

# Exinda How to Guide: IPMI

Exinda Firmware Version 6.1

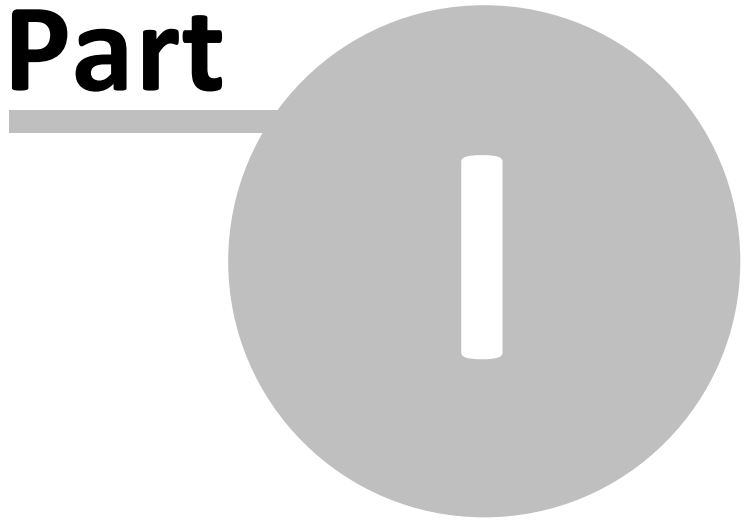
© 2011 Exinda, Inc



# Table of Contents

<b>Part I Introduction</b>	<b>4</b>
1 Using this Guide .....	4
2 Further Reading .....	5
<b>Part II Overview</b>	<b>7</b>
<b>Part III Configuration</b>	<b>9</b>
<b>Part IV Remote Power</b>	<b>12</b>
<b>Part V System Event Log</b>	<b>14</b>
<b>Index</b>	<b>15</b>

**Part**



# 1 Introduction

## IPMI

Exinda Firmware Version: 6.1

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

## 1.1 Using this Guide

Throughout the manual the following text styles are used to highlight important points:

- Useful features, hints and important issues are called "notes" and they are identified in a light blue background.

**Note:** This is a note.

- Practical examples are presented throughout the manual for deeper understanding of specific concepts. These are called "examples" and are identified with a light green background.

This is an example.

- Warnings that can cause damage to the device are included when necessary. These are indicated by the word "caution" and are highlighted in yellow.

**Caution:** This is a caution.

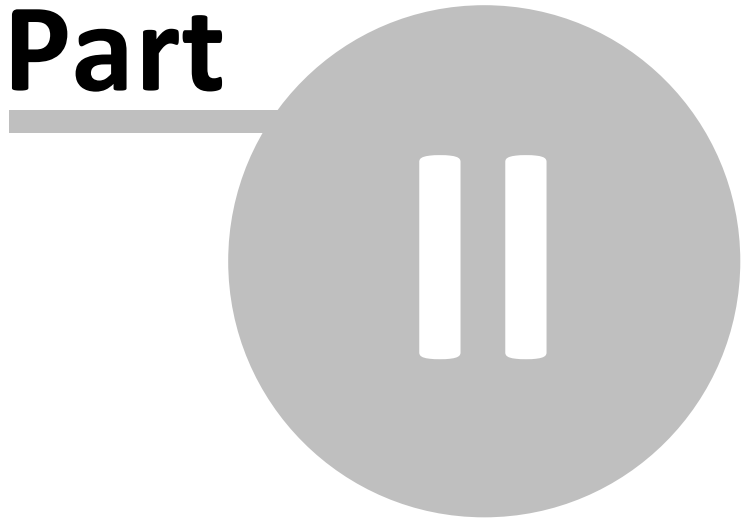
## 1.2 Further Reading

In addition to this How to Guide, the following relevant user documentation is available and should be read in conjunction with this guide:

- Exinda User Manual
- Exinda CLI Reference Guide

Please visit <http://www.exinda.com> for more information.

**Part**



## 2 Overview

The Intelligent Platform Management Interface (IPMI) is a specification for remote server management. The specification is maintained by a consortium of computer system vendors led by Intel. The current revision is 2.0. Further information on the IPMI specification is available [here](#).

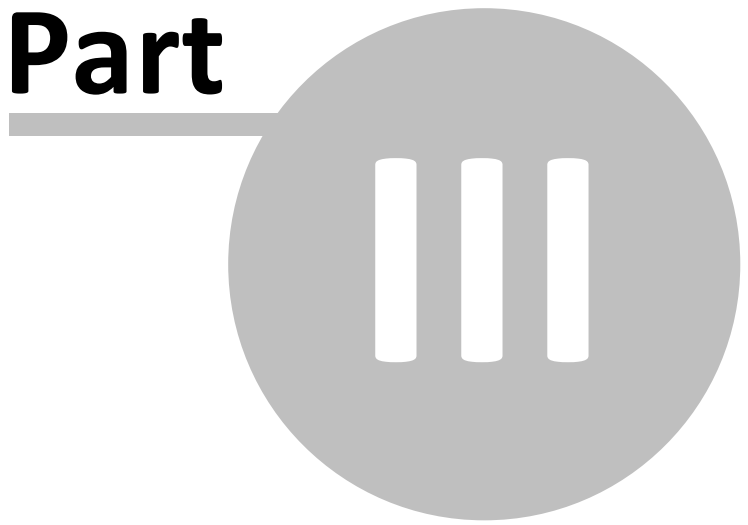
An IPMI enabled server contains a separate, dedicated micro-controller for monitoring and controlling the hardware, usually referred to as the Baseboard Management Controller (BMC). The BMC monitors system components (e.g. power supplies, fans, temperatures) and makes this data available over the LAN using either a shared or dedicated NIC. In either case the IPMI interface must be assigned a dedicated IPv4 address.

The table below shows the Exinda models that support IPMI and their capabilities.

Model	NIC	User Interface
406X	Shared (eth1)	CLI
606X	Shared (eth1)	CLI, Web
806X	Shared (eth1)	CLI, Web
1006X	Dedicated	CLI, Web

**Table 1: Models supporting IPMI**

**Part**



### 3 Configuration

To configure IPMI connectivity on the Exinda appliance, navigate to System | Network | IPMI.

Use the form to enable the IPMI LAN interface and to configure an IPv4 address and gateway. Note that although the IPMI LAN interface may be the same as the appliances eth1 interface, a separate IPv4 address is required. Alternatively you may use DHCP to configure the IPMI interface, although this is not recommended.

**Example: Enable IPMI with an IPv4 address of 172.16.0.71, subnet 255.255.254 and gateway 172.16.1.254.**

IPMI Network Settings	
Enable	<input checked="" type="checkbox"/>
DHCPv4	<input type="checkbox"/>
IPv4 Address	<input type="text" value="172.16.0.71"/> / <input type="text" value="23"/>
IPv4 Gateway	<input type="text" value="172.16.1.254"/>
Admin User	admin

This will allow the appliance to be managed using IPMI on the 172.16.0.71 address, either from another Exinda appliance or by connecting to <http://172.16.0.71> (where a Web interface is supported). When a Web interface is not supported, a command line tool such as [ipmitool](#) may be used.

Use the form below to change the authentication details. The default is username: admin, password: exinda.

Change IPMI Administrator Details	
Administrator User Name	<input type="text" value="admin"/>
New Password	<input type="password" value="••••••"/>
Confirm Password	<input type="password"/>

The equivalent CLI commands are:

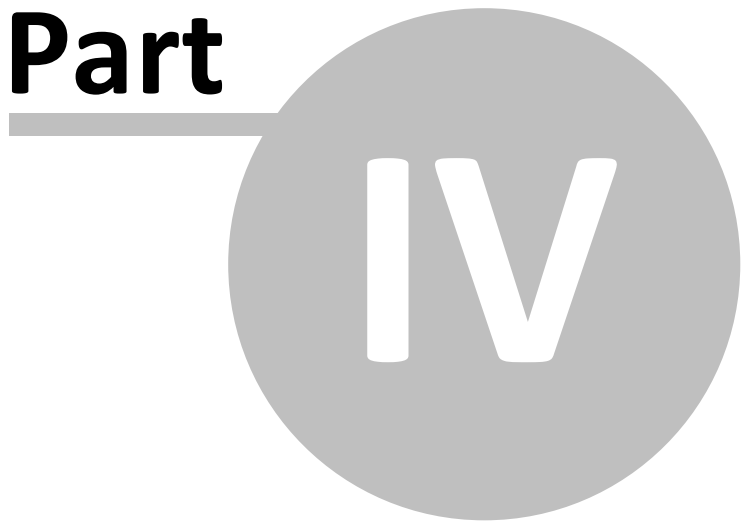
```
> en
# configure terminal
(config) # ipmi enable
```

```
(config) # ipmi ip address 172.16.0.71 255.255.254.0
```

```
(config) # ipmi ip default-gateway 172.16.1.254
```

```
(config) # ipmi username admin password exinda
```

**Part**



## 4 Remote Power

To use an Exinda appliance to manage the power settings of another appliance that has IPMI enabled, navigate to System | Tools | IPMI

**Power Control Options**

Command

---

**Remote IPMI Login Details**

IPv4 Address

Username

Password

Enter the IPv4 address of the remote appliance and authentication details. Select an operation from the dropdown list and click on the 'Do Power Action' button.

**Example: Power cycle the Exinda appliance with IPMI address 192.168.110.61**

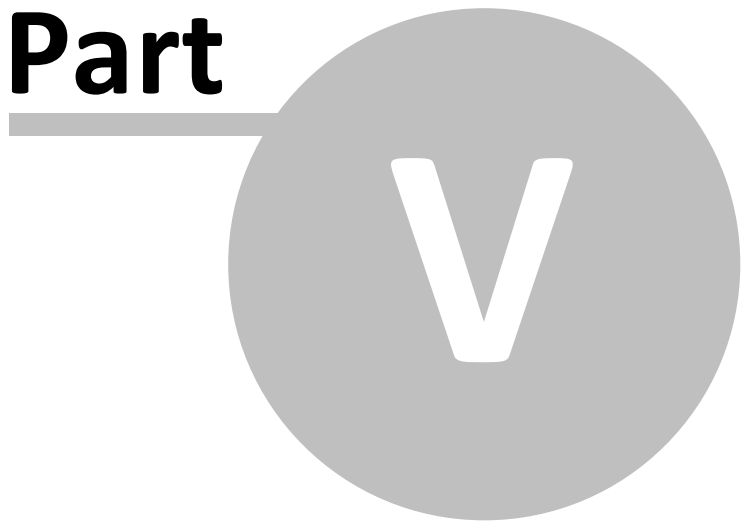
```
(config) # ipmi power address 192.168.110.61 username admin password exinda control cycle
Chassis Power Control: Cycle
```

**Example: Show the current power state of the Exinda appliance with IPMI address 192.168.110.61**

```
(config) # show ipmi power address 192.168.110.61 username admin password exinda
Chassis Power is off

(config) # show ipmi power address 192.168.110.61 username admin password exinda
Chassis Power is on
```

**Part**



## 5 System Event Log

The BMC processor keeps a log of systems events including power status, power redundancy, chassis intrusion. The following command can be used to periodically flush these events to the appliances system log.

```
(config) # ipmi sel enable
```

---

# Index

## - F -

Further Reading 5

## - I -

Introduction 4

## - U -

Using this Guide 4