ASWM Enterprise

System Web-based Management

User Manual

E9286

Durian Edition V2.00
March 2014

Disclaimer

The manufacturer is not responsible for any damages, including loss of profits, loss of information, interruption of business, personal injury, and/or any damage or consequential damage without limitation, incurred before, during, or after the use of our products.

Contents

Contents ..... **iii**
About this guide ..... **vi**

Getting Started 1-1

1.1 Introduction to ASWM Enterprise **1-2**
1.1.1 How ASWM Enterprise works 1-2
1.1.2 Supported OS platforms 1-3
1.2 ASWM Enterprise installation **1-5**
1.2.1 ASWM Enterprise main server requirement 1-5
1.2.2 Installing ASWM Enterprise 1-6
1.3 Uninstalling ASWM Enterprise **1-9**
1.3.1 Uninstalling from Windows 1-9
1.4 Login ASWM Enterprise **1-11**
1.5 The main page **1-13**

Deployment management 2-1

2.1 Deploying new ASWM Enterprise agent **2-2**
2.1.1 Automatically scanning the active directory 2-2
2.1.2 Manually deploying the ASWM Enterpise agents 2-8
2.1.3 Discover Clients with preload service (ThinClient mode) 2-10
2.1.4 Manually Install the ASWM Enterprise Linux Agent 2-12
2.2 Removing ASWM Enterprise agent **2-13**
2.2.1 Scanning the self ASWM main server 2-13
2.2.2 Automatically scanning the Active Directory 2-16

Main Server Functions 3-1

3.1 Monitor **3-2**
3.2 Account Management **3-5**
3.2.1 Current Login Account 3-5
3.2.2 Account 3-6
3.2.3 Role privilege 3-7
3.3 Deployment Management **3-8**
3.4 Centralized Management **3-9**
3.4.1 BIOS Flash Centralized Management 3-9
3.4.2 Remote Control Centralized Management 3-10
3.4.3 Power Control Centralized Management 3-12
3.4.4 Thin Client EWF Centralized Management 3-13
3.4.5 Software Dispatch Centralized Management 3-15

Contents

3.4.6 Task Scheduler Centralized Management 3-16
3.5 Report Management 3-22
3.5.1 Asset Report Management 3-22
3.5.2 Software Dispatch Report Management 3-23
3.5.3 Agent Connection Report Management 3-24
3.6 Server Configuration 3-25
3.6.1 SMTP Server 3-25
3.6.2 Security 3-26
3.6.4 ASWM Group 3-27
3.6.5 BIOS 3-28
3.6.6 DataBase 3-28
3.6.7 Software Pool 3-29
3.6.8 Monitor 3-31

Client Monitor Information 4-1

4.1 Monitor Overview 4-2
4.2 HW Sensor 4-4
4.2.1 Setting thresholds 4-5
4.2.2 Hardware sensor tabs 4-6
4.3 Inventory 4-9
4.3.1 Disk Info 4-9
4.3.2 Device Manager 4-11
4.4 Event Log 4-12
4.5 Utilization 4-15
4.5.1 Partition 4-15
4.5.2 CPU 4-15
4.5.3 Memory 4-16
4.5.4 Network 4-16
4.6 Software 4-17
4.6.1 Application 4-17
4.6.2 Service 4-17
4.6.3 Process 4-18
4.6.4 Environment Variables 4-19
4.6.5 Software Dispatch 4-19
4.6.6 Export function 4-21
4.7 Security 4-22
4.8 BMC 4-25

4.9 BIOS Flash 4-27
4.10 Configuration 4-28
4.10.1 Information 4-28
4.10.2 Network 4-29
4.10.3 Notification 4-30
4.11 Remote Control 4-32
4.12 ThinClient features 4-33
4.12.1 EWF (Enhanced Write Filter) 4-34

Reference information A-1
A.1 Glossary A-2
A.2 Agent Function Comparison Table A-3
ASUS contact information 1

About this guide

Audience

This user guide is intended for system integrators, and experienced users with basic knowledge of configuring a server.

Contents

This guide contains the following parts:

Chapter 1: Getting Started

This chapter provides an overview of ASWM Enterpirse, and how to install or uninstall it under Windows®.

Chapter 2: Deployment Management

This chapter describes how to deploy ASWM Enterprise agents and remove agents manually or from the Active Directory.

Chapter 3: Main Server Functions

This chapter describes the Main Server Functions, including Monitor, Account Management, Deployment Management, Remote Control, and Server Configuration.

Chapter 4: Client Monitor Information

This chapter describes the client's system status and information.

Appendix: Reference

This appendix includes a glossary of terms used in this document.

Conventions

To make sure that you perform certain tasks properly, take note of the following symbols used throughout this manual.

WARNING: Information to prevent injury to yourself when trying to complete a task.

CAUTION: Information to prevent damage to the components when trying to complete a task.

IMPORTANT: Instructions that you MUST follow to complete a task.

NOTE: Tips and information to aid in completing a task.

Reference

Visit the ASUS websites worldwide that provide updated information for all ASUS hardware and software products. Refer to the ASUS contact information for details.

Chapter 1

This chapter provides an overview of ASWM Enterprise, and how to install or uninstall it under Windows®.

Getting Started

1.1 Introduction to ASWM Enterprise

Welcome! Thank for buying our server products bundled with ASWM Enterprise System Web-based Management software. The ASWM Enterprise is a proprietary server management solution that gives a vital distinction to our servers.

In server management, system stability is a major factor, with efficiency, cost-effectiveness, and convenience following close behind. To comply with this, we have created a reliable and user-friendly ASWM Enterprise monitoring tool. The ASWM Enterprise is a web-based interface that allows system administrators to conveniently manage computers either locally (from the same server), or remotely (using a web-browser).

With its colorful, graphical, and informative interface, the ASWM Enterprise makes server management a delightful experience!

1.1.1 How ASWM Enterprise works

The ASWM Enterprise is composed of an “agent” that generally acts as a data collector, and a set of HTTP web pages that serve as the user interface (UI). The data collected by the agent, which are essential for the continuous monitoring operations performed by ASWM Enterprise, are displayed in the UI.

In the monitoring process, the agent basically keeps track of the hardware and software status of the system. The agent has “sensors” that monitor fan rotation speeds (in RPM), working voltages, motherboard and CPU temperatures, and the backplane (if present).

In addition, the agent also monitors hard disk drives health status through the SMART (Self-Monitoring, Analysis, and Reporting Technology) feature, space utilization of a file system, CPU or system memory loading, and even the traffic status of a network device.

The agent records the history of the detected status of all monitored hardware items. The status record includes the time of alert events (fan, voltage, or temperature), and the type of alert event (critical, warning, or normal).

You can also configure ASWM Enterprise to react to exceptional situations. For example, the administrator can be automatically notified by e-mail when a hard drive starts to malfunction or when a chassis intrusion is detected. In this way, ASWM Enterprise acts as an active guardian of the system’s key components.

1.1.2 Supported OS platforms

The ASWM Enterprise agent supports the following operating systems, You can choose the appropriate package depending on the primary OS installation of your server.

Main Server Support Operating System

Windows® Server 2012 R2 64 bit

Windows® Server 2012 64 bit

Windows® Server 2008 R2 64 bit

Windows® Server 2008 32/64 bit

Windows® Server 2003 32/64 bit

Agent Support Operating System

Windows® Operating System

Windows® Server 2012 R2 64bit

Windows® Server 2012 64bit

Windows® Server 2008 R2 64 bit

Windows® Server 2008 32/64 bit

Windows® Server 2003 32/64 bit

Windows® 8.1 32/64 bit

Windows® 8 32/64 bit

Windows® 7 32/64 bit

Linux Operating System

RHEL 6.5 32/64 bit

RHEL 6.4 32/64 bit

CentOS 6.5 32/64 bits

CentOS 6.4 32/64 bits

Scientific Linux 6.5 32/64 bits

Scientific Linux 6.4 32/64 bits

SLES 11 SP3 32/64 bits

SLES 11 SP2 32/64 bits

The ASWM Enterprise web pages are fully compatible with W3C HTML 4.0/DOM standard. The web browsers with Microsoft Silverlight support can work with ASWM Enterprise:

Operating System	Internet Explorer 10	Internet Explorer 9	Internet Explorer 8	Internet Explorer 7	Internet Explorer 6	Firefox 3.6+	Safari 4+	Chrome 12+
Windows 8 Desktop	✓*	-	-	-	-	✓	-	✓
Windows Server 2012	✓*	-	-	-	-	✓	-	✓
Windows 7	-	✓*	✓*	-	-	✓	-	✓
Windows 7 SP1	✓*	✓*	✓*	-	-	✓	-	✓
Windows Server 2008 SP2	-	✓	✓	✓	-	✓	-	✓
Windows Server 2008 R2 SP1	-	✓*	✓*	-	-	✓	-	✓
Windows Vista SP2	-	✓	✓	✓	-	✓	-	✓
Windows Server 2003 SP2, Windows XP SP3	-	-	✓	✓	-	✓	-	✓
Macintosh OS 10.5.7+ (intel-based)	-	-	-	-	-	✓	✓	-

*** Supports 64-bit mode.**

Minimal Requirements

Components	Requirements
Windows®	x86 or x64 (64-bit mode support for IE only) 1.6-gigaherts (GHz) or higher processor with 512-MB of RAM

1.2 ASWM Enterprise installation

You can install ASWM Enterprise in Windows platform. Proceed to the succeeding sections for the instructions that are applicable to your operating system.

1.2.1 ASWM Enterprise main server requirement

System Requirement

- Microsoft SQL Server 2005 or above (Including Express version)
  SQL Server 2005 ~ SQL Server 2008 r2 sp2
- Web Server IIS 6 or above
- .NET Framework 3.5 SP1
- .NET Framework 4.0 (Full)
- Active Directory (Deployment by Active Directory)

* Time zone setting must be the same

For Windows Server 2008 or above

Ensure to add the following Features / Roles

- Features: .NET Framework 3.5.1
- Roles: Web Server (IIS)
- Role Services under WebServer(IIS):

  (A) Common Http Features (and all sub-items) have to be selected.

  (B) IIS 6 Management Compatibility (and all sub-items) have to be selected.

  (C) Application Development
  - ASP.NET
  - .NET Extensibility
  - ISAPI Extensions
  - ISAPI Filters

For Windows Server 2012

Ensure to select the following Features

- Features:
  - .NET Framework 3.5 Features
    - .NET Framework 3.5 (include .NET 2.0 and 3.0)
    - HTTP Activation
  - .NET Framework 4.5 Features
    - .NET Framework 4.5
    - ASP .NET 4.5
    - WCF Services
      - HTTP Activation

1.2.2 Installing ASWM Enterprise

Any user with administrator privileges on the local system can install ASWM Enterprise.

To install ASWM Enterprise in Windows:

1. Insert the support DVD into the optical drive and click **ASWM Enterprise**.

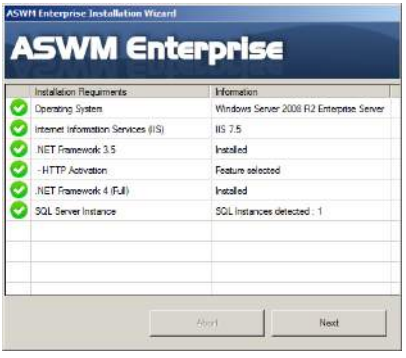
Ensure that your system meets the requirements metioned in the previous page.

2. The ASWM Enterprise Setup program wizard appears. Click **Next** to continue.

3. Click **Next** to start installation.

4. The system is installing ASWM Enterprise.

5. The system is checking the installation requirements. Click **Next** to continue.



6. Select an **Authentication** type and click **Connection Test** to proceed.

7. After passing the Connection Test, click **OK** and **Next** to continue.

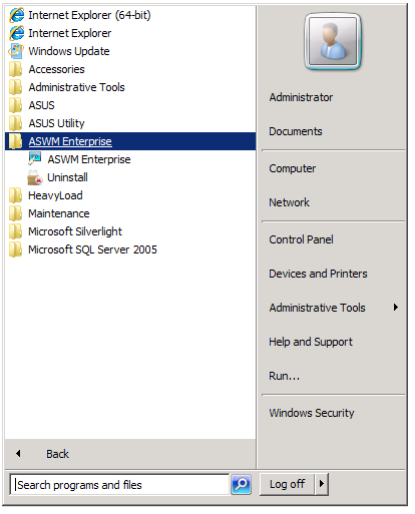
8. When the installation completes, click **Close** to exit the wizard.

1.3 Uninstalling ASWM Enterprise

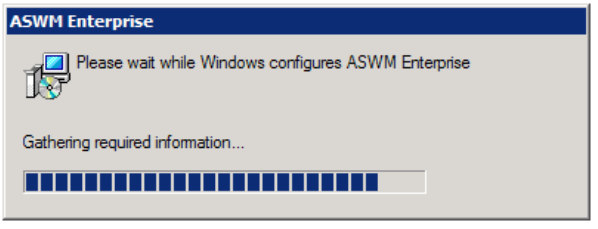
1.3.1 Uninstalling from Windows

To uninstall ASWM Enterprise from a Windows platform:

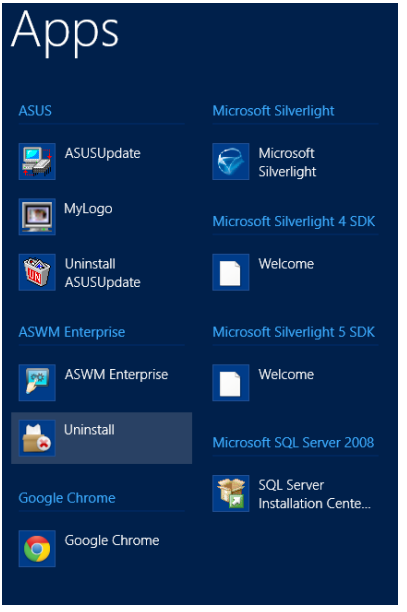
1. Click **Start > All Programs > ASWM Enterprise > Uninstall**.

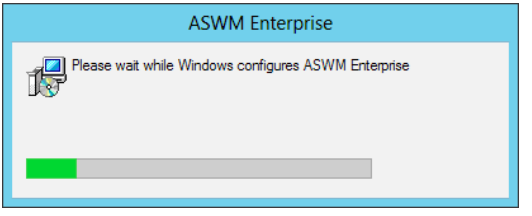


2. The system automatically uninstalls ASWM Enterprise.



For Windows® 2012:

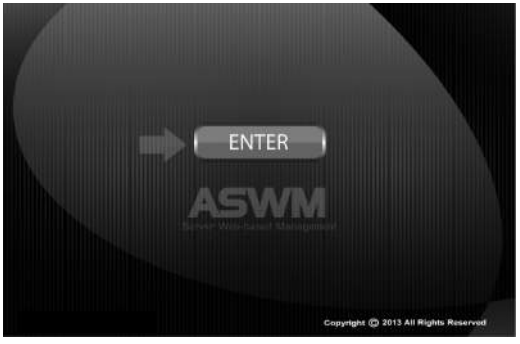




1.4 Login ASWM Enterprise

To login ASWM Enterprise:

1. Double-click the ASWM Enterprise shortcut on the desktop when you login from the local server. If you login from the remote server, enter the ASWM Enterprise website (http://HostName(IP)/aswment) through the web browser.
2. Click **Enter**.



3. Enter your **Name** and **Password**. Click **Login** to enter ASWM Enterprise.

- The default **login name: Administrator**, **password: aswm**. Note that the login name and password are case sensitive. Refer to **Account Management** if you would like to change the password.
- In additional to **Administrator**, You can also login as a **User**. Note that users have only limited privileges. **Login name: User**; **password: user**.

Limitation when logining as a User

- Only limited functions, including **Monitor** and **Account Management** are available.
- **HW Sensor** is read-only. You cannot customize the threshold.
- You cannot delete the EventLog, but you are allowed to use the **Advanced Search** function.
- **Utilization** is read-only. You cannot customize the threshold.
- You can check the information of the installed software, but **Service** of starting, restarting or stopping the selected service is unavailable. Ending process is also unavailable.
- **Remote Control** is dimmed and unavailable.
- Deleting SEL information on BMC is not allowed.
- **BIOS Flash** is read-only. You cannot flash the BIOS.
- **Configuration** in **Monitor** is unavailable.

1.5 The main page

The main control panel of the ASWM Enterprise user interface is displayed as shown.

1 **Full screen view** : Click this banner to switch to the full screen view and press <Esc> to return to the normal window view. You cannot input text in the full screen view.

2 **Function buttons** : The overall functions of ASWM Enterprise, inlcuding health monitoring, account management, deployment management, centralized management, and server configuration. Refer to later chapters for details.

3 **Login information** : This area displays the login ID. Different login users have different level of controlling ASWM Enterprise. Click **LogOut** to exit ASWM Enterprise.

4 **Group List** : The Group List shows the existing groups. It is more convenient for administrator to manage a large number of computers through groups.

5 **Models in the group** : This area shows the computers and their general information in your selected group above.

6 **Switch Monitor View** : This area allows you to switch the monitor view between "Server/MB" and "Storage".

Chapter 2

This chapter describes how to deploy ASWM Enterprise agents and remove agents through AD or manually.

Deployment management

2.1 Deploying new ASWM Enterprise agent

Install new ASWM Enterpise agents on computer and add them the ASWM Enterprise server for convenient management, monitor and control.

ASWM Enterprise client agent system requirement

- .NET Framework 3.5
- Requires ASUS Management IPMI Driver for all models with BMC device on Windows® 7 32/64bit
- Firewall Setting

  Allow "Windows® Management Instrumentation (WMI)"

  Allow "File And Printer Share"

  Allow "ICMP Packet Response"

  Add Outbound Rules "UDP Port" ranging from 50000 ~ 50100 if "Power control" is carried out through remote BMC

2.1.1 Automatically scanning the active directory

To deploy new agents

1. Click **Deployment Management** on the left.

2. Click **Deploy New ASWM Enterprise Agent**.

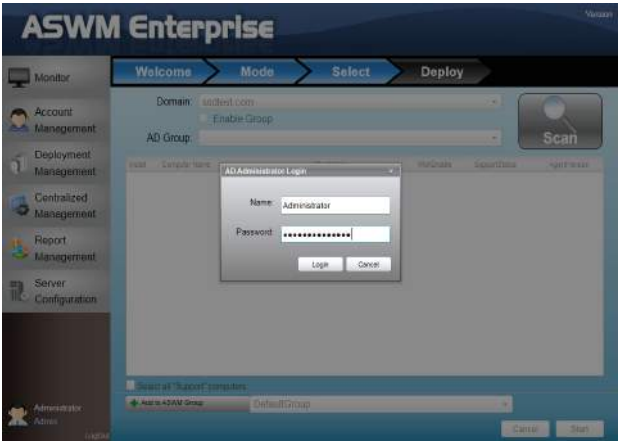
3. The wizard will guide you through the deployment process. Click **Start** to continue.

4. Select **Automatically Scan the Active Directory** and click **Next** to continue. The system will automatically scan the directory for agents.

5. Select a **Domain** and click **Scan** to start scanning.

Click **Enable Group** and select a desired group to downsize the scanning range. Doing so shortens the time for agent deployment.

6. Enter the **Name** and **Passowrd** to login as the AD Administrator.



7. The system starts scanning.

8. Click wanted computers to deploy agents and click **Start**. The computer must be listed as **Support** in the **SupportStatus** field. Click the computer that shows **Not Support,** the reasons will be shown below.

   If your wanted computers are listed as **Not Support**. Double check the followings:

   - If it is a supported model. Refer to the beginning of the section for details.
   - If it has installed .NET 3.5
   - If it has installed ASWM Enterprise Agent
   - If old ASWM version existed

- Click **Select all "Support" computers** if you want to deploy agents on all Support Computers.
- Click **Add to ASWM Group** if you would like to catergorize the selected computers to different groups.
- The **SupportStatus** shows **Unknown** when **WMIEnable** shows **OFF**.

9. The deployment starts.

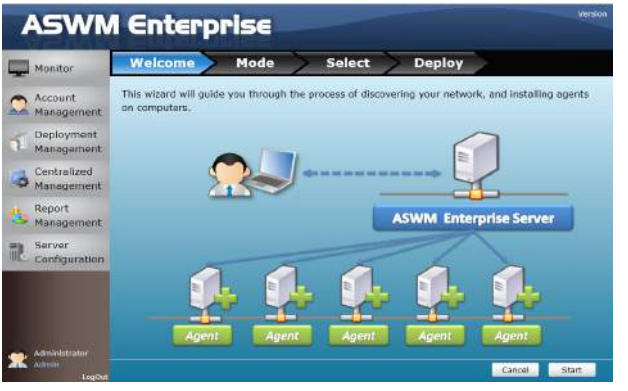
2.1.2 Manually deploying the ASWM Enterprise agents

To deploy new agents

1. Click **Deployment Management** on the left.

2. Click **Deploy New ASWM Enterprise Agent**.

3. The wizard will guide you through the deployment process. Click **Start** to continue.



4. Select **Manual Deploy the ASWM Enterprise Agent** and click **Next** to continue.

5. Click **Add Target PC**. You can add the target PC through IP Address or Host Name. Fill in the required fileds and click **Scan**.

You can also click the Import button to import a deploy table manually.

6. Follow the instructions in the previous section to install the agent when the scanning result is shown.

2.1.3 Discover Clients with preload service (ThinClient mode)

The ThinClient mode allows you to search for Thin Clients (eg.TC-710) in the same network for multiple client deployment via the ASWM Enterprise.

Ensure that the ThinClient has boot up and connected to the same network with the Main Server.

1. Select **Discover Clients with preload service (ThinClient mode)** and click **Next** to search for the ThinClient in the network.

2. The clients are classified into **Support** and **Not Support** in **SupportStatus** field.

Support: The ThinClient supports ASUS ASWM Enterprise agent.

Not Support: The ThinClient has probably already installed ASUS ASWM Enterprise agent. Please remove it and re-install the agent.

3. Click **Discovery** to search again.

Set the firewall in the Main Server properly since the Discovery function will send broadcast packet through the Main Server.

4. Under the **Install** column, select the Thin Client, and click **Start** to install the agent.

5. Wait until the installation process is completed.

2.1.4 Manually Install the ASWM Enterprise Linux Agent

OS Support and Requirements

- **OS Support:**
  RHEL 6.5 32/64 bit
  RHEL 6.4 32/64 bit
  CentOS 6.5 32/64 bits
  CentOS 6.4 32/64 bits
  Scientific Linux 6.5 32/64 bits
  Scientific Linux 6.4 32/64 bits
  SLES 11 SP3 32/64 bits
  SLES 11 SP2 32/64 bits
- **System requirements**
  - Requires “sysstat”, “smartmontools”, “wireless-tools”, “ethtool”, “ipmitool” software
  - Requires “OpenIPMI” driver
  - Requires ASMB

Ensure that your system environment meets the above requriements and the client is connected to the main server before installing ASWM Enterprise Linux Client Agent

To install the ASWM Enterprise Linux Agent manually:

- Use the root account to login Linux;
- Unzip the file, tar -zxvf ASWMLinuxAgent-XXX.tar.gz
- Type ./install.sh
- Choose the directory that you want to install or use the default directory **/root/ASWMLinuxAgent**
- Input the IP address of your main server
- Wait for 1 - 2 minutes for the installation to finish.

2.2 Removing ASWM Enterprise agent

You are allowed to remove the ASWM Enterprise agents from the main server or in Active Directory.

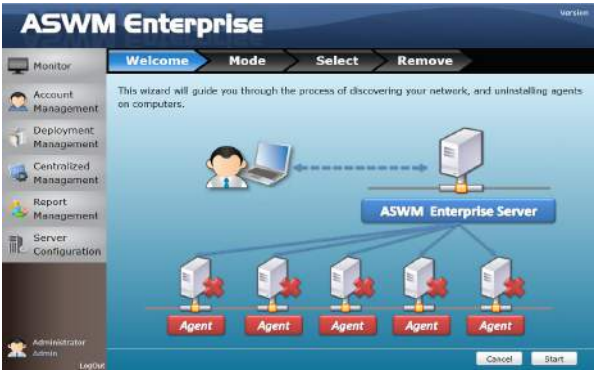
2.2.1 Scanning the self ASWM main server

To remove the existing agents

1. Click **Deployment Management** on the left.

2. Click **Remove ASWM Enterprise Agent**.

3. The wizard will guide you through the uninstallation process. Click **Start** to continue.



4. Click **Scan the self ASWM Enterprise Main Server** and click **Next** to continue. The system will scan the main server.

5. Select the desired computers for agent uninstallation and click **Start**.

You can easily select all computers, all offline computers or all online computers with the checkboxes on the bottom.

6. The server automatically removes the agents on the selected computers. When done, it shows **Success**. Click **Finish** to finish the process.

2.2.2 Automatically scanning the Active Directory

To remove the existing agents

1. Repeat the step 1—3 in the previous section.
2. Click **Automatically Scan the Active Directory** and click **Next** to continue. The system will scan the Active Directory.

3. All the computers in Active Directory are shown here, grouped by Support Status.

4. Select the desired computers for agent uninstallation and click **Start**.

5. The server automatically removes the agents on the selected computers. When done, it shows **Success**. Click **Finish** to finish the process.

Chapter 3

This chapter describes the Main Server Functions, including Monitor, Account Management, Deployment Management, Centralized Management, and Server Configuration.

Main Server Functions

3.1 Monitor

The overview screen gives you a quick overall status check for all the computers. You are also allowed to shut down, restart or start the selected computers.

To see the monitor overview

1. Click **Monitor** on the left.

2. Select a desired group from the **Group List**. The group clearly shows the information of **Client Counts**, **Connection**, **Health**, and **Utilization** status. (Red: Critical; Yellow: Warning; Green: Normal)

3. In the **Models In the XXX Group**, the general monitoring information of all computer in this group is displayed as shown, including Connection status, Model Name, Alias Name, Operating system, BMC WebGUI status, Health status.

- The crossed-out BMC card means that the BMC is not installed in that computer.
- If the status of BMC WebGUI shows **NO**, the WebGUI is inaccessible.
- When you click **BMC WebGUI**, a pop-up window appears. Ensure that your web browser does not block the pop-up window.
- The yellow warning icon indicates that you are not authorized to access BMC. Please check your BMC account privilege. You can set your BMC account information from **BMC** > **Authentication** page.

To shut down or restart the computer

1. Right-click the desired computer.

2. You can select **Restart** or **PowerOFF** if the computer appears online.
3. You can select **Maintain Mode** to enable or disable the Maintain Mode function.

PowerON is available only when the selected computer appears **Offline** and you have installed ASMB card on that computer or on our Thin Client product which has **Wake On LAN** function.

You can also power off or restart the selected computer after entering **Monitor**.

If you select **Maintain Mode**, the connection status between Thin Client and other servers will be recorded in **Agent Connection Report** and **Event Log** only, and will not trigger **Agent Connection Event Notification** (For more details, refer to section **3.5.3 Agent Connection Report Management** and **4.4 Event Log**).

3.2 Account Management

Account Management allows you to see the current login account and edit the account.

Only limited functions, including **Monitor** and **Account Management** are available when you login as a user. Other functions will be dimmed and become unavailable.

3.2.1 Current Login Account

Click Account Management on the left to display the **Login Account**, **Account** and **Role Privilege** tab, than click **Login Account** tab to display current Login Account.

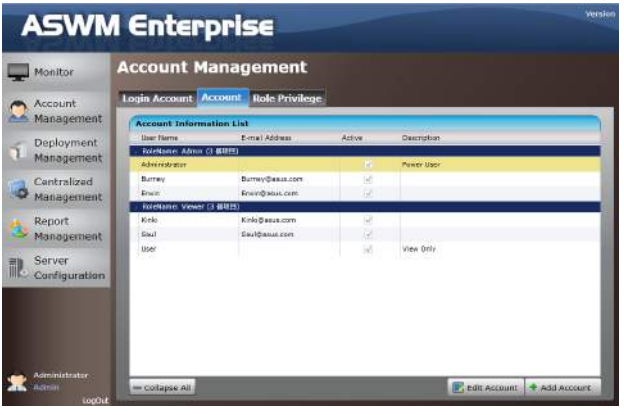
Editing the Login Account

Click **Edit Account** to edit the login account. Click **Save** when done.

The **Account E-Mail** shows in the **Email Settings** of **Client Configuration**.

3.2.2 Account

Click Account Management on the left to display the **Login Account**, **Account** and **Role Privilege** tab, than click **Account** tab to display Account Role and Account Role members of the account information.



You can click **Add Account** to add a new account. In **Edit Account** / **Add Account** of the **Account Role** section, you can specify the **Account Role** for this Account. The Administrator also can check / uncheck **Account** to enable or disable the account.

3.2.3 Role privilege

Click **Role Privilege** tab to display every role owns right of every model's function (a check mark indicate enable).

Administrator also can Add or modify the Role's right. (check / uncheck the role's right of there's function).

Click “**Add New Role”** shows as below.

3.3 Deployment Management

You can deploy ASWM Enterprise agents and remove agents through AD or manually. Refer to Chapter 2 for details.

3.4 Centralized Management

3.4.1 BIOS Flash Centralized Management

1. Click **Centralized Management** on the left and select **BIOS Flash Centralized Management**.

2. You can simultaneously on multiple Models for BIOS Flash. System will detect the latest BIOS files on ASUS official website and show the latest BIOS version in **LaestVersion** field.

   User can use check box to:
   Select all models which are online and can be update.
   Select all models which are online and can be update then TurnOnLED (LocatorLED) light and Reboot.(Locator LED can only be controled on the Model with BMC)

The Live Update function of BIOS Flash automatically detects the latest BIOS in ASUS support site. The new BIOS information will be displayed in the column of **LatestVersion**. Click the blue bar to view the release note of the BIOS version.

2. Click **Upadte BIOS** button to start BIOS Flash and show all models progress.

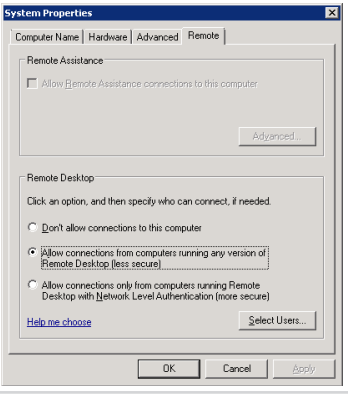
3.4.2 Remote Control Centralized Management

1. Click **Centralized Management** on the left and select **Remote Control Centralized Management**.

2. This show will follow the group under each Group based information.

3. Click **Connect** button can remote control the model.

You have to enable the Remote Desktop on your client computer before using the remote control function.



3.4.3 Power Control Centralized Management

1. Click **Centralized Management** on the left and select **Power Control Centralized Management**.

2. You can simultaneously turn on multiple Models for **Maintain Mode** or **Power Control**.

3. Click **Start** to enable/disable **Maintain Mode** or **Power Control** and show the progress status of all models.

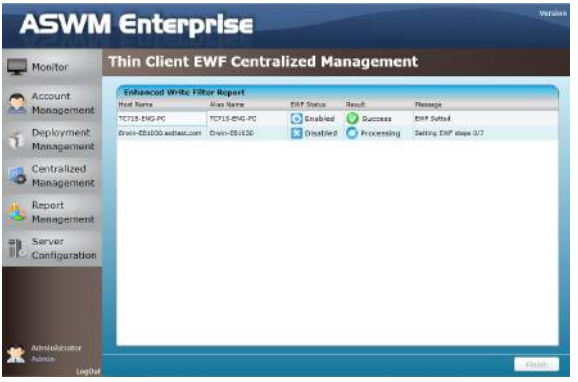
3.4.4 Thin Client EWF Centralized Management

If your Thin Client is embedded with Windows Embedded operating system, it can support EWF function. The centralized management interface allows you to manage multiple Thin Clients in a single page.

- When you select the group, only the Thin Clients with EWF support will be displayed.
- For more details, refer to section **4.12 ThinClient Features**.

The EWF centralized management allows you to enable or disable the EWF feature to all the disks in selected Thin Clients. When enabled, you can select to enable or disable the HORM (Hibernate Once Resume Many) function. Click **Start** to start the EWF changes in selected clients.

The EWF status displays as follows.



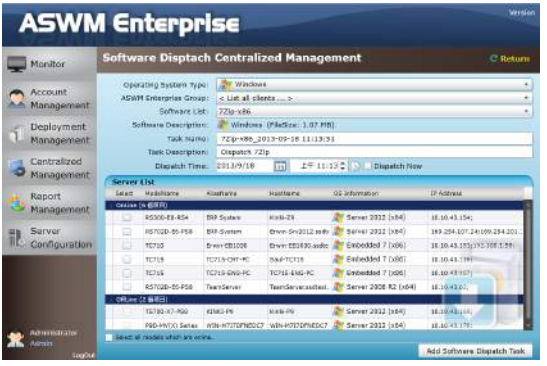
The Thin Client might restart several times during EWF configuration.

3.4.5 Software Dispatch Centralized Management

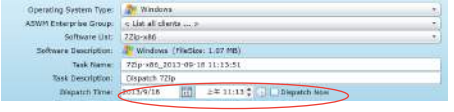
This function allows the administrators to dispatch one software to several clients.

1. Select software list (create in software pool) and the target clients.

> Refer to section **3.6.7 Software Pool** to create a software pool.



2. Set the dispatch time, or tick **Dispatch Now** to dispatch immediately.



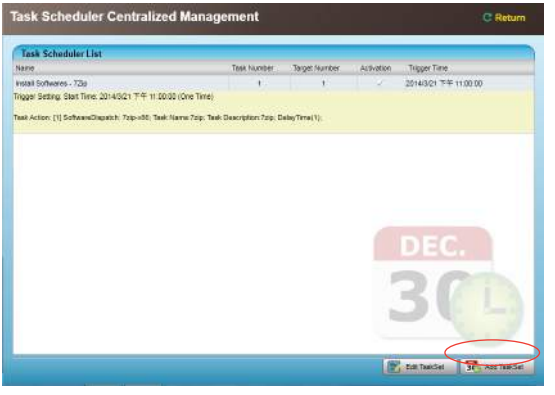
3. Click **Add Software Dispatch Task** to start the task. The software dispatch status is displayed.

3.4.6 Task Scheduler Centralized Management

This function allows the administrators to perform a specific task on a specific client on scheduled time or time cycle. These specific tasks include Power Control, Software Dispatch, Service Control, SecurityUSB and EWF.

1. Click **Centralized Management** on the left and select **Task Scheduler Centralized Management**.

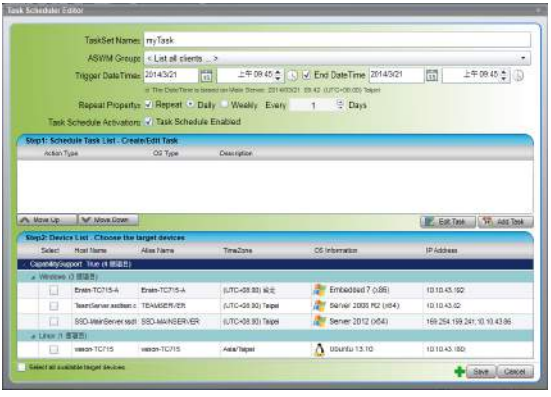
2. Click **Add TaskSet** or **Edit TaskSet** to add a new task schedule or edit an existing task schedule.



Scheduling a taskset

To schedule a taskset:

1. Click **Add TaskSet** and the following screen appears.



2. In the **TaskSet Name** field**,** assign the name for a task schedule.
3. In the **ASWM Groups** dropdown list, select the ASWM group for the task schedule.
4. In the **Trigger Date Time** field**,** set the start and end time for the task schedule.

Follow the system time of the Main Server installed with ASWM to set the trigger time, which should be later than the current time on the Main Server.

5. Tick **Repeat Property** to set the frequency for the task schedule.
6. Tick **Task Schedule Activation** to enable the task schedule.
7 When done, click **Save**.

Adding a task to the taskset

To add a task to the taskset:

1. In the **Task Scheduler Editor**, click **Add Task**. The following screen appears.

2. In the **Action Type** dropdown list, selects an action type from these five action types: Power Control, Software Dispatch, Service Control, SecurityUSB and EWF.

- **Power Control:** Allows you to set tasks of Power On, Power Off and Reboot control.

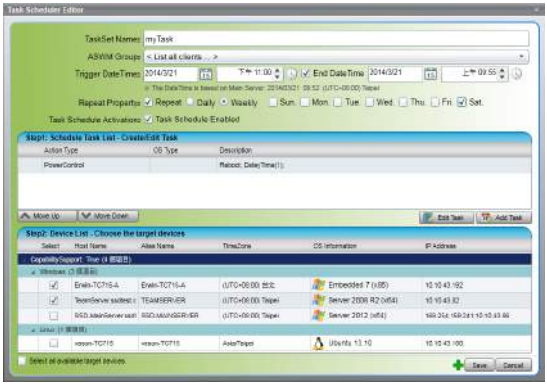
- **Software Dispatch:** Allows you to select a specific software from a software pool that you have established earlier.

- **Service Control:** Allows you to enter a name in the **Service Name** field and select the operation that you want to perform to the the service.

- **SecurityUSB:** Allows you to enable or disable the USB flash device.

- **EWF:** Allows you to enable or disable the EWF feature if the target client is a ThinClient supported by ASWM, and allows you to enable or disbale HORM when you have enabled EWF.

3. Select a property of your selected action type.
4. In the In the **Delay Time** field, set the time interval between this task and the previous one.
5. When done, click **Save**. The following screen appears.



Repeat the above steps if you want to add more tasks, and then select the target device that you want to perform the tasks on from the **Device List**.

The device in the **Device List** can be selected only when you have established an Action Type that it supports.

3.5 Report Management

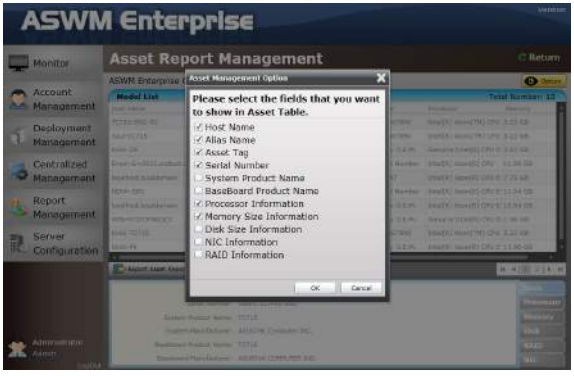
This function allows you to configure report management.

3.5.1 Asset Report Management

To configure asset report management:

1. View the **Asset Tag**, **Serial Number**, **Processor**, **Memory**, **Disk**, **RAID** and **NIC** Information.

2. Click the **Option** button to select the field that you want to show in the table.

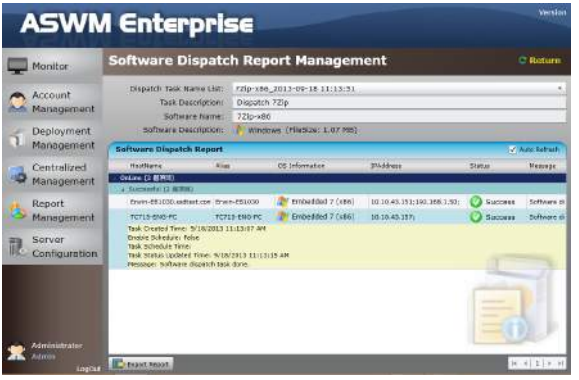


3.5.2 Software Dispatch Report Management

To configure the software dispatch report management:

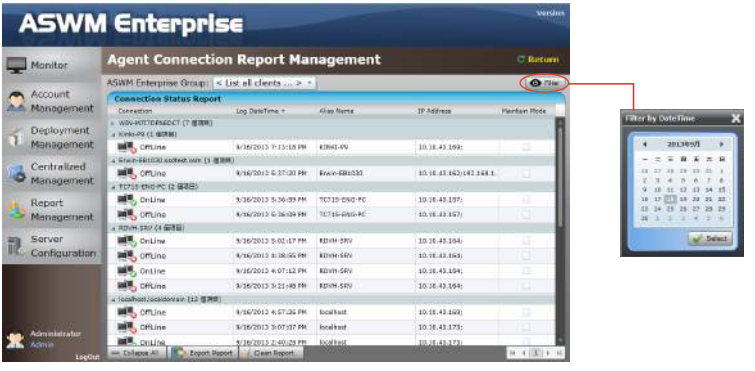
1. From the dropdown list, select the dispatch task name to view the dispatch status.

2. Tick **Auto Refresh** to refresh the dispatch status. Select the dispatch task whose detailed dispatch information you want to view. Click **Export Report** to export the current fields in .csv format.



3.5.3 Agent Connection Report Management

The **Agent Connection Report** lists the server's start and shutdown time and whether the client is in Maintain Mode.



Use the **Filter** function to list the continuous report after the specified date.

3.6 Server Configuration

You are allowed to do general server configurations, including SMTP server, SNMP Trap, security, etc..

3.6.1 SMTP Server

To set up the SMTP server

1. Setting up the correct SMTP server information if you would like to send the notification through Email. Click **Edit SMTP Setting** to fill in the fields.

2. Click **Send Test E-Mail** and enter a receiver's E-Mail to see if the SMTP server has been successfully set up. If so, click **Save** to save the configuration.

3.6.2 Security

You can set the Access Control List, which permits or denies the specific IPs' access.

The ACL settings is based on Cisco router settings. Fill in the blank fields and click **Add New ACL Rule** to add a IP on the control list. Use the **ACL Rule Test** on the bottom to test if it has been added successfully.

Click **Export ACL Rule** or **Import ACL Rule** to export or import ACL Rule.

Examples of ACL settings

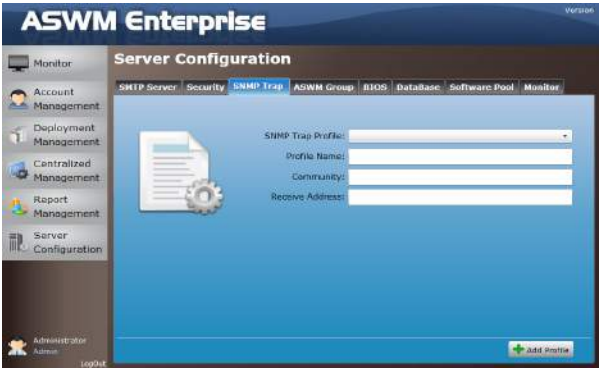
1. If you want to permit Class C IP addresses 192.168.0.0—192.168.0.255
   Rules:
   Permit: IP 192.168.0.0 Wildcard Mask: 0.0.0.255
   Deny: IP 0.0.0.0 Wildcard Mask: 255.255.255.255

2. If you want to permit IP 192.168.0.200 only
   Rules:
   Permit: IP 192.168.0.200 Wildcard Mask: 0.0.0.0
   Deny: IP 0.0.0.0 Wildcard Mask: 255.255.255.255

3. If you want to deny IP 192.168.0.200 only
   Rules:
   Deny: IP 192.168.0.200 Wildcard Mask: 0.0.0.0
   Permit: IP 0.0.0.0 Wildcard Mask: 255.255.255.255

3.6.3 SNMP Trap

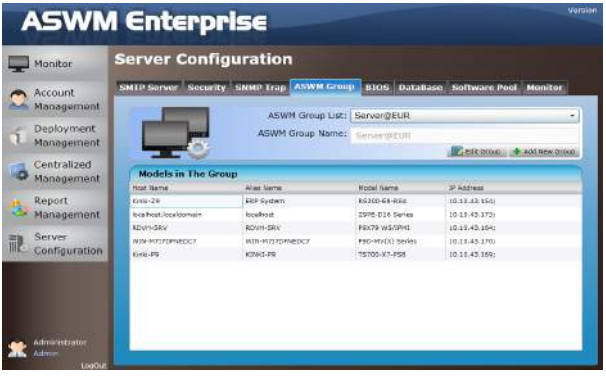
Fill in the blank fields and click **Add Profile** to add the SNMP Trap profile. If you would like to edit the profile, click **Edit Profile**.



The SNMP profile information is used for sending notificatiton.

3.6.4 ASWM Group

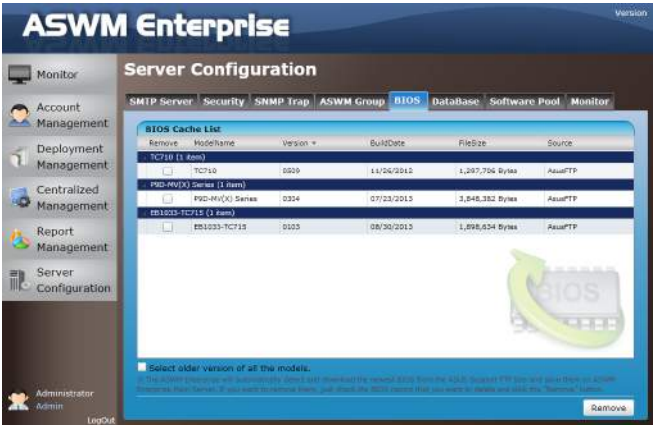
You can add new ASWM Groups or edit the existing groups. The information of computers in each group is displayed when the group is selected.



You cannot delete the **DefaultGroup** and all the clients will be regrouped under **DefaultGroup** when their groups are deleted.

3.6.5 BIOS

The BIOS screen displays all the BIOS cache information. The ASWM Enterprise automatically detect and download the newest BIOS from the ASUS support site.



It is more convenient to click the check box on the bottom to select the older version BIOS if you want to remove the older ones.

3.6.6 DataBase

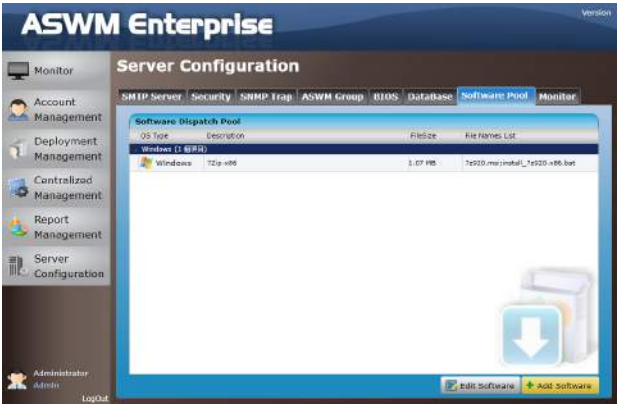
You can view the database information of ASWM Enterprise here.

3.6.7 Software Pool

This function allows you to create the software list from where you can select and dispatch the software to clients.

To set up a software pool:

1. Click **Add Software**.

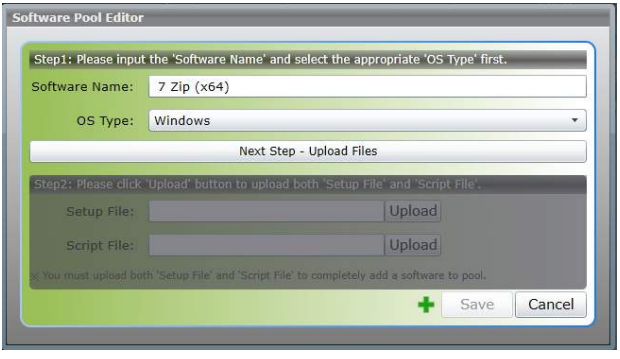


2. Assign the software name and click **Next Step - Upload Files**.

Two files must be uploaded:

A) Setup File, namely the installation file, including .exe, .msi, .msu and .zip (for several files) format

B) Script File, namely the silent installation script of the setup file, supports .bat file format.



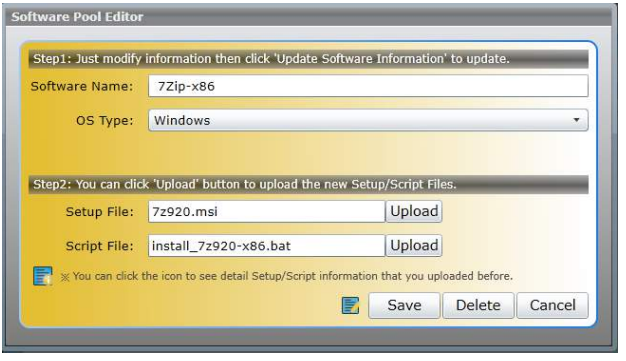
- To ensure a successful dispatch without uer's responding to the dispatch screen, it is recommended that you test the files before starting the large amount dispatch since the files will be dispatched to remote clients and the ASWM Agent will run the script to install the setup file, and that the script contains the silent install parameters.
  - For example, if you want to dispatch a 7zip file, you need to upload:

    Setup File: 7zip.exe

    Script File: Install.bat, containing 7zip.exe /S

If there are several setup files, you can pack these files in .zip format.

3. Click **Edit Software** to edit the software or upload the setup file, script file again.



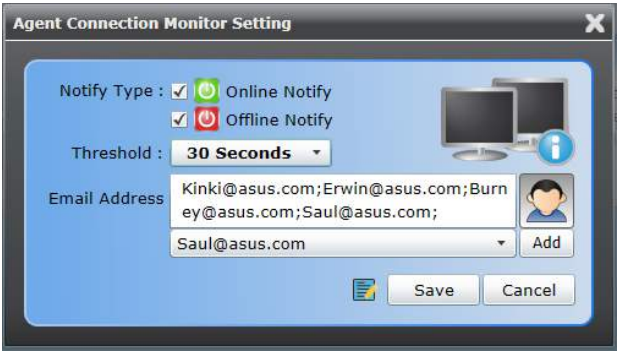
3.6.8 Monitor

You can enable or disable the Connection Monitor function that monitors the connection between Main Server and Agent. Click **Setting** to set the detailed monitor information.

Notify Type: online and/or offline notification;

Threshold: set the upper time limit for offline. For example, 30 seconds means the connection status will be seen as offline if the last connection between Agent and server is 30 seconds ago.

Email Address: The email address of the receiver who will receive the notification.



ASWM Enterprise Main Server routinely checks the status of Agent Connection. If the connection between Agent and Server breaks unexpectedly, the Main Server records and sends an email notification to the specified recipient. If the Server is in Maintain Mode, there will be only a record of the connection status.

Chapter 4

This chapter describes system status and information of the client.

Client Monitor Information

4.1 Monitor Overview

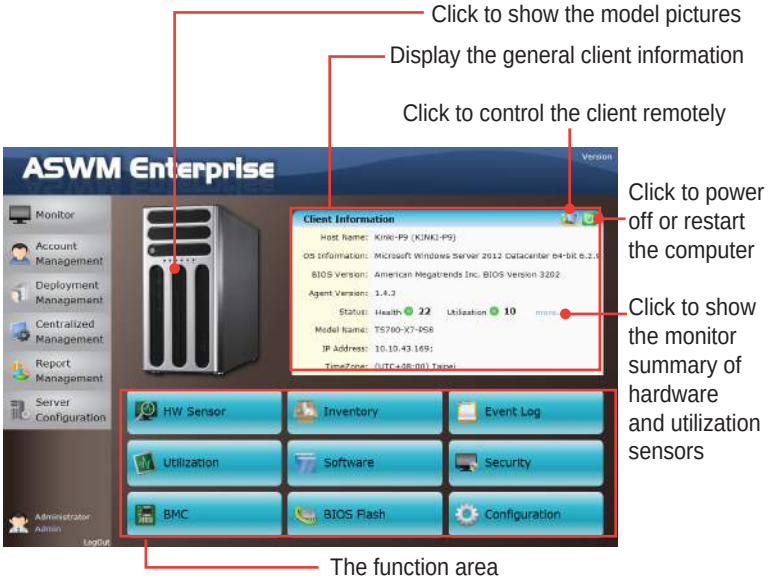
You can have detailed monitoring information of each client in realtime.

1. Click **Monitor** on the left.

2. Select a desired group from the **Group List**.

3. Select a desired client for monitoring in the **Group**

4. The Client Information of the selected computer is displayed as shown.



- The BMC button is available only when you have installed a BMC card on your client.
- Under **Client Informaiton > more...**, view the connection status of one or more network adapters on your client, such as if the ethernet cable is connected or disconnected, or if the network adapter is enabled or disabled.

4.2 HW Sensor

Hardware sensors are responsible for voltage, fans, temperature and backplanes monitoring. You can have a realtime notification of each component with colored signals or customize your warning threshold.

4.2.1 Setting thresholds

Click the dashboard to customized your own threshold value, including **High Critical**, **High Warning**, **Low Warning**, and **Low Critical**.

To set the threshold

1. Click a desired dashboard for customizing.
2. Move the slider to adjust the threshold value.
3. Click **OK** to save the configuration.

The value of **High Warning** must be lower than **High Critical** and the **Low Warning** must be higher than **Low Critical**.

4.2.2 Hardware sensor tabs

Voltage

Scroll down for more voltage dashboards or click **Return** to go back to the previous Client Information screen.

Fan

This screen displays the threshold fan status and power supply related discrete fan sensor.

Temperature

This screen displays the device threshold temperature and power supply related discrete temperature sensor.

Backplane

This screen displays the blackplane status, including **Drive Presence**, **Drive Not Exist**, **Fault**, and **Rebuild**. Click **Return** to to back to the previous Client Information screen.

This tab is only available when your system is equipped with backplanes.

Power Supply

This screen displays the power supply related sensor, for example, the power consumption (Watt), whether the power cord cable is connected to the power supply, and whether the power supply is installed to the server properly. Click **Return** to the previous Client Information screen.

Chassis

This screen displays the chassis status. If the chassis of the client computer is opened, the ChassisIntrusion Lock icon will appear unlocked. Click **Return** to the previous Client Information screen.

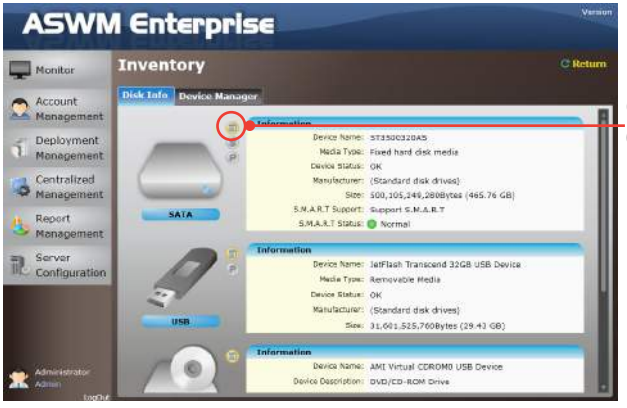
4.3 Inventory

Inventory shows the general disk info of your installed Hard disk drive, optical disk drive and the connected external disk drive.

4.3.1 Disk Info

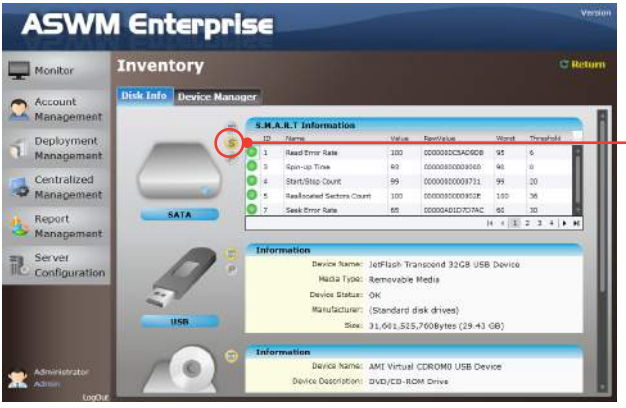
Disk Information

The disk information screen includes **Name**, **Media Type**, **Status**, **Manufacturer**, **Size**, **S.M.A.R.T Support** and **S.M.A.R.T Status**.



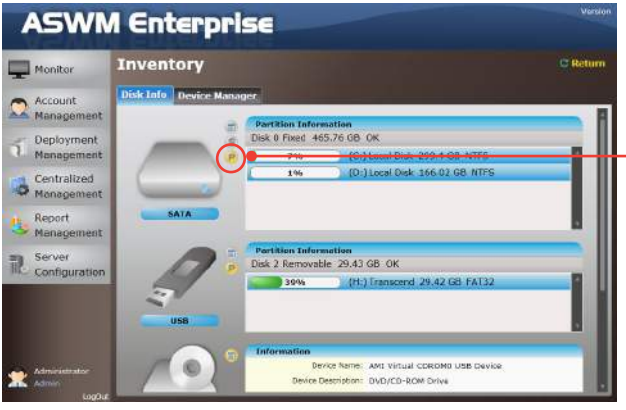
Scroll down for more items.

S.M.A.R.T Information



Click to show SMART information

Partition Information



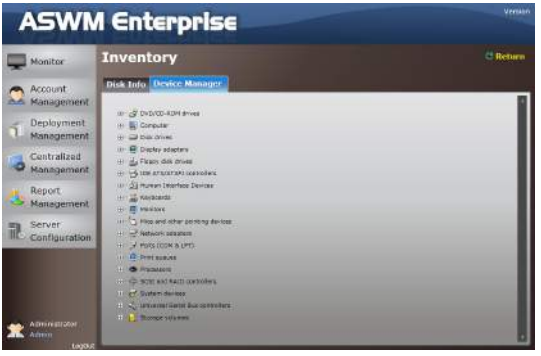
Click to show Partition information

4.3.2 Device Manager

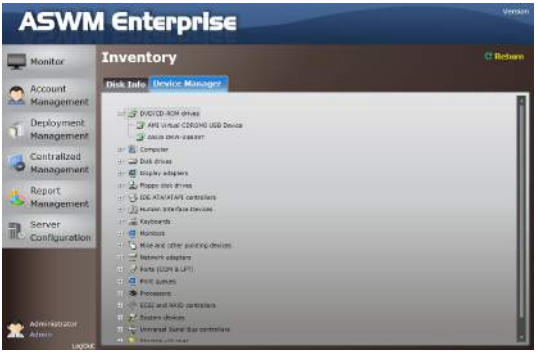
The Device Manager displays all the devices installed on the client PC.

To check device properties

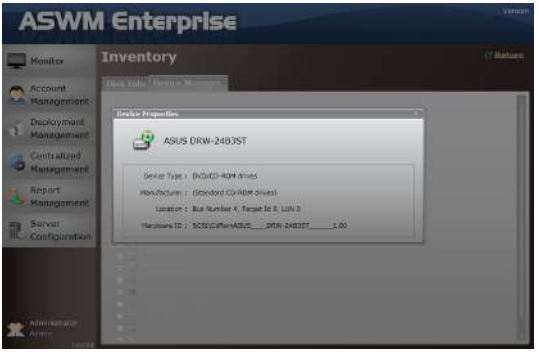
1. Click **Device Manager** tab on the top.



2. Click the desired category to expand and show the devices.



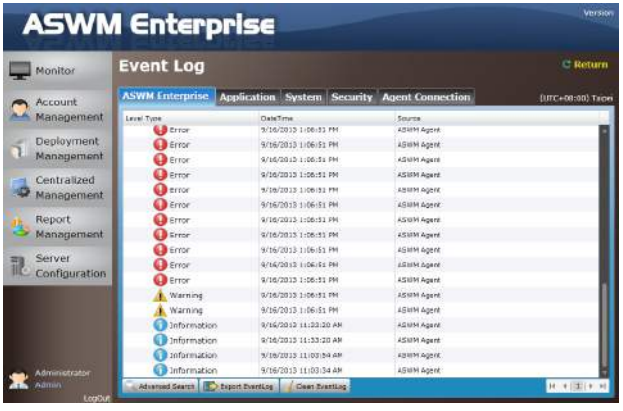
3. Click the device to show the device properties.



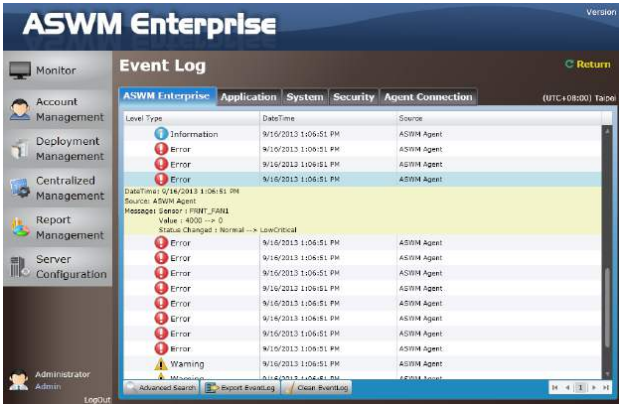
4.4 Event Log

ASWM Enterprise automatically creates and records all the significant events happening on your system in the event logs. Click the tabs (**ASWM Enterprise**, **Application**, **System**, **Security** and **Agent Connection**) on the top to browse different categories. The level types are **Information**, **Warning** and **Error**.

ASWM Enterprise Main Server routinely checks the status of Agent Connection. If the connection between Agent and Server breaks unexpectedly, the Main Server records and sends an email notification to the specified receiver. For more details, recer to section **3.6.8 Monitor**.

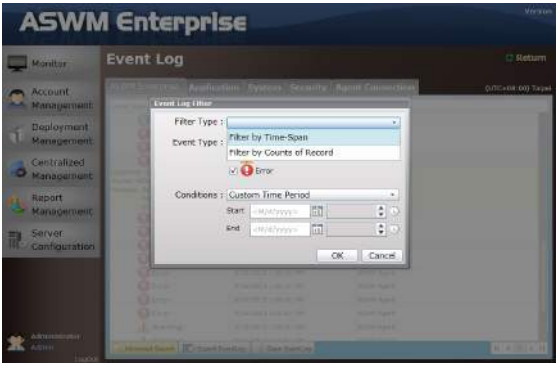


Click a desired log to see the detailed information.



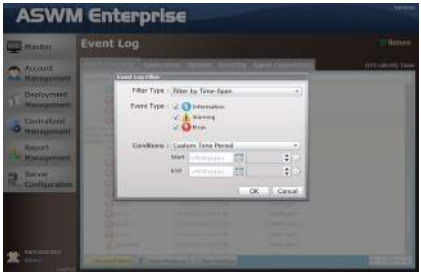
Advanced Search

Click **Advanced Search** to use the **Event Log Filter** to locate your desired log more quickly.



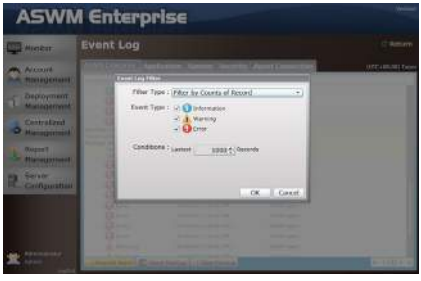
Filtering by Time Span

If you select **Filter by Time Span**, you can decide and search your desired time period for the logs.



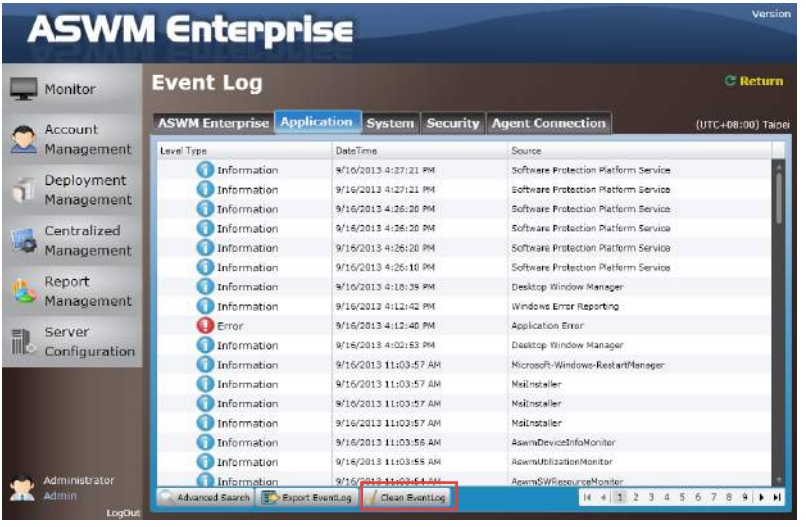
Filtering by Counts of Record

If you select **Filter by Counts of Record**, you can decide the number of the logs you would like to see. Click the arrow buttons to increase or decrease the number, or you can enter a desired number directly.



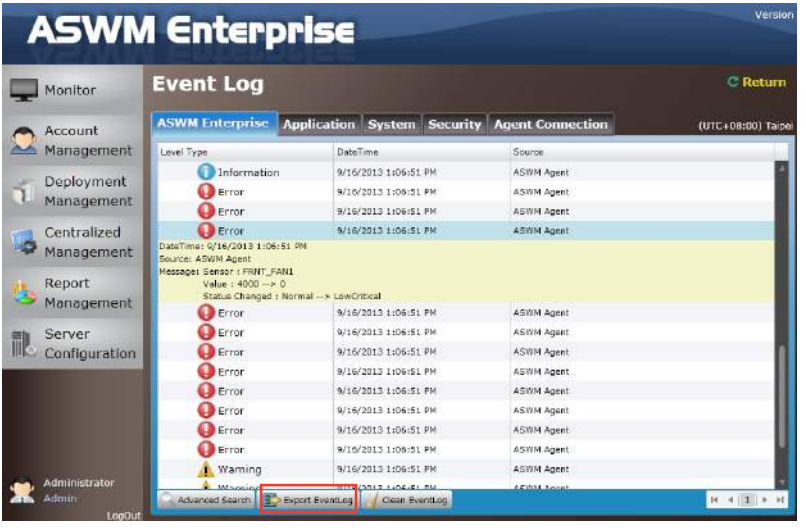
Clean EventLog

Click **Clean EventLog** to clear all the event logs stored in your client PCs.



Export EventLog

Click Export EventLog to export a *.csv file to your client PC.



4.5 Utilization

Utilization Sensor shows the utilization status of disk drives, CPU, Memory and Network. You can customized the threshold value of each sensor for sending notifications.

4.5.1 Partition

The Partition screen shows the information of your installed hard disk drives and the connected external storage devices. Move the slider under each disk drive to set the warning threshold.

4.5.2 CPU

This screen shows the CPU usage of each installed CPU.

The number of the CPU here is the logical number of the CPU, not the number of the installed CPU.

4.5.3 Memory

This screen shows the total physical memory, used memory, the available memory, and the memory utilization status.

4.5.4 Network

This screen shows the general information of the network and the network utilization status.

4.6 Software

Click **Auto Refresh** to refresh the monitoring screen automatically.

4.6.1 Application

Displays all the installed applications on this client and their general information.

4.6.2 Service

Displays the status of each installed applications. Right-click a desired service and you can start, restart or stop the selected service.

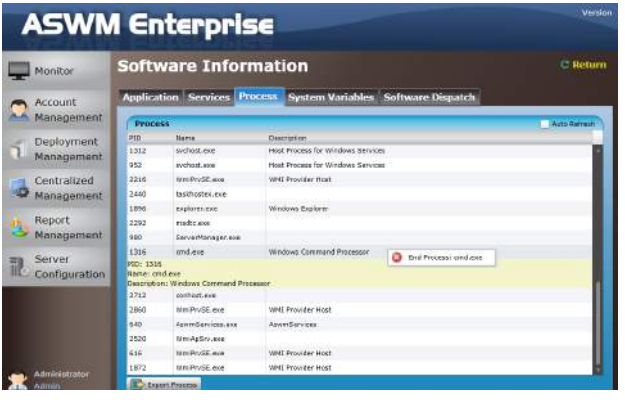
If the **Start Mode** of the selected service shows **Disabled**, you cannot control that service.

4.6.3 Process

Displays the process of the running applications.

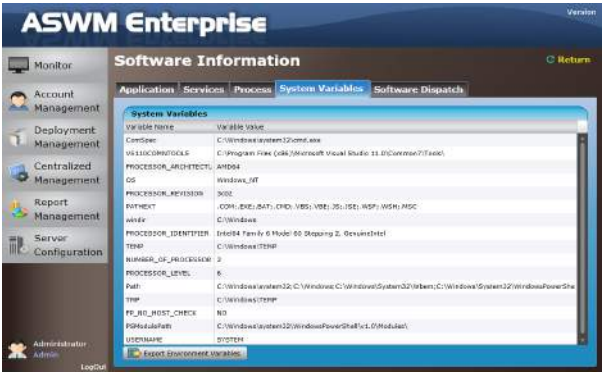
To end the process of the running application

1. Right-click the application that you would like to end the process.
2. Select **End Process:XXXXX** to stop the application running.



4.6.4 Environment Variables

Displays the environment variables.



4.6.5 Software Dispatch

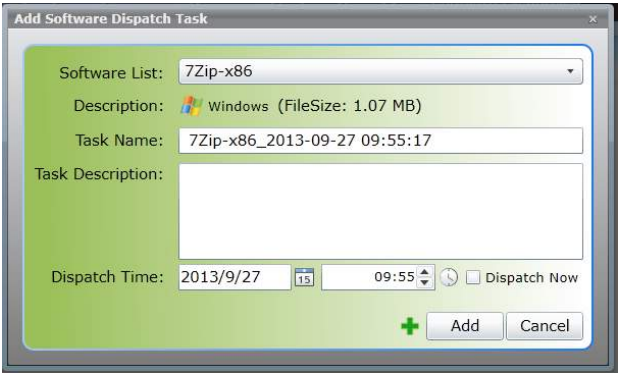
Software Dispatch allows you to dispatch an application to the assigned clients. To use this function, add a new dispatch task that includes the application name created in the software pool, the target client, and the dispatch time.

- Refer to section **3.6.7 Software Pool** to create a software pool.
- Refer to section **3.4.5 Software Dispatch Centralized Management** if you want to dispatch a large amount of softwares to several clients simutaneously.

To usesoftware dispatch:

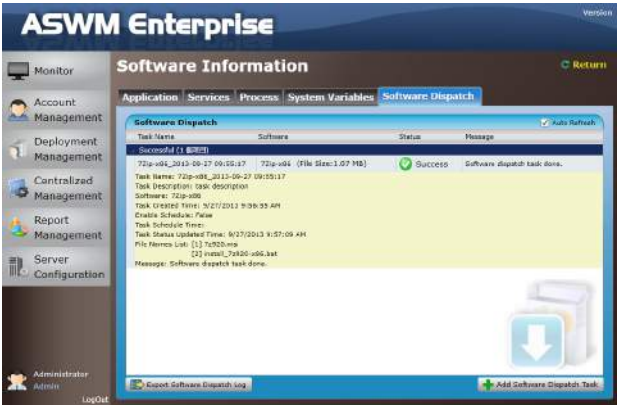
1. Click **Add Software Dispatch Task**.

2. From the Software List dropdown field, select the software that you want to dispatch to a client and enter a task name and task discription.
3. Assign the dispatch time or tick **Dispatch Now** to dispatch immediately.



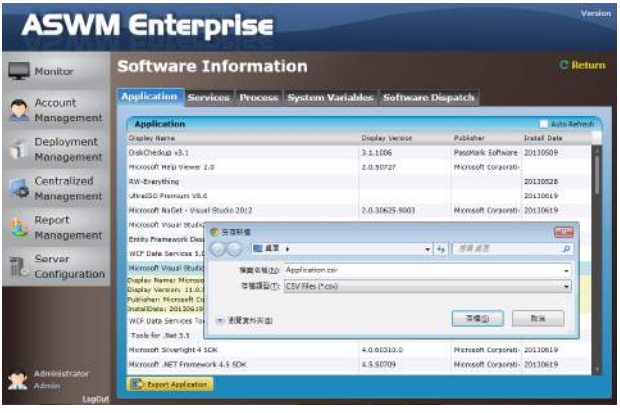
4. Click **Add** when done. The dispatch status for the newly-created dispatch task is displayed on the task list.

5. When the dispatch task is completed, the dispatch status is displayed on the task list. Click the dispatch status to display the dispatch task's detailed information.



4.6.6 Export function

Click **Export** button to export a *.csv file.



4.7 Security

Security function allows you to manage your USB Flash and Registry Tool safely.

USB Flash management

Use this function to prevent other users from copying the files in the Client to their USB flash disks. Follow the steps below:

1. Click **USB Flash** tab to view the status of the uSB flash disk.

2. Click **Edit USB Flash Setting** if you want to change the current status. When done, click **Save**.

Regedit Tool

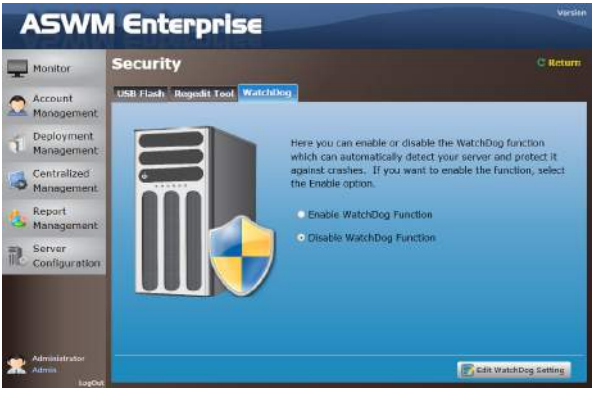
Regedit.exe is a built-in registry editor in Windows OS. To improve the system security, follow the steps to disable the Regedit.exe in Windows OS:

1. Click the **Regedit Tool** tab to view the status in Regedit Tool.

2. Click **Edit Regedit Tool Setting** to change the current setting. When done, click **Save**.

WatchDog

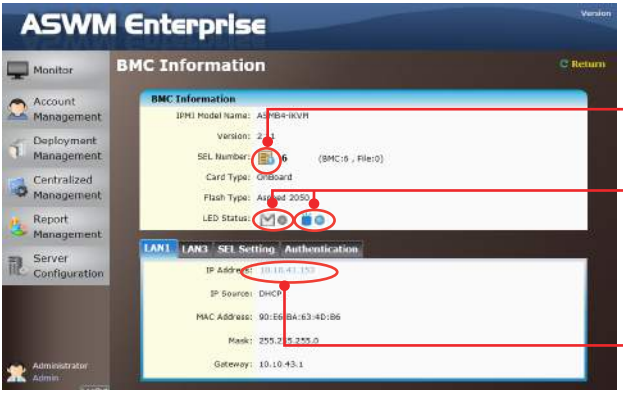
Watchdog automatically detects your server and protects it against crashes. Select enable/disable to enable or disable this function.



4.8 BMC

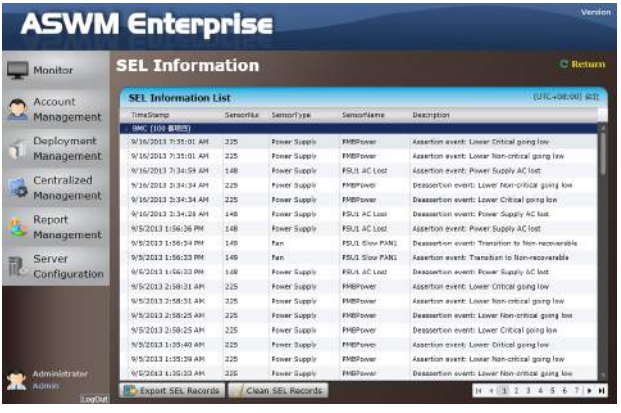
BMC Information displays the general information of the installed BMC card.

This button is available only when you BMC card to the client computer.



Ensure that your web browser does not block the pop-up window.

Click 654 to check the SEL (System Event Log) records of BMC, click **Export to SEL Records** to export the SEL to a CSV file, or click **Clean SEL Records** to clean the SEL of BMC.



SEL Setting allows you to enable or disable the SEL Backup Function, and set the upper limit of SEL usage.

When SEL entries in IPMI device reach the upper limit of SEL Usage (in percent), the ASWM Enterprise will backup and then clean them until the remaining occupies a lower ratio (in percent) of SEL usage.

Authentication allows you to set the user name and password of a BMC account. The on the **Authentication** tab indicates that you are not authorized to access the BMC. Click **Edit Account** to update the user name and password of the BMC account.

4.9 BIOS Flash

BIOS Flash screen displays your current BIOS information and you can configure the settings of BIOS Flash.

Click **BIOS Flash Type** > **Manual Upload BIOS ROM File** to manually upload the BIOS ROM, or select **ASUS BIOS Live Update** to automatically detect and download the latest BIOS from ASUS Support Website.

- Click **Reboot After BIOS Flash** if you would like to reboot your system after updating the BIOS.
- If you have installed BMC card to your system, you can click to turn on the **Locator LED** if needed.

The latest BIOS version will be displayed if the new BIOS is detected. You can also click The Latest BIOS Version: 0505 to check the release note of this version.

4.10 Configuration

4.10.1 Information

Click **Edit Information** to relocate this client computer to another group or change its **Alias Name**.

Click **Uninstall Client** if you want to remove the ASWM Enterprise Agent from this computer.

Add or delete groups in **Server Configuration** > **ASWM Group**.

4.10.2 Network

You can remotely control the network to enable / disable the DHCP, configure IP addresses and DNS, and change the Subnet Mask and Default Gateway.

The **Enable connection failure recovery** setting ensures that if the network configuration test fails, the system will automatically revert to the original network settings.

4.10.3 Notification

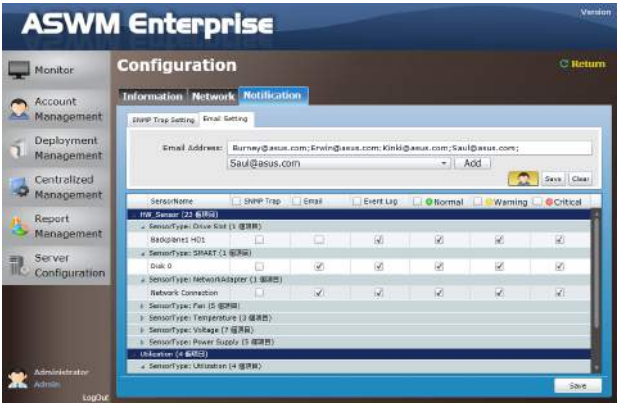
You can set up the notification types, including sending SNMP Traps and Emails, or you can just keep the event logs.

SNMP Trap Setting

You can manually enter the **Community** and **Receive Address** of SNMP Trap or click the amplifier button to select the built SNMP Trap profile.

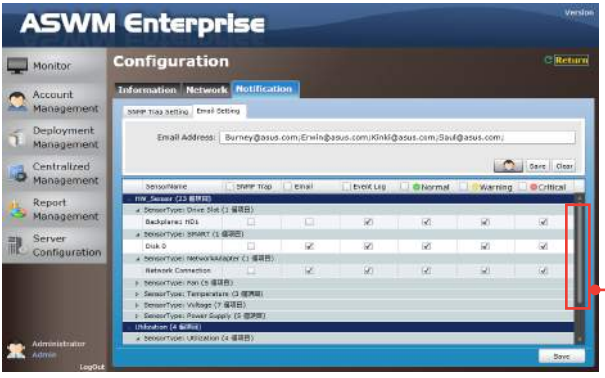
Email Setting

You can select the E-mail address from your contacts or manually enter the E-mail address. Use semicolons if you have more than one receivers.



Customizing notifications for each sensor

You can the select the notification methods of each sensor, Hardware and Utilization.

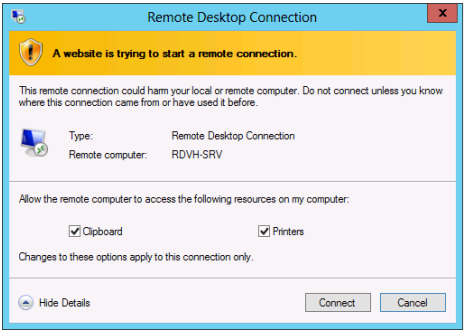


The Network Adapter Sensor monitors the connection status of one or more network adapters on the client, such as if the network cable is connected or disconnected, or if the network adapter is enabled or disabled. When the connection status is changed, the server records and sends out an e-mail notification to the specified recipient.

4.11 Remote Control

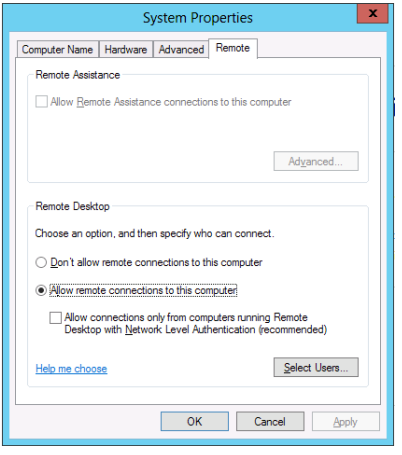
Remote Control allows you to open the Remote Desktop and control the client remotely.

1. Click **Connect** to allow the **Remote Desktop Connection**.



2. Cofirm the name of the remote computer and click **Connect** to start the connection.

You have to enable the Remote Desktop on your client computer before using the remote control function.



4.12 ThinClient features

When monitoring a ThinClient, the Function Area will be different from that of a Server's function area in the following:

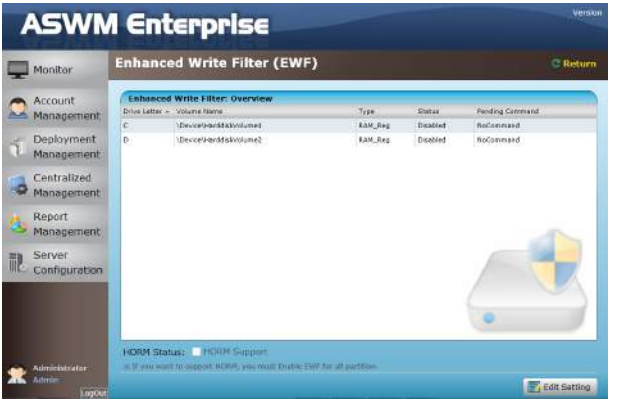
1. **HW sensor** changes to **EWF** (see below)
2. **BMC** changes to **Security** (see below)

The ThinClient is powered on through WOL, ensure that the Switch / Router can forward WOL packet.

4.12.1 EWF (Enhanced Write Filter)

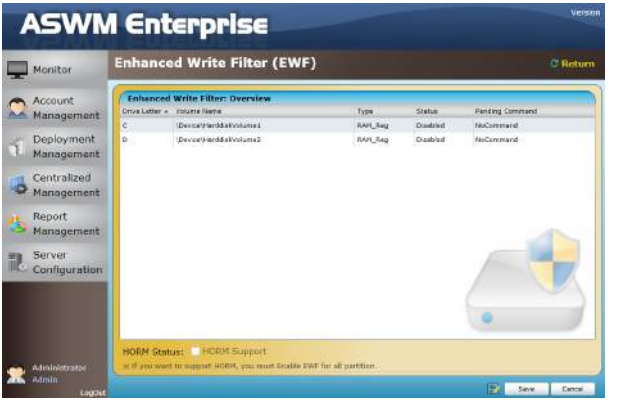
When monitoring the ThinClient, you can view and configure the EWF (Enhanced Write Filter).

EWF (Enhanced Write Filter) function protects one or several partitions against from being writting in.

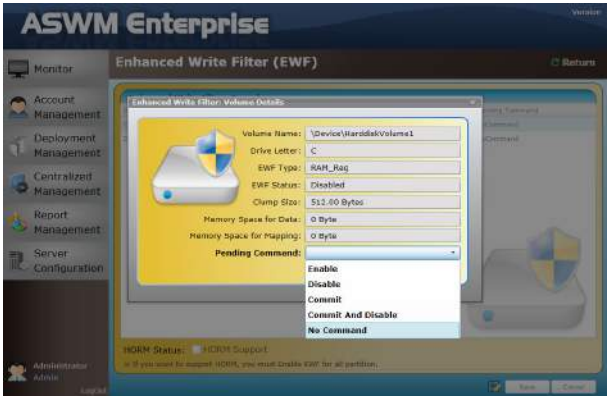


To configure the EWF:

1. Click **Edit Setting** to configure EWF. The background turns to yellow and the EWF become configurable.



2. Double-click the Partition that you want to change the EWF. When the EWF configuration dialog box appears, select different options from the Pending Command dropdown list to change the partition's EWF status, including:
   - No Command: Keeps current EWF or removes the previous Pending Command).
   - Enable: Enables EWF.
   - Disable: Disables EWF.
   - Commit And Disable: Write the changes of all the files to the hard drive and disable EWF.



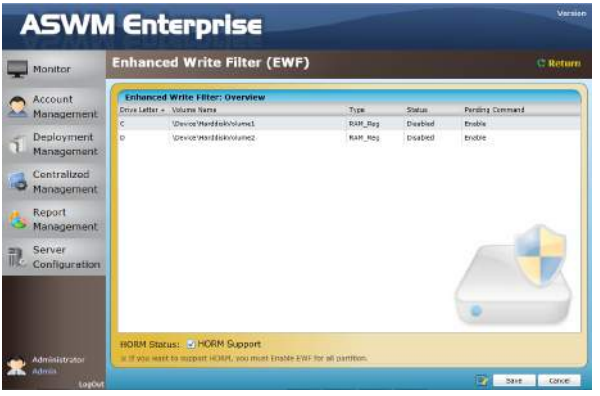
3. When finish, click **Save** to save the changes.

Configure HORM (Hibernate Once, Resume Many)

1. You can configure HORM while setting EWF. Ensure to enable EWF of each partition when enabling HORM function.

While enabling the HORM function, put the system to hibernate mode..

2. After finish configuring EWF and HORM, click **Save** and the Client settings will update immediately.



The Client may reboot for one or several times for the EWF configuration to take effect.

Appendix

This appendix includes a glossary of terms used in this document.

Reference information

A.1 Glossary

Community

Users can define their own SNMP trap community for a clearer categorization and convenient management of SNMP traps.

Backplane

A circuit board with sockets in which additional devices can be plugged.

Event Notifier

This sends a message to administrators/users When sensors detect changes in the system.

IIS

Internet Information Server. A web server built into Windows NT and later.

IPMI

Intelligent Platform Management Interface. It is a type of firmware which continues to monitor the system's hardware even after a crash or the system has shut down.

Service

A Windows program that runs in the background to perform a certain function when required such as programs for handling print jobs, e-mail or network connectivity.

SMTP

Simple Mail Transfer Protocol. The protocol used for transferring e-mail over a network.

SNMP

Simple Network Management Protocol. A TCP/IP protocol that transmits hardware or software status messages over the Internet.

A.2 Agent Function Comparison Table

Function Category	Modules	Sub-items	Agent Type		
			Win (Server)	Win (TC)	Linux
Monitor	OverView		•	•	•
	Client Detail Information		•	•	•
	HW Sensor	FAN	•		•
		Temperature	•		•
		Voltage	•		•
		Backplane	•		•
		Chassis Intrusion	•		•
		Power Supply	•		•
		Network Adapter	•	•	
	Inventory	Disk Information	•	•	•
		Device Management	•	•	
	Event Log	ASWM Log	•	•	
		System	•	•	
		Application	•	•	
		Security	•	•	
		Agent Connection	•	•	•
	Utilization	CPU	•	•	•
		DIMM	•	•	•
		Network	•	•	•
		Partition	•	•	•
	Software	Application	•	•	
		Service	•	•	
		Process	•	•	
		Environment Variables	•	•	
		Software Dispatch	•	•	
	Remote Control		•	•	
	BMC	Basic Information	•		•
		LAN Information	•		•
		BMC SEL	•		
		Task Scheduler	•	•	•
		Authentication	•		•
		SEL Setting	•		
	BIOS Flash	BIOS Information	•	•	•
		WinFlash	•	•	
	Power Control	Reboot	•	•	•
		Shutdown	•	•	•
		Power On	•	•	•
	EWF			•	
	Security	USB Control	•	•	
		Registry Control	•	•	
	Configuration	Notification	•	•	
		Network	•	•	
		Client Information	•	•	•

Function Category	Modules	Sub-items	Agent Type		
			Win (Server)	Win (TC)	Linux
Deployment Management	Deploy New Agent	Automatically Deploy	•	•	
		Manually Deploy	•	•	
		Discover Clients with preload service		•	
	Remove Agent	Remove Agent on main server	•	•	•
		Remove Agent by Scanning the AD	•	•	
Centralized Management	BIOS Flash		•		
	Remote Control		•	•	
	Power Control		•	•	•
	Thin Client EWF			•	
	Task Scheduler		•	•	•
	Software Dispatch		•	•	
Report Management	Asset Report Management	Basic Information	•	•	•
		Processor	•	•	•
		Memory	•	•	•
		Disk	•	•	•
		RAID	•	•	•
		NIC	•	•	•
	Software Dispatch Report Management		•	•	
	Agent Connection Report Management		•	•	•

ASUS contact information

ASUSTeK COMPUTER INC.

Address	15 Li-Te Road, Peitou, Taipei, Taiwan 11259
Telephone	+886-2-2894-3447
Fax	+886-2-2890-7798
E-mail	info@asus.com.tw
Web site	www.asus.com.com/

Technical Support

Telephone	+86-21-38429911
Fax	+86-21-5866-8722, ext. 9101#
Online support	http://www.asus.com/tw/support/

ASUSTeK COMPUTER INC. (Taiwan)

Address	15 Li-Te Road, Peitou, Taipei, Taiwan 11259
Telephone	+886-2-2894-3447
Fax	+886-2-2890-7798
E-mail	info@asus.com.tw
Web site	http://www.asus.com/tw

Technical Support

Telephone	+886-2-2894-3447 (0800-093-456)
Online Support	http://www.asus.com/tw/support/

ASUSTeK COMPUTER INC. (China)

Address	No.508, Chundong Road, Xinzhuang Industrial Zone, Minhang District, Shanghai, China.
Telephone	+86-21-5442-1616
Fax	+86-21-5442-0088
Web site	http://www.asus.com.cn/

Technical Support

Telephone	+86-21-3407-4610 (400-620-6655)
Online Support	http://support.asus.com/techserv/techserv.aspx

ASUS contact information

ASUS COMPUTER INTERNATIONAL (America)

Address	800 Corporate Way, Fremont, CA 94539, USA
Fax	+1-510-608-4555
Web site	http://www.asus.com/us/

Technical Support

Support fax	+1-812-284-0883
General support	+1-812-282-2787
Online support	http://www.service.asus.com/

ASUS COMPUTER GmbH (Germany and Austria)

Address	Harkort Str. 21-23, 40880 Ratingen, Germany
Fax	+49-2102-959911
Web site	http://www.asus.de
Online contact	http://www.asus.de/sales

Technical Support

Telephone	+49-2102-5789555
Support Fax	+49-2102-959911
Online support	http://www.service.asus.com/