Out-of-Band Management Reference
ZENworks® 11 Support Pack 3 Beta

February 2014

Novell®

Contents

About This Guide

This *Novell ZENworks 11 SP3 Out-of-Band Management Reference* includes information about power management of Intel AMT devices.

For detailed information on Intel AMT, see the *Intel Active Management Technology Architecture Guide (http://software.intel.com/en-us/articles/architecture-guide-intel-active-management-technology/)* before reading this document.

The information in this guide is organized as follows:

- Chapter 1, "Overview," on page 7
- Chapter 2, "Introducing Intel Active Management Technology," on page 9
- Chapter 3, "Configuring Intel AMT Devices," on page 11
- Chapter 4, "Power Management of Intel AMT Devices," on page 19

Audience

This guide is intended for Novell ZENworks administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Additional Documentation

ZENworks Configuration Management is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the ZENworks 11 SP3 documentation Web site (http://www.novell.com/documentation/zenworks113).

1 Overview

Out-of-band management uses a dedicated management channel, in contrast to the traditional resource management technologies that use the same infrastructure for managing both the system and operations. For example, ZENworks uses the operating system resources like networking and system APIs to establish a management communication channel between the managed device and server.

The out-of-band management solution is independent of the platform and operating system, and can also manage devices that do not have the operating system active. For example, some out-of-band technologies such as Intel AMT and IPMI manage devices that are currently shut down, but connected to the power socket.

Some out-of-band technologies use additional dedicated hardware connections specifically for management tasks. For example, to enable an active and reliable connection between a management console and a managed device, the IPMI technology uses a dedicated serial connection from the management console to the managed device. However, other technologies such as Intel AMT establish connectivity between a management server and a managed device by using an independent Ethernet network, which is different from the network connection used for an operating system.

The in-band management architecture uses the operating system services. The following figure differentiates an out-of-band management infrastructure from an in-band management infrastructure:

Figure 1-1   *In-Band Versus Out-of-Band Management*
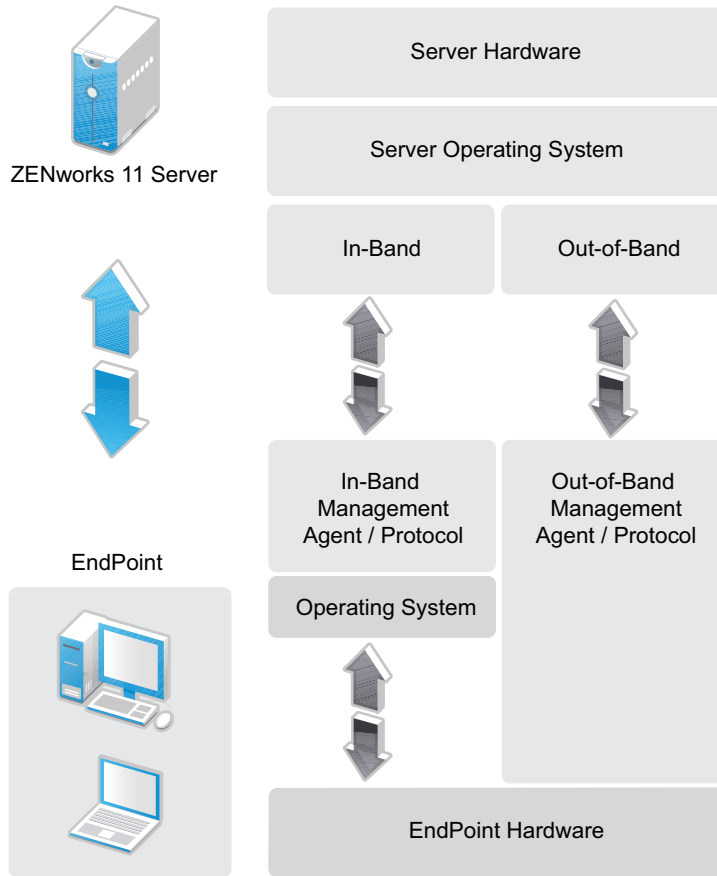
The out-of-band management technologies have been in existence for quite some time now, and standardization of some of them has taken place in last decade, using standards like Desktop and mobile Architecture for System Hardware (DASH), Systems Management Architecture for Server Hardware (SMASH), and the Alert Standard Format (ASF). The adoption of such technologies is becoming part of the mainstream, with hardware platform vendors like Intel promoting Intel Active Management Technology (AMT) and Intelligent Platform Management Interface (IPMI), and implementing these technologies in their chipsets and architecture.

With green computing being a significant priority for desktop and server administrators today, the need to alter the configuration of devices on demand and manage the power states of these devices is a significant use case today. ZENworks allows power management of endpoint devices that have the Intel AMT capability.

2 Introducing Intel Active Management Technology

Intel Active Management Technology (AMT) is an out-of-band management technologies for desktop and mobile platforms. It uses hardware or firmware technology implemented as part of the Intel Management Engine that is built into Intel processors that have vPro technology, such as Intel Core 2 Duo processors.

This technology enables system management solutions to access the Intel Management Engine remotely and perform the following system configuration tasks:

- Power management (switching on or switching off devices)
- Collecting hardware and software inventory
- Monitoring the boot sequence of the operating system from the BIOS boot to the operating system through a combination of the Serial-over-LAN (SOL) and KVM-over-IP technologies
- Booting a device from a remote disk by using the IDE redirection technology
- Sending alerts on software and hardware failure

Review the following sections:

- Section 2.1, "Intel AMT Architecture," on page 9
- Section 2.2, "Provisioning an Intel AMT Device to a Management Console," on page 10

2.1 Intel AMT Architecture

Intel AMT is a hardware or firmware management engine that is part of the Intel chipset. It virtualizes the platform Ethernet interface at the device hardware level and creates a separate logical channel for the device that can access the LAN connections independently of the operating system connection interface. This allows the Intel Management Engine that is available with the Intel chipset to access the Ethernet connectivity even when the operating system is not running on the device and the device is just plugged in without being switched on.

Typical management commands are initiated from an AMT management console to the endpoint device by using a SOAP-encoded Web Service API.

For detailed information on the Intel AMT architecture, see the Intel AMT Architecture Guide (http:/ /software.intel.com/en-us/articles/architecture-guide-intel-active-management-technology/).

2.2 Provisioning an Intel AMT Device to a Management Console

Intel AMT devices provide a secured access control methodology to manage devices. Depending on the level of sophistication of security and access control, the device management can be classified as either the Small Business Mode or the Enterprise Mode.

For a detailed understanding of the provisioning technologies, see Remote Configuration for Intel AMT (http://software.intel.com/en-us/articles/remote-configuration-for-intel-amt/).

3 Configuring Intel AMT Devices

Before managing the power of a device, you must configure certain settings for the device, depending on the mode used. You can choose to perform power management on Small Business Mode (SMB) or Enterprise Mode AMT devices.

- Section 3.1, "Configuring Intel AMT Devices in SMB Mode," on page 11
- Section 3.2, "Configuring Intel AMT Devices in Enterprise Mode," on page 13

3.1 Configuring Intel AMT Devices in SMB Mode

To prepare to manage power for Small Business Mode AMT devices, you must do the following tasks:

- Section 3.1.1, "Setting the Provisioning Mode of the Device to SMB," on page 11
- Section 3.1.2, "Adding the Intel ME Credential of the AMT Device to the Credential Vault," on page 12
- Section 3.1.3, "Configuring the SMB Settings," on page 12

3.1.1 Setting the Provisioning Mode of the Device to SMB

1 Power on the device. When you are prompted, press the Ctrl and P keys to display the Intel Management Engine BIOS Extension menu (MEBx).

To get detailed information on configuring the MEBx menu:

- **Dell devices:** See "Intel Management Engine BIOS Extension (MEBx) (http://support.dell.com/support/edocs/systems/latd630/en/amt/MEBX.htm)."
- **HP devices:** See "AMT Setup and Configuration for the Z200 Workstation with Intel AMT Technology (http://h50146.www5.hp.com/lib/doc/manual/workstation/hp_workstation/z200_amt_setup_configuration_z200_intel_amt_technology.pdf)."
- **Other devices:** Refer to the product documentation available at the vendor site.

2 In the *Intel ME Password* field, specify the Intel AMT password.

3 (Optional) To change the password, select the *Change Intel ME Password* option and specify the new password in the *Intel ME New Password* field.

4 Select *Host Name* and specify the name for the Intel AMT device. The host name of the AMT device should resolve through DNS.

5 Select *TCP/IP*, then enable or disable DHCP, depending on your network configuration.

6 (Conditional) If you choose to disable DCHP, specify the IP address, subnet mask, gateway address, the DNS addresses, and the domain name.

7 Select *Provision Mode* and press Enter.

8 Select *Small Business Mode* and press Enter.

9 Select *Return to Previous Menu* to return to the Main Menu.

10 In the Main Menu, select *Exit*.

11 When prompted, press Y to save the Intel AMT configuration.

12 Continue with Adding the Intel ME Credential of the AMT Device to the Credential Vault.

3.1.2 Adding the Intel ME Credential of the AMT Device to the Credential Vault

You can check the online Help for more information on how to add a credential to the Credential Vault.

1 In ZENworks Control Center, click *Configuration*.

2 Click *Credential Vault*.

3 Click *New > Credential*.

4 Specify the credential name.

5 Specify the login name as admin.

6 Specify the password that you set on the device in Step 2 on page 11.

7 Re-enter the password.

8 Deploy the agent on the device.

For detailed information on deploying the ZENworks Adaptive Agent, see "ZENworks Adaptive Agent Deployment" in the *ZENworks 11 SP3 Discovery, Deployment, and Retirement Reference*.

9 Continue with Configuring the SMB Settings.

3.1.3 Configuring the SMB Settings

1 In ZENworks Control Center, click *Devices*.

2 Click the device for which you want to configure the power management settings.

3 Click the *Settings* tab.

4 Click *Device Management > Intel AMT SMB Mode Settings*.

5 (Conditional) To delete any previously configured SMB setting, select the setting, then click *Delete Setting*.

6 Specify the IP address or the fully qualified domain name of the AMT device.

7 Click the browse icon to display the Credential Lookup dialog box. Browse to and select the credential from the Credential Vault, then click *OK*.

8 Click the browse icon to display the Select Server dialog box. Browse to and select the server to communicate with the AMT enabled device, then click *OK*.

9 Click *Apply*, then click *OK*.

Supported SMB Mode Configurations

While you configure the AMT chipset in the SMB mode, ensure that the host machine and AMT chipset are configured by using the following specifications:

Host Machine	AMT Chipset	Support
Static IP address	Static IP address	✔
DHCP	DHCP	✔
Static IP address	DHCP	✘
DHCP	Static IP address	✘

3.2 Configuring Intel AMT Devices in Enterprise Mode

To prepare to manage power for Enterprise Mode AMT devices, you must do the following tasks:

3.2.1 Configuring the ZENworks Primary Server for Intel AMT Management

In order to provision the Intel AMT enabled devices for Enterprise Mode, the AMT technology mandates that the Provisioning Server must have a server certificate with a unique Intel AMT OID and an OU that traces to a certificate authority (CA) whose root certificate hash is stored in the Intel AMT enabled device.

1 To generate the Intel AMT Management Certificate for a ZENworks Server that uses an internal certificate authority, run the `zman (iamt-create-mgmtcert | icmc)` command at the command prompt.

or

To generate the Intel AMT Management Certificate for a ZENworks Server that uses an external certificate authority, perform the following steps:

1a Create the certificate signing request (CSR) by running the following command:

```
zman (iamt-create-csr | icc) [isCA] [Type] (-c|--country=country) (-s|--
state=state) (-o|--organization=organization) [-u|--orgunit=Organization
Unit] [-n|--commonname=Common Name] (-d|--destination-folder=Destination
Folder)
```

Use one of the following values:

- isCA= true for Intel AMT Management if it can mint certificates for Intel AMT devices.
- isCA= false for Intel AMT Management if it cannot mint certificates for Intel AMT devices.

1b Use the generated CSR to get the Intel AMT Management Certificate signed by the external CA.

1c Ensure that the following properties are set for the certificate:

- ◆ OID = 2.16.840.1.113741.1.2.1
- ◆ OU = Intel Client Setup Certificate

1d Import the Intel AMT Management Certificate into the ZENworks certificate trust store by running the following command:

```
zman (iamt-create-mgmtcert|icmc) [-p|--certpath=Intel AMT Provisioning/
Management Certificate (DER format) Path]
```

2 To obtain the ZENworks CA hash, run the `zman [iamt-root-certificate-hash | irch]` command at ZENworks Server command prompt.

The ZENworks CA hash is displayed in two formats, MD5 and SHA1. However, you should only use the SHA1 thumbprint hash format. The SHA1 thumbprint hash is displayed as a string of 40 alphanumeric characters with a colon after every two digits. For example, `1F:0E:1C:88:A0:88:B5:6A:E8:82:6D:28:01:D4:2F:B4:6F:8D:16:77`

3 Continue with Configuring the Intel AMT Device with the ZENworks CA Hash.

3.2.2 Configuring the Intel AMT Device with the ZENworks CA Hash

You can choose to configure the Intel AMT device with the ZENworks CA hash in one of the following ways:

- ◆ "Specifying the ZENworks CA Hash in the MEBx Menu of the Intel AMT Device" on page 14
- ◆ "Specifying the ZENworks CA Hash by Using a Bootable USB Device" on page 15

Specifying the ZENworks CA Hash in the MEBx Menu of the Intel AMT Device

1 Power on the device. When you are prompted, press the Ctrl and P keys to display the Intel Management Engine BIOS Extension menu (MEBx).

To get detailed information on configuring the MEBx menu:

- ◆ **Dell devices:** See "Intel Management Engine BIOS Extension (MEBx) (http://support.dell.com/support/edocs/systems/latd630/en/amt/MEBX.htm)."
- ◆ **HP devices:** See "AMT Setup and Configuration for the Z200 Workstation with Intel AMT Technology (http://h50146.www5.hp.com/lib/doc/manual/workstation/hp_workstation/z200_amt_setup_configuration_z200_intel_amt_technology.pdf)".
- ◆ **Other devices:** Refer to the product documentation available at the vendor site.

2 In the *Intel ME Password* field, specify the Intel AMT password.

3 (Optional) To change the password, select the *Change Intel ME Password* field and specify the new password in the *Intel ME New Password* field.

4 Select *Host Name* and specify the name for the Intel AMT device. The host name of the AMT device should resolve through DNS.

5 Select *TCP/IP*, enable DHCP, then specify the domain name.

6 Select *Provision Mode* field and press Enter.

7 Ensure that *Enterprise Mode* is selected and press Enter.

8 Select *Setup and Configuration* to display the Intel Setup and Configuration Page.

9 Select *Provisioning Server* and specify the IP address and port number (9971) of the Provisioning ZENworks Server.

10 Select *TLS PKI* to display the Intel Remote Configuration page. Ensure that *Remote Configuration* is enabled.

11 Select *Manage Certificate Hashes* and press the Insert key to add a new hash. Specify the hash name.

12 Specify the hash certificate that you obtained in Section 3.2.1, "Configuring the ZENworks Primary Server for Intel AMT Management," on page 13. You must specify the characters in the same sequence as the generated hash, but in groups of four alphanumeric characters separated by a hyphen.

For example, if the generated certificated is `1F:0E:1C:88:A0:88:B5:6A:E8:82:6D:28:01:D4:2F:B4:6F:8D:16:77`, then you must specify the hash certificate as `1F0E-1C88-A088-B56A-E882-6D28-01D4-2FB4-6F8D-1677`.

13 Select *Provisioning Server FQDN* and specify the fully qualified domain name of the Provisioning ZENworks Server.

14 Select *Set PKI DNS Suffix* and specify the DNS suffix.

15 Select *Return to Previous Menu* to return to the Intel Setup and Configuration page.

16 Select *Return to Previous Menu* to return to the Intel AMT Configuration page.

17 Select *Return to Previous Menu* to return to the Main Menu.

18 In the Main Menu, select *Exit*.

19 When prompted, press Y to save the Intel AMT Configuration.

20 Continue with Section 3.2.3, "Adding the Intel ME Credential of the AMT Device to the Credential Vault," on page 16.

Specifying the ZENworks CA Hash by Using a Bootable USB Device

1 (Conditional) If the device is not bootable, run the following command to make the USB device bootable: `format <drive_name> /FS:FAT /V:AMT_USB`

2 Locate the `USBFile.exe` utility in the following location: `\Windows\Intel_Manageability_Configuration\Configuration\ConfigurationServer\Bin\ConfigScripts`.

If the `USBFile.exe` is not available, download the file from the latest "Intel AMT Software Development Kit (http://software.intel.com/en-us/articles/download-the-latest-intel-amt-software-development-kit-sdk/)".

3 Run the Intel Utility (`USBFile.exe`) to generate a USB file named `setup.bin`.

```
USBFile.exe -create setup.bin <current_MEBx_Password> <new_MEBx_password> -dns
<domain_name> -fqdn <prov_server_fqdn> -ztc 1 -hash <zcm_CA_certtificate_path>
<friendly_name>
```

4 Copy the generated `setup.bin` file to a USB device.

5 Boot the Intel AMT enabled device with the USB device.

6 Continue with Adding the Intel ME Credential of the AMT Device to the Credential Vault.

3.2.3 Adding the Intel ME Credential of the AMT Device to the Credential Vault

You can check the online Help for more information on how to add a credential to the Credential Vault.

1 In ZENworks Control Center, click *Configuration*.

2 Click *Credential Vault*.

3 Click *New > Credential*.

4 Specify the credential name.

5 Specify the login name as admin.

6 Specify the password that you set on the device in Step 2 on page 14.

7 Re-enter the password.

8 Continue with Provisioning the AMT Devices.

3.2.4 Provisioning the AMT Devices

You must provision a device to establish a mutual trust between the device and the Management Console.

   ◆ "Provisioning AMT Devices with the Device Certificate and a Private Key" on page 16
   ◆ "Provisioning AMT Devices with an External Certificate" on page 17

Provisioning AMT Devices with the Device Certificate and a Private Key

1 In the ZENworks Control Center, click *Devices*.

2 Click *Discovered*.

3 Click the *Intel AMT Devices* link to view all the discovered Intel AMT devices.

   The validity of the discovered Intel AMT devices is twelve hours, after which you need to rediscover the device.

4 Select the Intel AMT devices that you want to provision, then click *Action > Provision*.
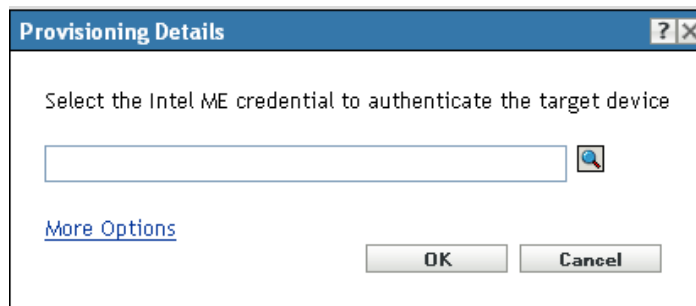
5 In the Provisioning Details dialog box, browse for and select the appropriate Intel ME credential of the target device.

6 Click *OK*.

7 Deploy the ZENworks Adaptive Agent to the devices so that you can manage them.

For more information on how to deploy the ZENworks Adaptive Agent, see "ZENworks Adaptive Agent Deployment" in the *ZENworks 11 SP3 Discovery, Deployment, and Retirement Reference*.

8 Continue with Section 3.2.5, "Reconciling the AMT Devices," on page 17.

Provisioning AMT Devices with an External Certificate

1 In the ZENworks Control Center, click *Devices*.

2 Click *Discovered*.

3 Click the *Intel AMT Devices* link to view all the discovered Intel AMT devices.

The validity of the discovered Intel AMT devices is one day, after which you need to rediscover the device.

4 Select the Intel AMT device that you want to provision, then click *Action > Provision*.

5 Provide the provisioning details:

    5a Browse for and select the appropriate Intel ME credential of the target device.

    5b Click *More Options*.

    5c Select the *Use External Certificate to Provision the device* check box.

    5d Browse for and select the private key file for the targeted Intel AMT device, then click *OK*.

    5e Browse for and select the certificate file for the targeted Intel AMT device, then click *OK*.

6 Click *OK*.

7 Deploy the ZENworks Adaptive Agent to the devices so that you can manage them.

For more information on how to deploy the ZENworks Adaptive Agent, see "ZENworks Adaptive Agent Deployment" in the *ZENworks 11 SP3 Discovery, Deployment, and Retirement Reference*.

8 Continue with Reconciling the AMT Devices.

3.2.5 Reconciling the AMT Devices

The devices must be inventoried for the reconciliation to take place. By default, the AMT devices are reconciled every 24 hours. However, you can choose to configure a schedule for reconciling the devices:

1 In ZENworks Control Center, click *Configuration*.

2 In the Management Zone Settings panel, click *Inventory > Out-of-band Inventory Reconciliation* to display the Out-of-band Inventory Reconciliation page.

3 (Conditional) To immediately start the reconciliation process, click *Start Now*.

4 In the *Schedule Type* field, select one of the following schedule types:

- No Schedule
- Date Specific
- Recurring

For more information on the various schedule types, click *Help* on the page.

5 Click *Apply*, then click *OK*.

3.2.6 Unprovisioning the AMT Devices

You can unprovision a provisioned Intel AMT device.

1 In ZENworks Control Center, click *Devices*.

2 Click *Discovered*.

3 Click the *Intel AMT Devices* link to view all the discovered/provisioned Intel AMT devices.

4 Select the Intel AMT devices that you want to unprovision, then click *Action > Unprovision*.

5 Provide the details:

    5a Browse for and select the appropriate Intel ME credential of the target device.

    5b Select the *Delete the device if unprovisioning fails* check box, if unprovisioning fails and you want to delete the Intel AMT device.

6 Click *OK*.

3.2.7 Changing the Zone Certificate of the Primary Server

Before you change the zone certificate of the Primary Server, unprovision all the provisioned Intel AMT devices, then run the `novell-zenworks-configure -c SSL -Z` command to change the zone certificate. After changing the zone certificate, provision the Intel AMT devices.

1 Clean the Intel AMT Management certificates by running the following command:

```
zman (iamt-delete-mgmtcert | idmc)
```

2 Restart the Novell ZENworks Server and Novell ZENworks Loader services by running the following commands:

```
/etc/init.d/novell-zenserver start
```

```
/etc/init.d/novell-zenloader start
```

3 Create the Intel AMT Management certificate by running the following command:

```
zman (iamt-create-mgmtcert | icmc)
```

4 Rediscover all the AMT devices.

For more information on how to discover a device, see "Device Discovery" in the *ZENworks 11 SP3 Discovery, Deployment, and Retirement Reference*.

5 Provision the Intel AMT devices.

For more information on how to provision an Intel AMT device, see "Provisioning the AMT Devices" on page 16.

4 Power Management of Intel AMT Devices

ZENworks 11 allows you to manage the power states of Intel AMT devices either on demand or based on a schedule. The Intel AMT devices should be configured in either the Small Business Mode or Enterprise Mode.

For Intel AMT devices that are configured in Small Business Mode, the server configured on the Intel AMT SMB Mode Settings page of the device triggers the power management operation on the devices. For more information, see Section 3.1.3, "Configuring the SMB Settings," on page 12.

For Intel AMT devices that are configured in Enterprise Mode, the configured Provisioning Server triggers the power management operation on the devices. For more information, see Section 3.2.1, "Configuring the ZENworks Primary Server for Intel AMT Management," on page 13.

For more information on the power management of Intel AMT devices, see the following sections:

- Section 4.1, "On-Demand Power Management," on page 19
- Section 4.2, "Scheduled Power Management," on page 19

4.1 On-Demand Power Management

The Intel AMT devices should be configured either in Small Business Mode or Enterprise Mode. For more information on the configuration steps, see Chapter 3, "Configuring Intel AMT Devices," on page 11.

1 In ZENworks Control Center, click *Devices*.
2 Select the Intel AMT devices for which you want to change the power state.

> **IMPORTANT:** If the selected devices include the server that is required to trigger the power management operation on the Intel AMT devices, it is possible that the server might reset or power off before the power management operation is successfully performed on the selected Intel AMT devices.

3 Click *Quick Tasks > Intel AMT Power Management*.
4 Select a new power state for the devices.
5 Click *OK*.

4.2 Scheduled Power Management

The Intel AMT devices should be configured either in Small Business Mode or Enterprise Mode. For more information on the configuration steps, see Chapter 3, "Configuring Intel AMT Devices," on page 11.

IMPORTANT: If the server that is required to trigger the power management operation on the Intel AMT devices has a power management schedule set, it is possible that the server might reset or power off before the power management operation is successfully performed on the Intel AMT devices.

1 In ZENworks Control Center, click *Configuration*.

2 In the Management Zone Settings panel, click *Device Management > Power Management*

Settings.

3 In the Power Management Settings panel, click *Add*.

4 Click the desired power state.

The supported power states include Power On, Power Off, Reset and Power Cycle Reset.

5 In the Schedule Editor dialog box, select one of the following schedule types:

- **No Schedule:** Does not trigger the power state on the device.
- **Recurring:** Triggers the power state at specified intervals on the device

6 Click *Apply*, then click *OK*.

By default, the Power Management settings configured at the zone level are applied to all the devices within the Management Zone. However, you can choose to override the settings at the device level or folder level.