download Path</b> | Specifies the full URL to which Activator download requests are to be issued, such as:<br>/activator/fileServer.asp.   | Set Http Client Activator Download Path |             |            |                      |           |                     |                                 |
| <b>Inactivity Timeout</b>      | Specifies the number of seconds after which an idle connection will time out.  | Set Http Client Inactivity Timeout      |             |            |                      |           |                     |                                 |
| <b>Connection Retries</b>      | Specifies the number of times to retry the connection before considering the connection failed. Retries are attempted after a timeout.   | Set Http Client Connection Retries      |             |            |                      |           |                     |                                 |
| <b>Secure Downloads</b>        | Specifies whether downloads will be performed over http or https.<br><br><table border="1"> <thead> <tr> <th>Option</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td><b>yes</b></td> <td>Downloads over HTTPS</td> </tr> <tr> <td><b>no</b></td> <td>Downloads over HTTP</td> </tr> </tbody> </table> | Option                                  | Description | <b>yes</b> | Downloads over HTTPS | <b>no</b> | Downloads over HTTP | Set Http Client Secure Download |
| Option                         | Description  |   |             |            |                      |           |                     |                                 |
| <b>yes</b>                     | Downloads over HTTPS   |   |             |            |                      |           |                     |                                 |
| <b>no</b>                      | Downloads over HTTP  |   |             |            |                      |           |                     |                                 |

Table 3: The HTTP client fields and their descriptions and CLI commands

### 2.2.3 Configure log Activator events

The Event Filtering System form is used to enable or disable event filtering and logging.

To enable logging Activator events, click **Advanced**. In the Advanced menu, click **Expert View -> system -> events > event system**.

Figure 6: The event filtering system page

| Field                               | Description   | CLI command                                |
|-------------------------------------|---|--|
| <b>Enabled</b>                      | Enables or disables the event log.<br>The default setting is <b>yes</b> .   | Set Event Forwarding Enabled               |
| <b>Discriminator Enabled</b>        | Enables or disables the filtering discriminator as configured in the Event Filtering form.<br>The default setting is <b>yes</b> .                                   | Set Event Forwarding Discriminator Enabled |
| <b>Discriminator Default Action</b> | Enables or disables storing system events to the internal event log of the router. The Event Filtering form is used to define specific actions for each event type. | Set Event Forwarding Default Action        |

|                                       |  |                                   |
|---------------------------------------|--|-----------------------------------|
|                                       | The default setting is <b>Log</b> .  |                                   |
| <b>Discriminator Default Severity</b> | Selects the severity to use as the default filtering criteria from the list of severity levels.<br>Severity levels are listed in order. Emergency is the highest severity and Debug-Level Messages is the lowest severity. | Event Forwarding Default Severity |
| <b>Log Size</b>                       | Specifies the size of the event log.   | Set Event Log Size                |
| <b>Log Activator Events</b>           | Logs Activator events in the event log. To log events, select <b>yes</b> .   | Set Event Activator Logging       |
| <b>Log IP Diffserv Info</b>           | Logs IP diffserv information. To log, select <b>yes</b> .  | Set Event Ip Diffserv Logging     |
| <b>Secure Downloads</b>               |  |                                   |

Table 4: The event filter system fields and their descriptions and CLI commands

## 2.2.4 Configure MAC alerts

The DHCP MAC alert feature is used to generate a specific DHCP event when a matching MAC address, or part MAC address, obtains a DHCP lease. This event is used to allow secure automatic provisioning of VoIP phones in conjunction with the Virtual Access Activator Management Server.

You must set an entry under the DHCP server parameters for a MAC address alert. This indicates that an alert is initiated when a MAC address matching the range tries to obtain an IP address.

To set an entry for a MAC alert, click **Advanced**. In the Advanced menu, click **Expert View -> system -> local servers > dhcp server > mac alert**. The DHCP Server AlertAlerts page appears.

**DHCP Server MAC Alert List**

| Index | Enabled      | Name | MAC Address | Operation           |
|-------|--------------|------|-------------|---------------------|
| 1     | unconfigured | -    | -           | <a href="#">add</a> |
| 2     | unconfigured | -    | -           | <a href="#">add</a> |
| 3     | unconfigured | -    | -           | <a href="#">add</a> |
| 4     | unconfigured | -    | -           | <a href="#">add</a> |
| 5     | unconfigured | -    | -           | <a href="#">add</a> |
| 6     | unconfigured | -    | -           | <a href="#">add</a> |
| 7     | unconfigured | -    | -           | <a href="#">add</a> |
| 8     | unconfigured | -    | -           | <a href="#">add</a> |
| 9     | unconfigured | -    | -           | <a href="#">add</a> |
| 10    | unconfigured | -    | -           | <a href="#">add</a> |

**Figure 7: The DHCP server MAC alert list page**

In the Operation column, beside the index that you want to add the entry in, click **add**. The DHCP Server MAC Alert Entry page appears.

Figure 8: The DHCP server MAC alert entry page

| Field                             | Description   | CLI command  |
|-----------------------------------|---|--|
| <b>Enabled</b>                    | Enables a DHCP alert.<br>Select <b>yes</b> .  | Set Dhcp Server Mac Alert Enabled                    |
| <b>Name</b>                       | Defines the name of the DHCP alert.   | Set Dhcp Server Mac Alert Name                       |
| <b>MAC Address</b>                | Defines the full MAC address or MAC portion to match before generating a DHCP alert.  | Set Dhcp Server Mac Alert Address                    |
| <b>MAC Address Mask</b>           | Defines the MAC address mask value used to indicate which portion of the MAC address is compared with the leasing device MAC address.   | Set Dhcp Server Mac Alert Mask                       |
| <b>Randomise TFTP Server Name</b> | Defines whether to append an 18 digit random number to DHCP Option 66 (TFTP Server Name).<br>This is required for automatic secure VoIP phone provisioning using Activator Managed Server | Set Dhcp Server Mac Alert Randomise Tftp Server Name |

Table 5: The SHCP server MAC alert entry fields, their descriptions and CLI commands

## 3 Polycom phone provisioning

This section describes the steps in automated phone provisioning.

### 3.1 Creating a phone account

The customer or reseller must first create an extension for the specific IP handset (MAC Address).

This is done on a Teleware portal that we cannot see.

### 3.2 Linking to DHCP

When a phone is powered up it tries to obtain an IP address from the SMG DHCP server

The following debug messages show what happens on the SMG:

- DHCP: Received DHCP Discover <any\_address> from MAC 0004f21a2457
- DHCP: Sent DHCP offer 192.168.100.100 - MAC Address 0004f21a2457
- DHCP: Received DHCP Request 192.168.100.100 from MAC 0004f21a2457
- DHCP Alert: Leased Mac 0004f21a2457 Rand 020319816065 [Name PhoneProv
- DHCP Alert: New Option 66 <http://193.164.253.250/phoneprovisioning/02>
- DHCP: Leased 192.168.100.100

### 3.3 HTTP operation

The SMG will append the random number at the end of the option 66 string.

The configured event filter and MAC alert feature send this event to Activator with the random number appended.

Activator issues a HTTP post to the Teleware server: POST/twautoprovisioning.

The Teleware server responds with the SIP user account and password.

The phone provisioning server creates a directory for the phone MAC address under C:\PhoneProvisioning\cfgs\TeleWare\“Reseller”

This directory contains the MACAddress.cfg, phone-MACAaddress.cfg, phone1.cfg and sip.cfg

The bootrom.id and sip.id are stored in C:\PhoneProvisioning\cfg\_templates\default

The phone then issues HTTP get requests for the various files.

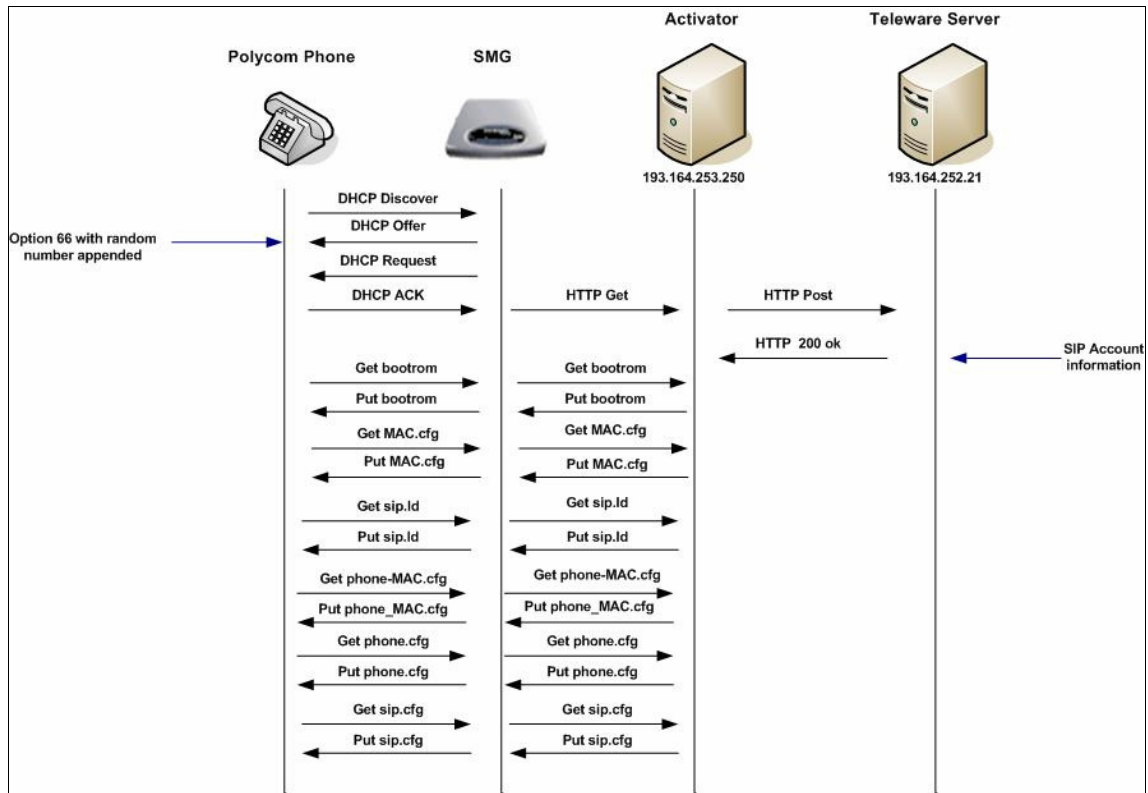


Figure 9: The Polycom phone provisioning process