v1.0

ReShield Control Center

User Guide

Contents

Contents

Chapter 4: Centralized Management

Contents

Chapter 7: Server Configurations

Appendix

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 ReShield Control Center, and how to install it.

Chapter 2: Deployment

This chapter describes how to deploy ReShield Control Center agents and remove agents through Microsoft® Active Directory or manually. You may also add and manage agentless VMware or digital signage devices.

Chapter 3: Device Monitoring

This chapter describes the various monitoring tools and options available.

Chapter 4: Centralized Management

This chapter describes centralized management of metadata, security, software, and tasks of the ReShield Control Center.

Chapter 5: Notification Settings

This chapter describes setting the notifications and SMTP Server

Chapter 6: Account Management

This chapter describes how to add and edit accounts for different users.

Chapter 7: Server Configurations

This chapter describes system configuration options, and license information.

Appendix

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.

DANGER/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 additional information to help you complete a task.

Typography

Bold text	Indicates a menu or an item to select.
Italics	Used to emphasize a word or a phrase.
<Key>	Keys enclosed in the less-than and greater-than sign means that you must press the enclosed key. Example: <Enter> means that you must press the Enter or Return key.
<Key1>+<Key2>+<Key3>	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: <Ctrl>+<Alt>+<Del>
`Command`	Means that you must type the command exactly as shown, then supply the required item or value enclosed in brackets. Example: At the DOS prompt, type the command line: **`format A:/S`**

Reference

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

Chapter 1

This chapter provides an overview of ReShield Control Center, and how to install it.

Getting Started

1.1 Introduction to ReShield Control Center

Welcome! The ReShield Control Center is a server management solution that gives a vital distinction to our servers, and is also compatible with our ReShield commercial products. 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 monitoring tool. The ReShield Control Center is a web-based interface that allows system administrators to conveniently manage computers either locally or remotely using a web-browser. With its colorful, graphical, and informative interface, the ReShield Control Center makes server management a delightful experience!

1.1.1 How ReShield Control Center works

The ReShield Control Center is composed of “agents” that generally act as data collectors, 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 ReShield Control Center, 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 ReShield Control Center 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, ReShield Control Center acts as an active guardian of the system’s key components.

1.1.2 ReShield Control Center

Licensing ReShield Control Center provides three license editions:

- **Classic edition** for assisting management on ReShield servers and workstations.
- **CSM edition** for enterprise level management suitable for enterprises, medium, or small businesses.
- **Enterprise edition** for a comprehensive management on ReShield servers and workstations, and all supported ReShield commercial products.

Features		Classic	CSM	Enterprise
Monitor (Overview)	Mission Center	√	√	√
	System Overview	√	√	√
	VM Overview	-	-	√
Monitor (one node)	Host Information	-	-	√
	Signage Information	-	-	√
	Device Information	√	√	√
	Hardware Sensor	√	√	√
	Utilization	√	√	√
	Inventory	-	√	√
	BMC	Partial functions unavailable	-	√
	Software	Partial functions unavailable	√	√
	Event Log	Partial functions unavailable	Partial functions unavailable	√
	BIOS	-	√	√
	Security	-	√	√
	Configuration	√	√	√
	Power Control	√	√	√
	Remote Control	-	√	√
Deployment	Agent Management	√	√*	√
	Agentless Management	-	-	√
Centralized	Metadata Management	√	√	√
	BIOS Flash Management	-	√	√
	Security Management	-	√	√
	Software Dispatch	-	√	√
	Task Scheduler	-	√	√
Notification	SMTP Settings	-	√	√
	Rule Management	-	√	√
Account	Accounts Management	-	√	√
	Role Privilege	-	√	√

(continued on the next page)

Features		Classic	CSM	Enterprise
Options	General Configuration	-	√	√
	Network Configuration	-	√	√
License	License	√	√	√
Update	Update	-	√	√

*** Please contact your local ReShield Sales representative and/or TPM for more information on the availability of other functions this feature supports.**

1.2 ReShield Control Center installation

ReShield Control Center is a virtual appliance running on a virtual machine (VM), with all required services and settings pre-installed. The system requirements can be found in the **Appendix** section of this manual.

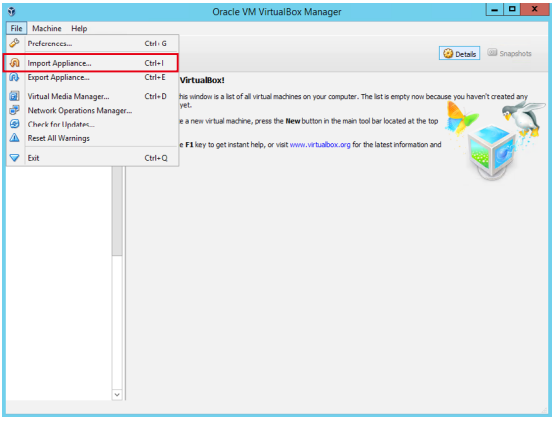
To install the ReShield Control Center on the Oracle VirtualBox, follow the steps below:

1.2.1 Deploying the OVA file

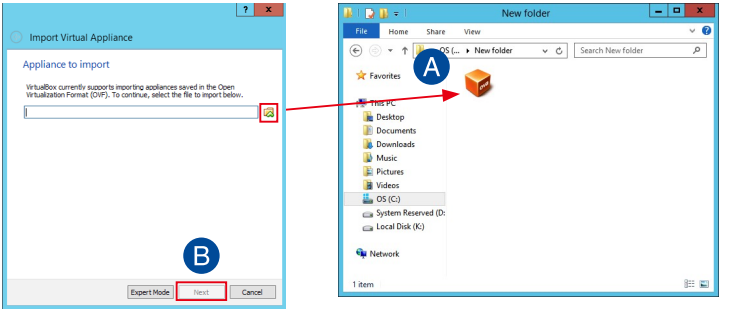
1. Download **Oracle VirtualBox** and the **ReShield Control Center** OVA file.

- Please refer to http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html to download **Oracle VirtualBox**.
- Please refer to http://reshield.nav-it.ru/index.php/upravlenie-serverami/reshield-control-center to download the **ReShield Control Center** OVA file.

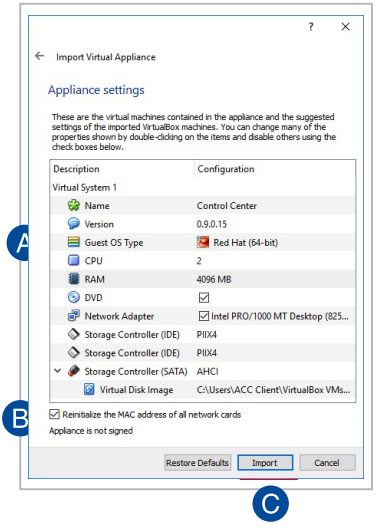
2. Install and launch **Oracle VirtualBox**, then select **File** > I**mport Appliance...** to launch the **Import Virtual Appliance** wizard.



3. Select the OVA file to import (A) and click **Next** (B).



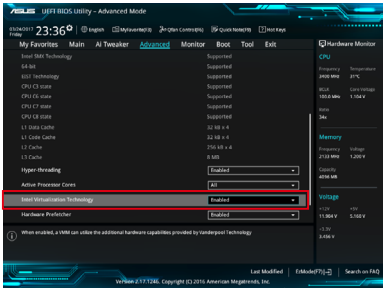
4. Ensure the **Guest OS Type** is set to **Red Hat (64-bit)** (A).
5. Check the **Reinitialize the MAC address of all network cards** checkbox (B), then click **Import** (C).



6. Wait for the appliance to be imported. This may take a few minutes.
7. Select the VM on the list, then click **Start** on the toolbar to start the VM.

If your **Oracle VirtualBox** installation was unsuccessful, please check the following:

- VT-x: **BIOS** > **Advanced** > **Intel Virtualization Technology** > **Enabled**

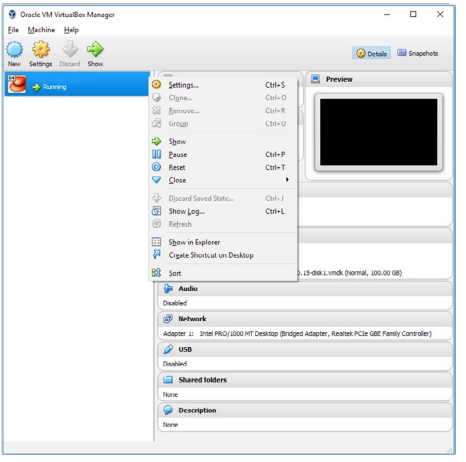


- Network Card: Select the network connection you are currently using.

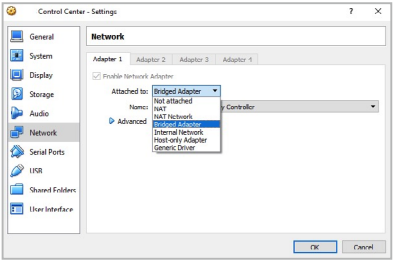
1.2.2 Setting the Network Settings for your VM

A message may appear when starting up the VM for the first time, follow the steps below to set up the network settings:

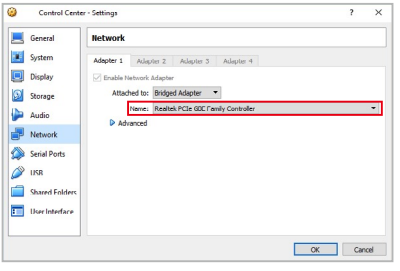
1. Launch your VM, then right click on the OVA and select **Settings**.



2. Select **Network** from the menu list on the left, then select **Bridged Adapter** in the **Attached to:** field.



3. Select the Network card you are currently using from the drop down menu in the **Name:** field.

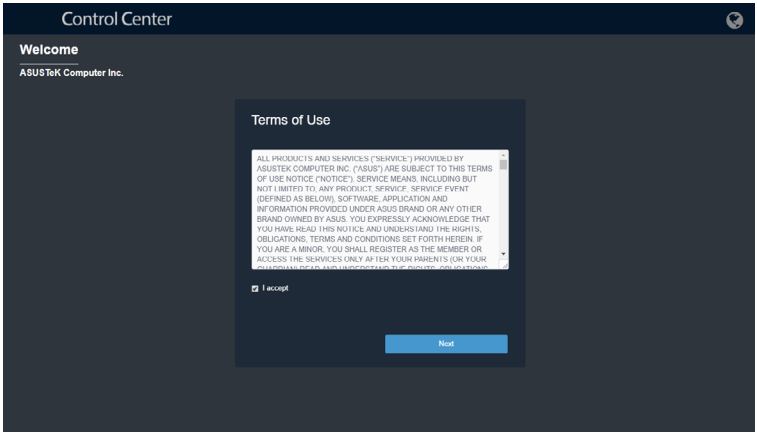


1.2.3 Initialize startup settings

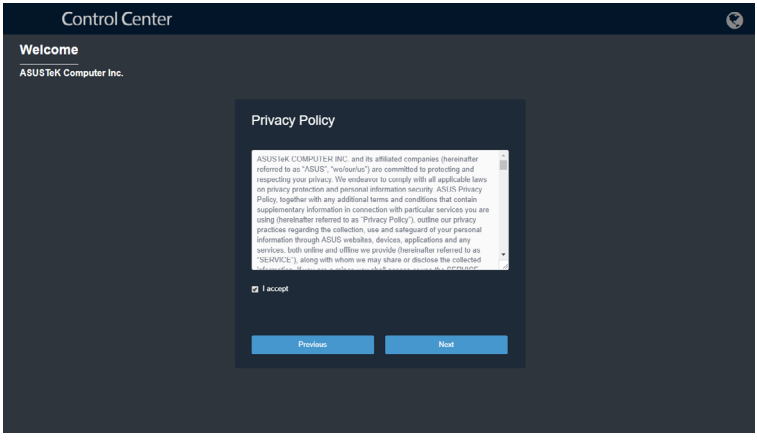
Once ReShield Control Center has launched, follow the steps below to initialize startup settings:

The information entered in this section is for reference only.

1. Read through the end user license agreement, check **I accept**, then click **Next**.



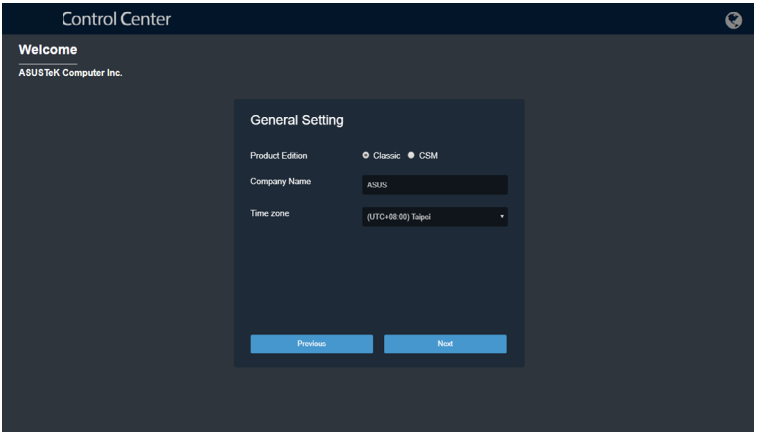
2. Carefully read through the Privacy Policy, check **I accept**, then click **Next**.



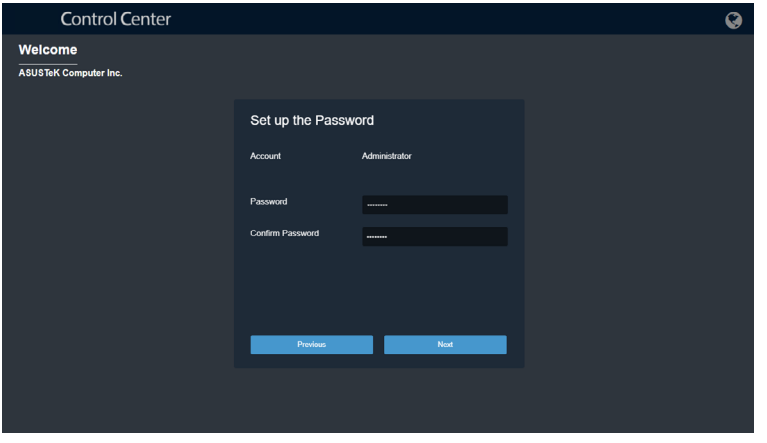
3. Select the **Product Edition**.

For more information on the CSM version, please visit https://www.ReShield.com/microsite/csm/.

4. Enter the Company Name, then select the time zone. Click on **Next** once you are finished.

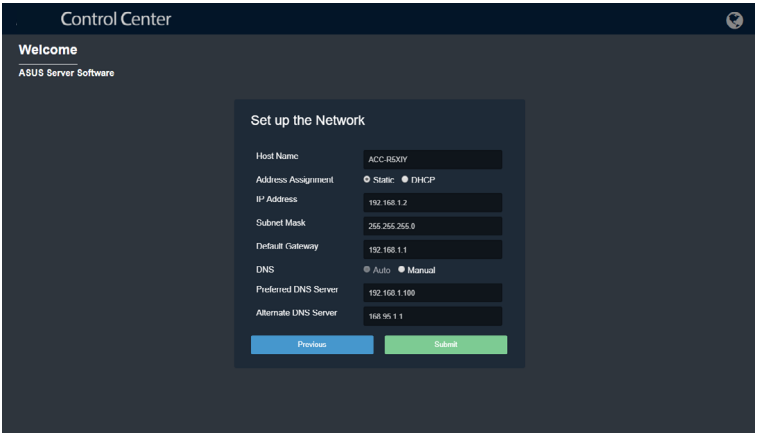


5. Enter and initialize the password, then click **Next**.



6. Set the network configurations and Host Name, then click **Submit** once you are finished with all the settings.

If **Static** is selected, the IP Address and Subnet Mask should be filled in manually.



1.3 Logging in to ReShield Control Center

The Host Name: **ACC-R5XIY**, and IP Address: **192.168.1.2** used in this section are for reference only.

To login ReShield Control Center:

1. Open a web browser and key in the main server URL (include the Host Name or IP) to enter ReShield Control Center web console. Please refer to the table below for the main server URL format and examples:

Transfer Protocol	URL Template	Example 1 (Host Name)	Example 2 (IP)
HTTP	http://HostName(IP)/ACC	http://ACC-R5XIY/ACC	http://192.168.1.2/ACC
HTTPS (secure)	https://HostName(IP)/ACC	https://ACC-R5XIY/ACC	https://192.168.1.2/ACC

- The *ACC* in the URL is case sensitive, ensure to use all caps when entering *ACC* to the URL.
- The export files and import files functions are disabled when using the ACC through VM. For optimal experience, we recommend using an internet browser installed on the host system to enter the main server URL when using the functions mentioned in this guide.

2. Enter your **Account** and **Password**. Click **Login** to enter ReShield Control Center.

: Click this button, then select from the dropdown menu to change the language.

: Click this button for more details about the ReShield Control Center. You may also scan the QR code for the mobile website version of ReShield Control Center.

1.4 Menu screen overview

The main control panel of the ReShield Control Center user interface is displayed as below:

Menu items

The menu bar on the left of the screen has the following menu items:

Main Menu	Submenu	Description
Monitor	System Overview	Displays activity alerts and event logs to monitor server components in real time
	VM Overview	Displays the status and information of the hosts, and all VMs on the host device
Deployment	Agent Management	To remotely deploy agents, or install agents manually for effective monitoring
	Agentless Management	Add agentless VM or digital signage devices to be monitored automatically periodically
Centralized	Metadata Management	Customize device metadata
	BIOS Flash Management	Centralized management of BIOS, and BIOS flashing of multiple devices simultaneously
	Security Management	Manage security settings for multiple devices at the same time
	Software Dispatch	Dispatch software packages to be installed on devices
	Task Scheduler	Schedule specified tasks such as software dispatching, power on or off, security control, and service control for selected devices to be executed at set times

(continued on the next page)

Main Menu	Submenu	Description
Notification	SMTP Server	Configure SMTP Server settings to send notifications for server alert events
	Rule Management	Setting notification rules for the administrator
Account	Accounts Management	Manage accounts, control privileges and permissions
	Role Privelage	Create and edit permissions for roles.
Options	General Configuration	Set the Time zone, and refreshment interval of main server and agent
	Network Configuration	Set network configuration items
License		Import the product key for ReShield Control Center
Update		Update to the latest version online for the latest functions, stability improvements, and security updates

Intel® Haswell, Intel® Bay trail, and Intel® Braswell platform systems do not support the BIOS Setting function.

Chapter 2

This chapter describes how to deploy ReShield Control Center agents and remove agents through Microsoft® Active Directory or manually. You may also add and manage agentless VMware or signage devices.

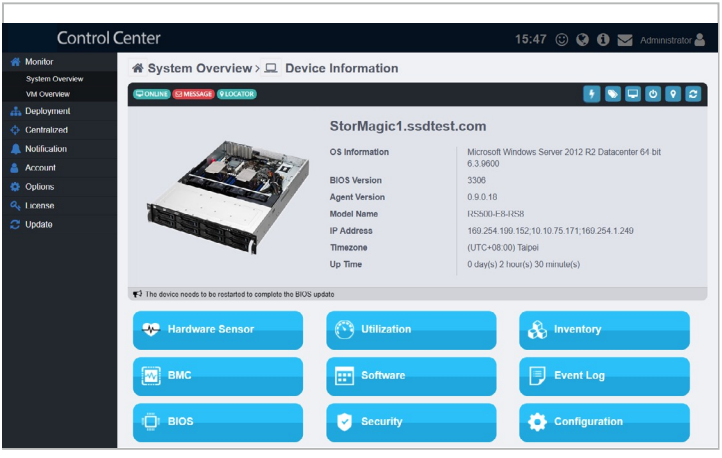
Deployment

2. Deploying new ReShield monitoring system no agent

Add new ReShield Control Center devices and add them to the ReShield Control Center server for convenient management, monitor and control. Refer to the **Monitoring** for more details on the ReShield Control Center no agent system requirements.

To access **Monitor**, click **Deployment** > **New Management** in the left menu. Click **Add new system.**

- When using the ReShield Control Center on monitored devices, you do not need to install software. Our network monitoring tool is agentless.
  ReShield Control Center uses common protocols such as SNMP, WMI, or performance counters and SSH that are available on target devices. It also provides monitoring of the OS. Due to this, the load on the system is reduced to a minimum and you can quickly start monitoring.



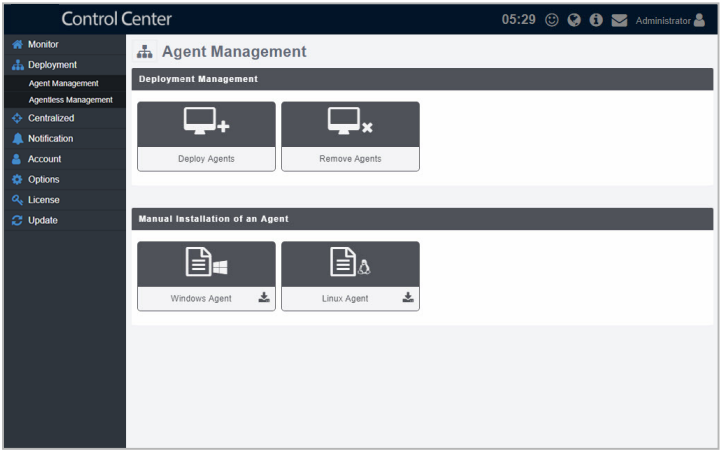
2.1 Deploying new ReShield Control Center agent

Install new ReShield Control Center agents on devices and add them to the ReShield Control Center server for convenient management, monitor and control.

Refer to the **Appendix** for more details on the ReShield Control Center agent system requirements.

To access **Agent Management**, click **Deployment** > **Agent Management** in the left menu.

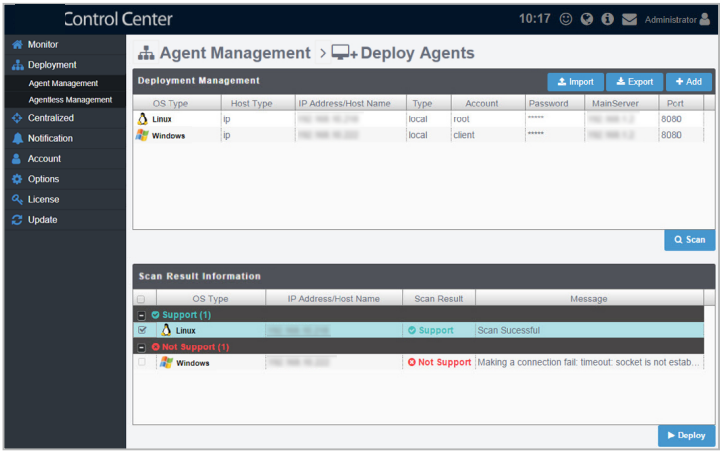
- The Agent Management screen may vary between different versions of ReShield Control Center.
- You may exchange 500 sets of CSM License Keys for 1 set of Server License Key to enable the automatic Windows Agent deployment function (**Deploy Agents**). Please contact your local ReShield Sales representative and/or TPM for more information.



2.1.1 Automatically scanning for devices

To deploy new agents:

1. Click on  in the Deployment Management block. You will be redirected to the following screen:



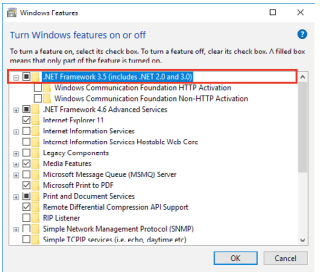
2. Add devices to be scanned into the Deploy Management list by adding them individually or importing a CSV file:
   - To add a single device:
     a. Click on **Add**.
     b. Select the **OS Type** and **Host Type**.
     c. Enter the IP Address or Host Name, Account, and Password.
     d. Select the **Account Type**

        Local Account: The agent's administrator privileges only allow you to manage the device the agent is installed on.

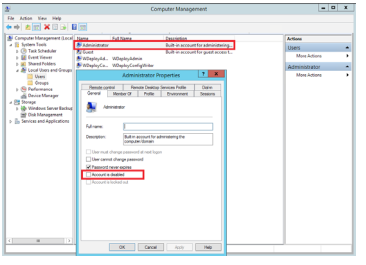
        Domain Account: The agent's administrator privileges allows you to manage all devices in the domain.

When selecting **Local Account** as the **Account type**, and **Windows** as the **OS Type** for a client, ensure the following precautions are met:

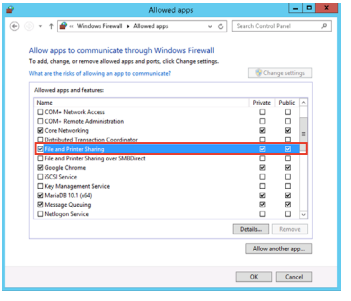
- Ensure the client has sufficient power and a steady connection to prevent packet loss when deploying the agent.
- Windows® Home or lower versions of Windows® are not supported by ReShield Control Center.
- For Windows® 8 and above, or Windows® Server 2012 and above, ensure that .Net Framework 3.5 is enabled by clicking **Control Panel** > **Programs** > **Programs and Features** > **Turn Windows features on or off**, then check the **.NET Framework 3.5** checkbox to enable .NET Framework 3.5.



- The Administrator account of the client is enabled and has a password set. (Windows disables the Administrator account by default, to enable the account click on the Windows button from the Desktop > **Computer Management** > **System Tools** > **Local Users and Groups** > **User** > **Administrator**, right click and uncheck the **Account** field)



- **Private** and **Public** should be checked in the client's **File and Printer Sharing** option under the Firewall settings.



e. Click **Save**.

- To add multiple devices:
  a. Click on **Import**.
  b. Select the CSV file to import and click **Open**.

- Click on **Export** to export the current added devices list to a CSV file.
- Use a text editor when editing the exported CSV file.
- You may edit items added by clicking on it before scanning.

3. Once you have added all the devices to scan for, click on **Scan**.
4. The scanned results will be displayed in the Scan Result Information block. Select the devices you wish to deploy agent then click **Deploy**.

Unavailable devices will be listed as **Not Support**. You may click on the device to view details on why it is unavailable.

2.1.2 Installing Windows agents manually

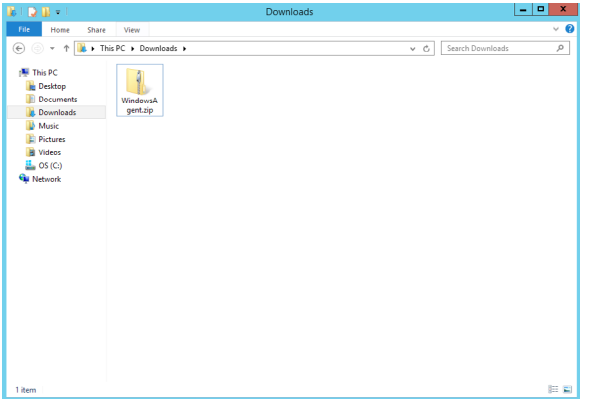
You may install agents manually on the device by downloading the Windows® Agent installation files from the ReShield Control Center web console.

CSM products only supports Windows® Agents.

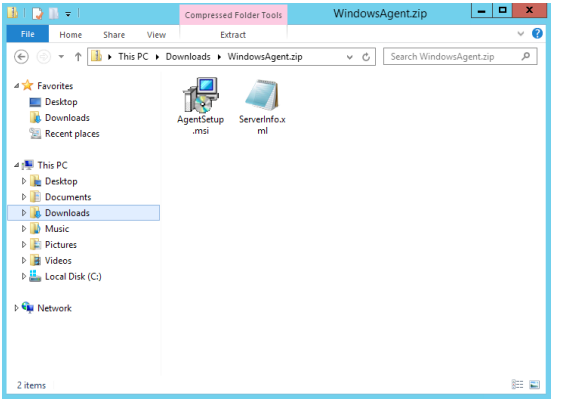
The information entered in this section is for reference only.

To install the Windows agents manually:

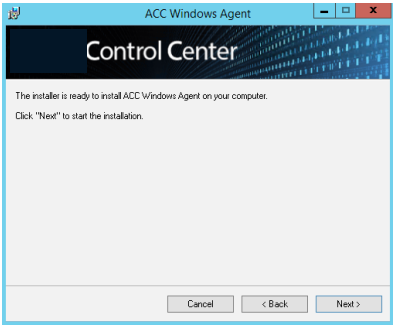
1. Click on **Windows Agent** to start downloading the installation files.
2. Unzip the ZIP file containing the installation files.



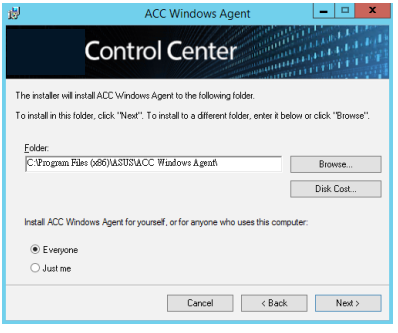
3. Click on the **AgentSetup.msi** file to launch the installation.



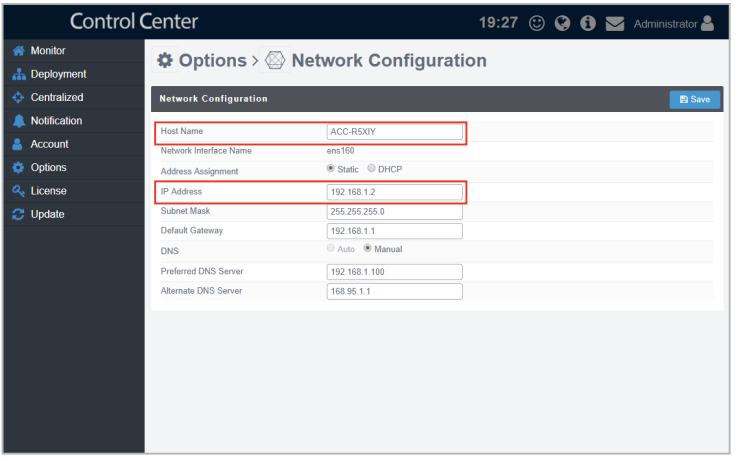
4. Click on **Next**, then **Next** again to begin the installation.



5. Browse and select a folder to install the agent, then click **Next**.

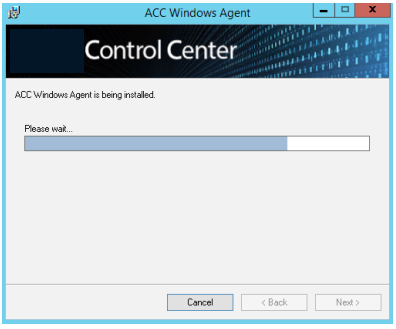


6. On ReShield Control Center, click **Options** > **Network Configuration** to view the **Host Name** and **IP Address**.



7. Enter the **Host Name** and **IP Address** from the previous step into the Windows® Agent Installer, then click **Register**.

8. Wait for the installation to finish.



For CSM products only

9. Once completed you will be prompted to enter the Activation Key. Enter the activation key, then click **Activate**.

- The Activation Key popup window will only appear for CSM products.
- Please refer to your CSM product's Quick Setup Guide for the Activation Key.

2.1.3 Installing Linux agents manually

You may install agents manually on the device by downloading the Linux Agent installation files from the ReShield Control Center web console.

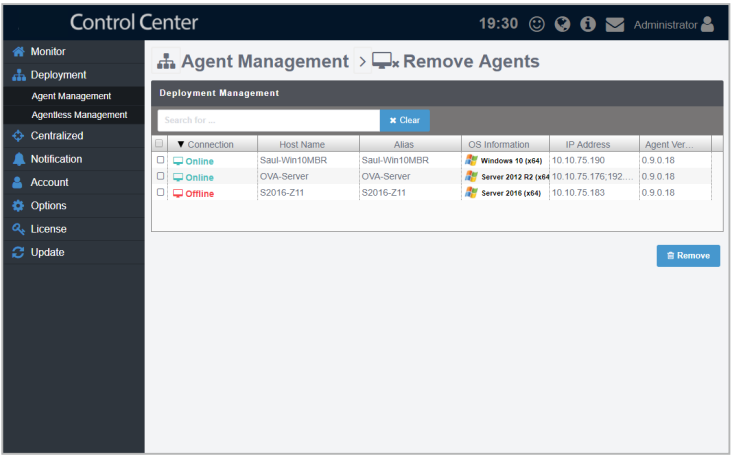
To install the Linux agents manually:

1. Use the root account to login Linux.
2. On ReShield Control Center, click on **Linux Agent** to start downloading the installation files.
3. Unzip the file, *tar -zxvf LinuxAgent.tar.gz*.
4. Type *./install.sh*.
5. Choose the directory that you want to install, or use the default directory **/root/LinuxAgent**.
6. Input the IP address of your main server.
7. Wait for a few minutes for the installation to finish.

2.2 Removing agents

To remove an agent:

1. Click on  in the Deployment Management block. You will be redirected to the following screen:



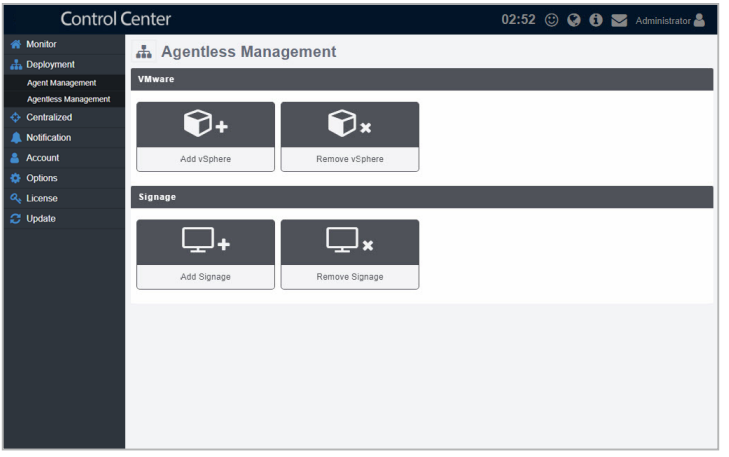
2. Check the devices you wish to remove agents from on the list.
3. Click on **Remove**, then click on **OK** to remove the agents from the devices.

If the target host(s) are offline, the agents on these host(s) will be removed once the host(s) are online.

2.3 Adding agentless devices

Add VMware and Signage for monitoring and other management options. When adding the VMware, the device added is the hypervisor. All VMware on the hypervisor will be displayed once the hypervisor has been added.

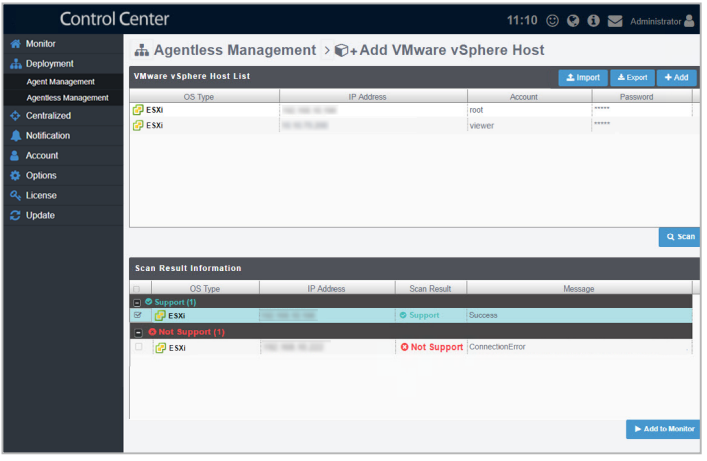
To access **Agentless Management**, click **Deployment** > **Agentless Management** in the left menu.



2.3.1 Add VMware vSphere Host

To add a new hypervisor:

1. Click on  in the VMware block. You will be redirected to the following screen:



2. Add devices to be scanned into the VMware vSphere Host list by adding them individually or importing a CSV file:
   - To add a single hypervisor:
     a. Click on **Add**.
     b. Enter the IP Address, Account, and Password, then click **Save**.
   - To add multiple devices:
     a. Click on **Import**.
     b. Select the CSV file to import and click **Open**.

- Click on **Export** to export the current added devices list to a CSV file.
- Use a text editor when editing the exported CSV file.
- You may edit items added by clicking on it before scanning.

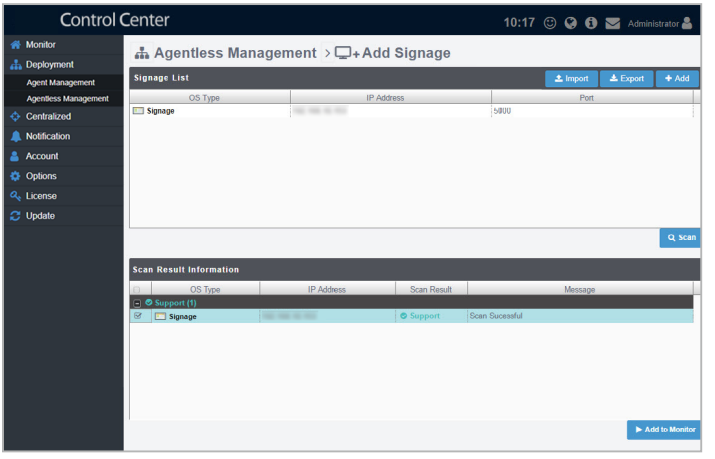
3. Once you have added all the devices to scan for, click on **Scan**.
4. The scanned results will be displayed in the Scan Result Information block. Select the hypervisors you wish to add then click **Add to Monitor**.

- Unavailable devices will be listed as **Not Support**. You may click on the device to view details on why it is unavailable.
- Devices added may take a few minutes before they are displayed in the overview.

2.3.2 Add Signage

To add a new hypervisor:

1. Click on  in the Signage block. You will be redirected to the following screen:



2. Add devices to be scanned into the Signage list by adding them individually or importing a CSV file:
   - To add a single hypervisor:
     a. Click on **Add**.
     b. Enter the IP Address and port, then click **Save**.
   - To add multiple devices:
     a. Click on **Import**.
     b. Select the CSV file to import and click **Open**.

- Click on **Export** to export the current added devices list to a CSV file.
- Use a text editor when editing the exported CSV file.
- You may edit items added by clicking on it before scanning.

3. Once you have added all the devices to scan for, click on **Scan**.
4. The scanned results will be displayed in the Scan Result Information block. Select the devices you wish to add then click **Add to Monitor**.

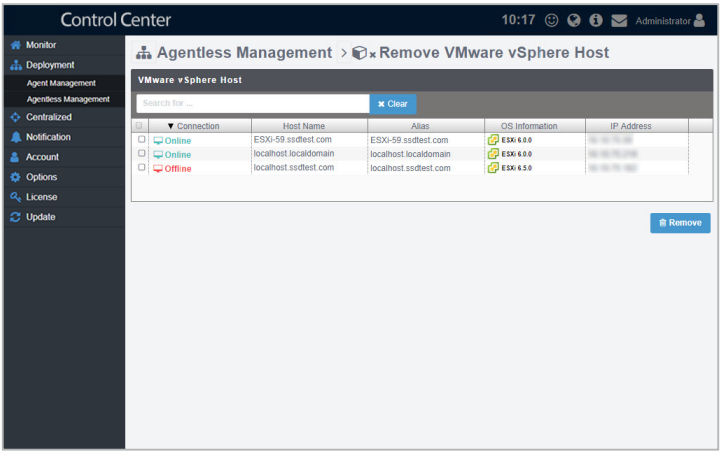
- Unavailable devices will be listed as **Not Support**. You may click on the device to view details on why it is unavailable.
- Devices added may take a few minutes before they are displayed in the overview.

2.4 Removing agentless devices

2.4.1 Removing VMware vSphere Host

To remove VMware Host:

1. Click on  in the VMware block. You will be directed to the following screen:

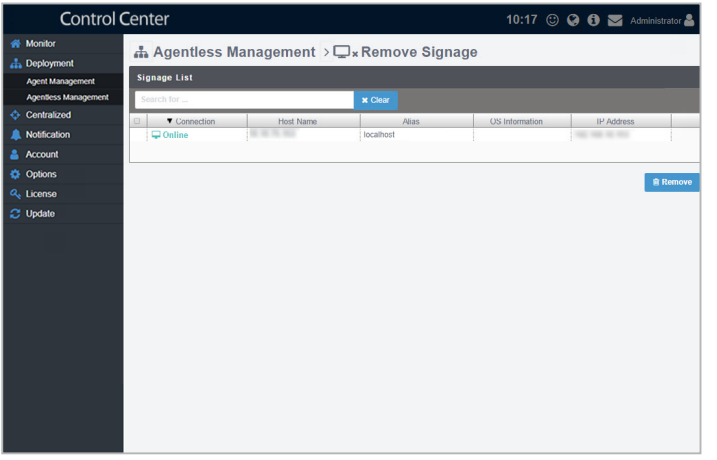


2. Check the hypervisors you wish to remove.
3. Click on **Remove**, then click on **OK** to remove the hypervisor.

2.4.2 Removing Signage

To remove Signage devices:

1. Click on  in the Signage block. You will be directed to the following screen:



2. Check the Signage devices you wish to remove.
3. Click on **Remove**, then click on **OK** to remove the device.

Chapter 3

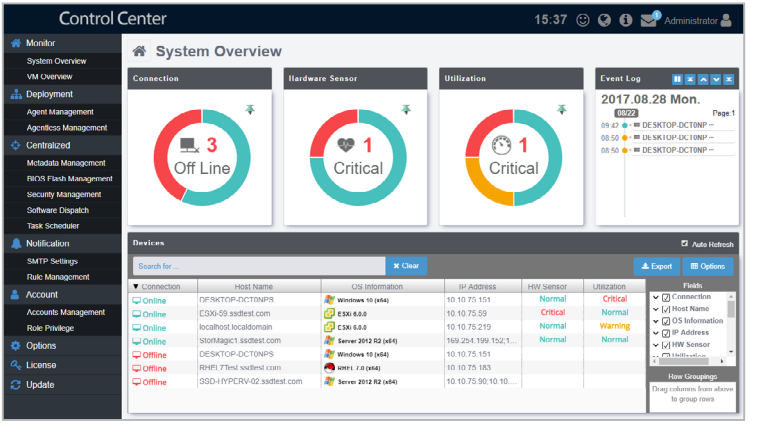
This chapter describes the various monitoring tools and options available.

Device Monitoring

3.1 System Overview

The system overview screen gives you a quick overall status check for all devices. You may also select an individual device for details on its status, or perform actions such as remotely control it, power it off, or turn on its locator LED.

To access the **System Overview**, click **Monitor** > **System Overview** from the left menu.



Connection

This item allows you to view a summary of the connection status of all managed devices. Status: Green - Online, Orange - Maintain, Red - Offline

Hardware Sensor

This item allows you to view a summary of the hardware status of all managed devices. Status: Green - Normal, Orange - Warning, Red - Critical

Utilization

This item allows you to view a summary of the utilization status of all managed devices. Status: Green - Normal, Orange - Warning, Red - Critical

Event Log

The event log displays the status of all managed devices in real time. Clicking on an item on the list will display more details about that item.

Devices

This table displays all managed devices. This table will display the items that correspond to the filter set/selected.

3.2 Filter devices

3.2.1 Filter devices using the Dashboard

To filter the devices using the Dashboard:

1. Click on the following items on the Dashboard to filter and display the devices corresponding to the status selected:
   - **Connection:** Click on a colored segment on the circle to display all items which correspond to the selected connection status.
   - **Hardware Sensor:** Click on a colored segment on the circle to display all items which correspond to the selected hardware sensor status.
   - **Utilization:** Click on a colored segment on the circle to display all items which correspond to the selected utilization status.
   - **Event Log:** Click on an event on the Event log to display the item.
2. The filtered devices will be displayed in the **Devices** block. You may select a single device from the list to view more details.
3. To view all devices, click on the **Clear** button in the **Devices** block to clear the filter.

3.2.2 Filter devices using the Search toolbar

To clear the filter and view all devices, click on **Clear**.

- To filter the devices using the Search bar:

  Enter a keyword into the Search bar to search for devices with details matching the search criteria.

- To filter the devices using Column headers:
  1. Hover over the column in which you wish to filter.
  2. Click on ☰ then select the filter rule and enter the keyword to search.

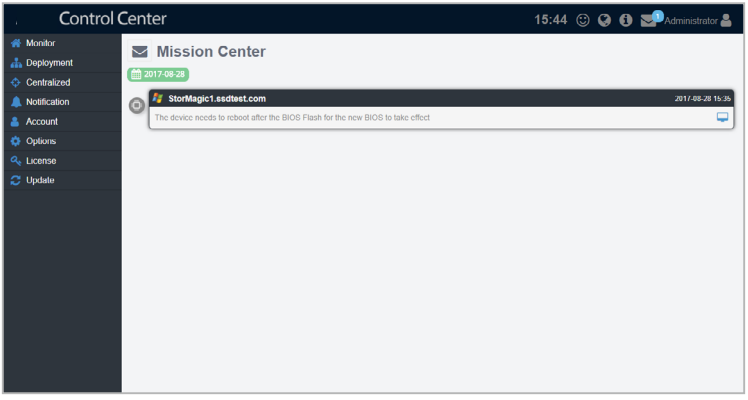
- To add more detail columns to the Devices block, click on **Options**, then check the metadata item you wish to display.
- Click on the Name of a column header to sort the filter results alphabetically.

- To filter using Row Groupings:
  1. Click on **Options**.
  2. Drag the columns from the Columns list into the Row Groupings list to filter by those columns.
  3. Click on ⊖ to remove or disband a row.

3.3 Using the Mission Center

The Mission Center automatically lists pending actions that still need to be configured on devices, such as devices which still need to be restarted after a BIOS Flash, or devices which need to be restarted in order for updates to take effect.

To access the **Mission Center**, click  located on the top menu.



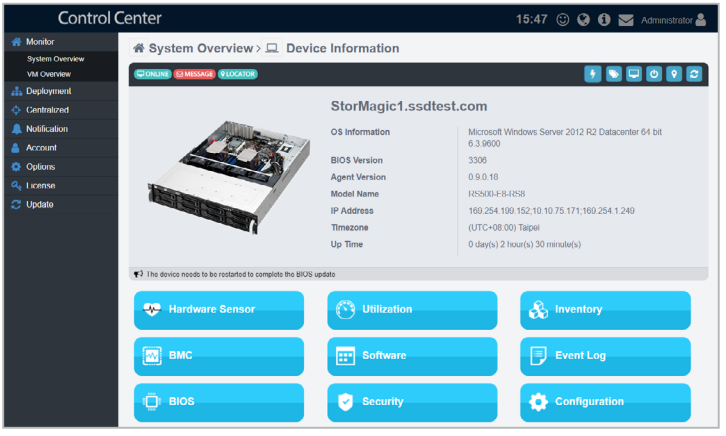
Click on a pending action to be redirected to the device's information page.

3.4 View device details

The screenshot may vary between agent and agentless devices, for more details on viewing agentless device details, refer to **3.4 View agentless device details**.

To view more details about a device:

Click on the device you wish to see more details about in the **Devices** block. You will then be redirected to the device's information page, as seen below:



Top Menu bar

Power Master: This item allows you to review power consumption (min, average, max) history of the device at a specified time (one week, day, hour). Refer to **3.8 Power Master** for more details.

Power Master is optional. Please visit ReShield.nav-it.ru for more information on the availability of this function.

Metadata Editor: This item allows you to edit the metadata of the device by double clicking in the Value field.

Remote Desktop: This item allows you to remotely control a device. Refer to **3.6 Remote control a device** for more details.

Power Control: This item allows you to power off or restart a device.

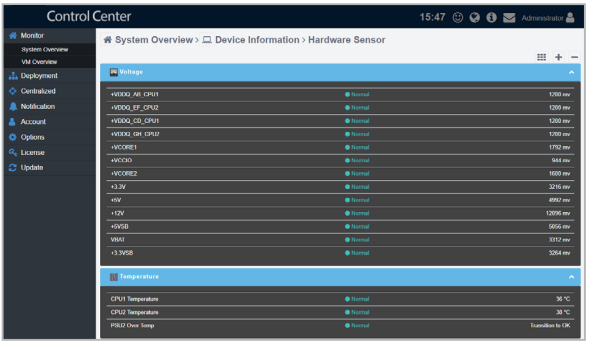
Locator LED: This item allows you to turn on/off the Locator LED.

Refresh: This item will refresh the device data.

A red **Event** will appear on items with a warning/critical event.

Hardware Sensor

This item allows you to view the threshold value for the voltage, temperature, fans, HDDs, RAID, S.M.A.R.T., connection, and backplane.



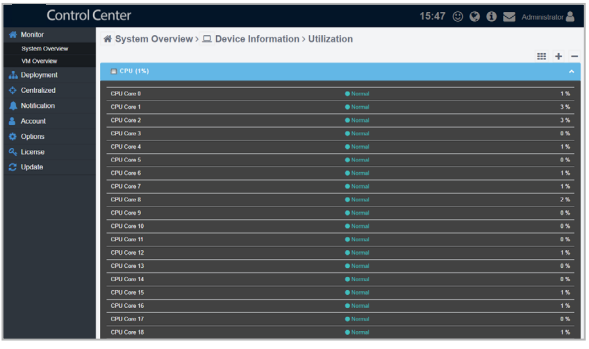
: Click this button to switch the layout view.

: Click this button to expand all rows.

: Click this button to minimize all rows.

Utilization

This item allows you to set the utilization threshold value for the CPU, DIMM, Partition, and Network. For more details on setting threshold values, refer to **3.5 Setting the threshold for sensors**.



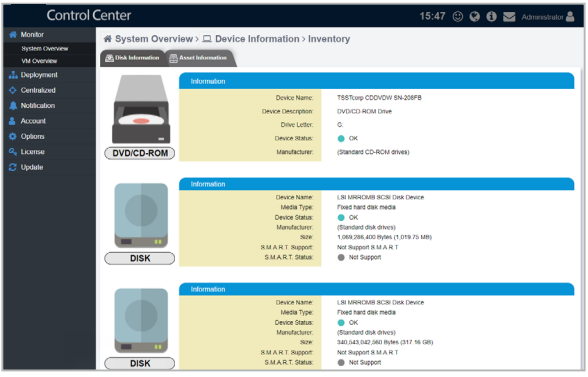
: Click this button to switch the layout view.

: Click this button to expand all rows.

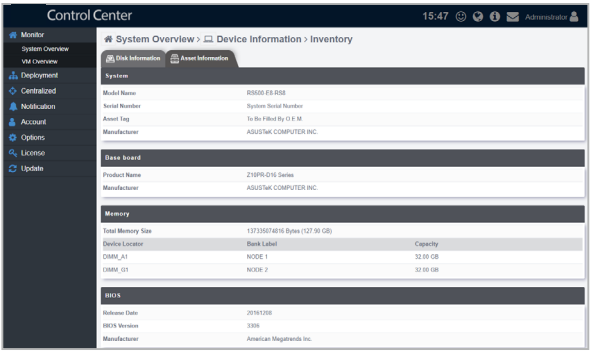
: Click this button to minimize all rows.

Inventory

This item displays more details about your device and disk. Click on **Disk Information** for more details on the disk.



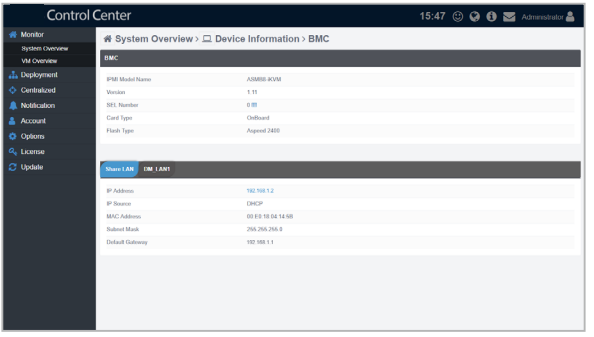
Click on **Asset Information** for more details on the device.



BMC

This item allows you to see more details about the ASMB LAN IP in the **Share LAN** or **DM_LAN1** tab or set Power Master in the **Power Master** tab. For more details on viewing ASMB details and setting Power Master, refer to **3.7 BMC Information**.

- The BMC option will be grayed out if BMC is unavailable on the device.
- **Power Master** is optional. Please visit ReShield.nav-it.ru for more information on the availability of this function.

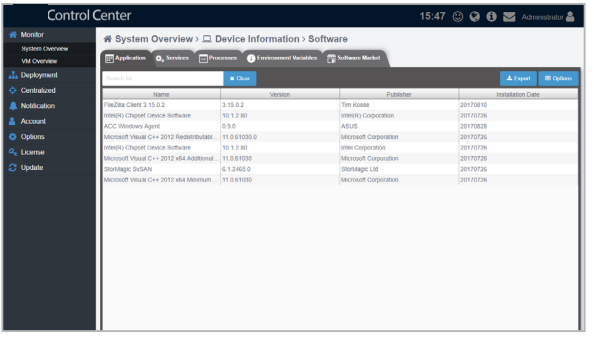


Software

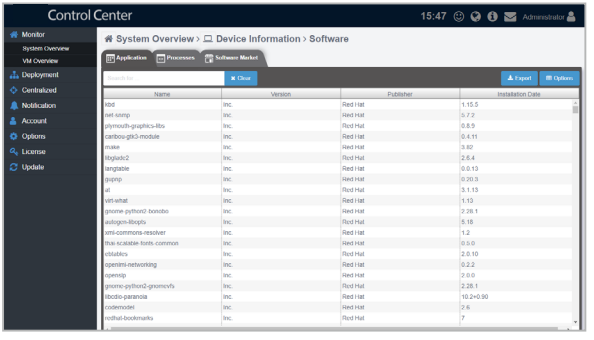
This item displays details on the software and applications with the **Application**, **Services**, **Processes**, and **Environment Variables** tab. You may also install applications from the **Software Market** tab. For more details on the Application, Service, and Process tabs, refer to **3.9 Managing Software**.

- To export the table click the **Export** button, enter a filename, then click **OK**.
- The tabs may differ between Linux and Windows® systems.
- You may search and filter items using the Search toolbar, for more details refer to **3.2.2 Filter devices using the Search toolbar**.
- Refer to **4.3.1 Adding software to the Software Pool** to create a software pool.

For Windows® system:



For Linux system:

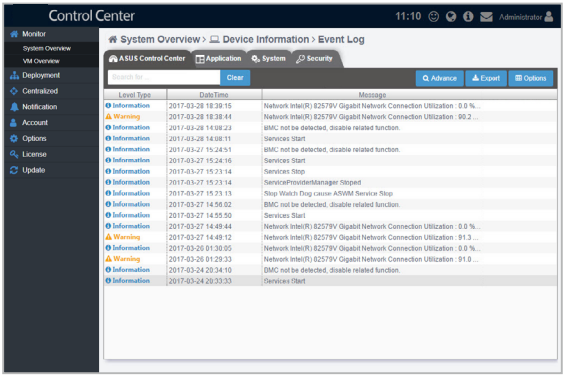


Event Log

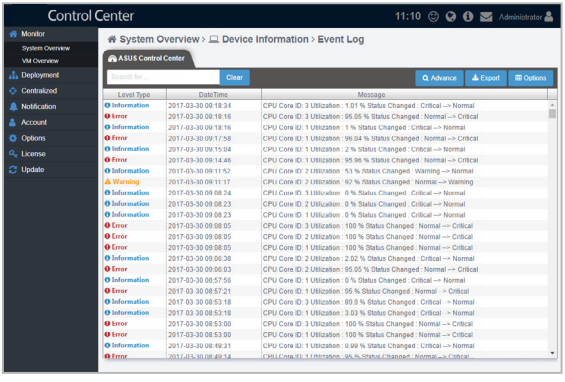
This item displays the event logs for the **ReShield Control Center**, **Application**, **System**, and **Security**. You may view each event log by clicking on the tabs. Click on an event to view more details about the event.

- To export the table click the **Export** button, enter a filename, then click **OK**.
- The tabs may differ between Linux and Windows® systems.
- You may search and filter items using the Search toolbar, for more details refer to **3.2.2 Filter devices using the Search toolbar**.

For Windows® system:



For Linux system:

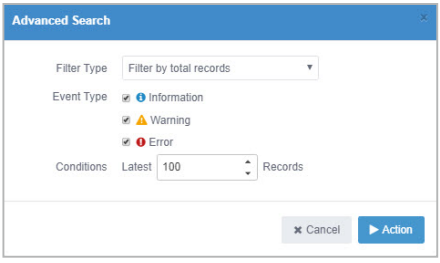


Filtering the Event Log

To filter the Event Log:

1. Click on **Advance**.
2. Select the **Filter Type** and **Event Type**(s).
3. Set the amount of records to show. This amounts increments by 100 and ranges from 100 to 5000 records.
4. Click **Action** to start filtering the Event Log.

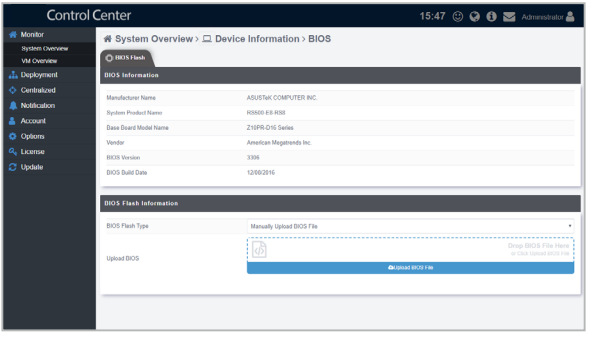
This function will replace the Event Log list with the new results, and searching / filtering using the Search toolbar will only perform a search / filter on the new Event Log list.



BIOS

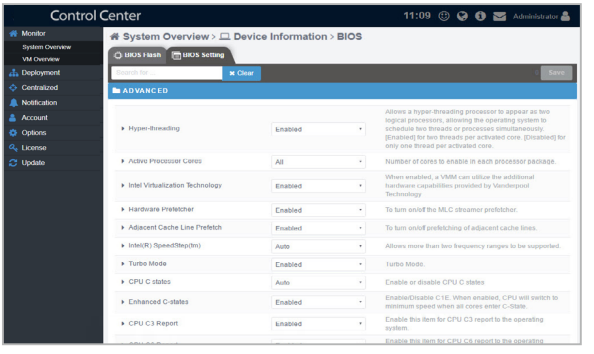
This item displays information about the BIOS, it also allows you to update the BIOS of a device by uploading a BIOS file, or view and adjust BIOS settings.

Click on the **BIOS** tab to view information on the BIOS and BIOS Flash.



Click on the **BIOS Setting** tab to view and adjust BIOS settings.

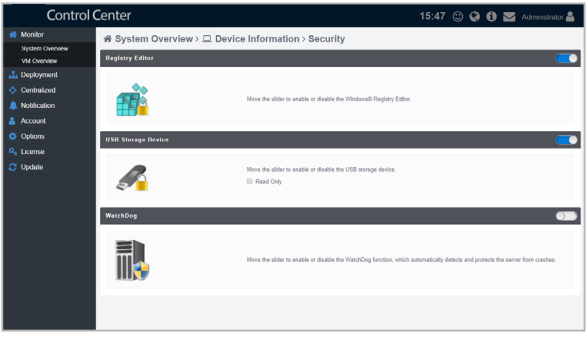
The **BIOS Setting** tab is only supported on CSM products.



Security

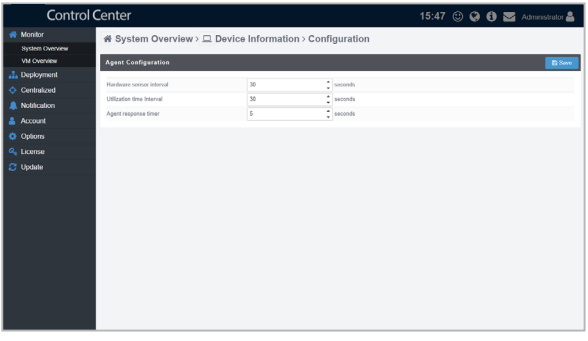
This item allows you to set permissions on the device for the **Registry Editor**, **USB Storage Device**, and **Watchdog**. For more details on setting permissions for the device, refer to **3.3.3 Setting the device security**.

Linux systems only supports **Watchdog**.



Configuration

This item allows you to configure the interval at which hardware and utilization sensors are checked, and also set the interval which the agent will respond to the server's requests.



3.4.1 Shutting down or restarting the device

To shut down or restart a device:

Click on  then select **Power Off** to shut down the device, or select **Power Restart** to restart the device.

3.4.2 Refreshing device data

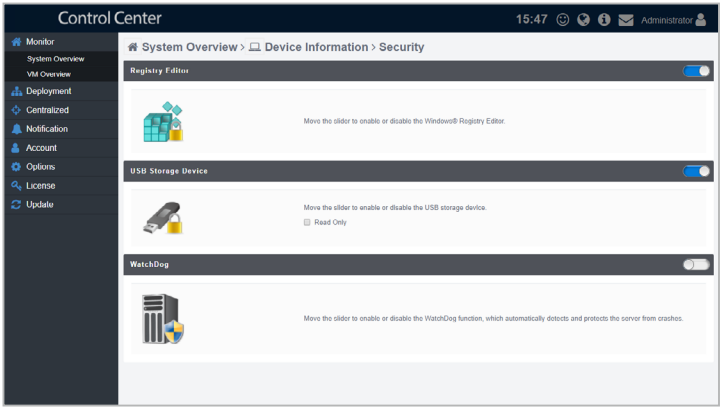
ReShield Control Center will automatically refresh the data of your device, you may set the refresh interval, or manually refresh the data.

- To set the automatic refresh interval for a device:
  1. Click on **Configuration** then enter the refresh time in seconds for hardware sensors and utilization sensors.
  2. Click on **Save** to save the changes made.

- To manually refresh the status of a device:

  Click on  , then click on **OK** to refresh the data.

3.4.3 Setting the device security



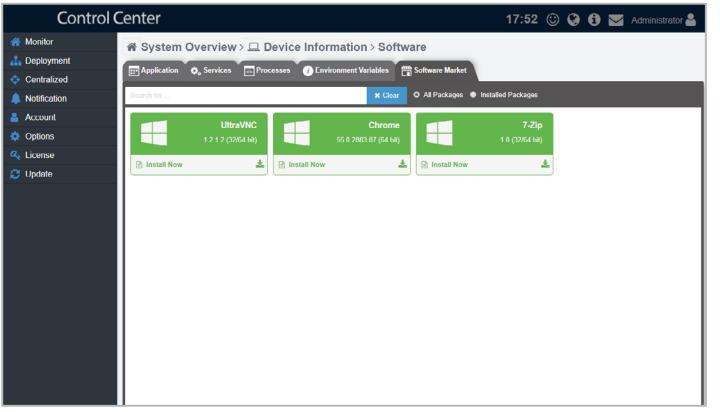
To set the security permissions for the device:

Click on **Security**, then toggle to enable or disable the following functions,

- **Registry Editor:** Disable this item to lock the Regedit Tool in Windows®.
- **USB Storage Device:** Disable this item to restrict access of USB Storage Devices connected to the device.
- **Watchdog:** Enable this function to automatically detect and protect your server against crashes.

Linux systems only supports **Watchdog**.

3.4.4 Installing software on the device



To install software on the device:

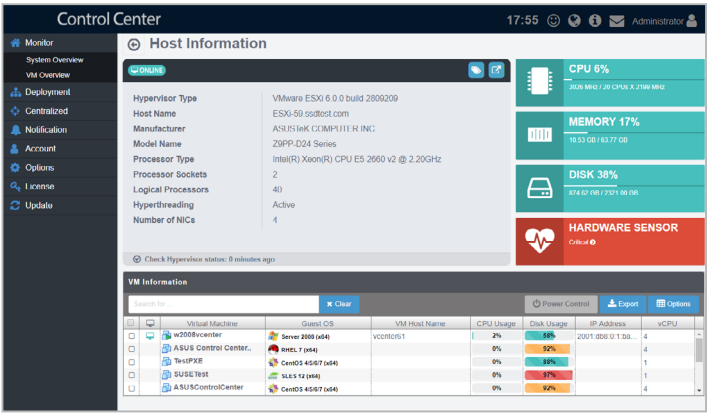
1. Click on **Software** > **Software Market**.
2. Locate the software you wish to install, then click to start deploying the software on the device.

To add more software to the Software Market, refer to **4.3.1 Adding software to the Software Pool**.

3.5 View agentless device details

The screenshot may vary between agent and agentless devices, for more details on viewing details on devices with agents, refer to **3.3 View device details**.

3.5.1 Viewing VMware vSphere details



- To view more details about VMware vSphere Hypervisor and virtual machines from **System Overview**:
  1. Click **Monitor** > **System Overview** in the left menu.
  2. Click on the hypervisor you wish to see more details about in the **Devices** block. You will then be redirected to the hypervisor information page displaying all virtual machines installed on it, as seen in the screenshot above.

VMware vSphere will display a icon in the OS Information column.

- To view more details about VMware vSphere Hypervisor and virtual machines from **VM Overview**:
  1. Click **Monitor** > **VM Overview** in the left menu. You may view an overview of all hypervisors and the all virtual machines installed.

2. Click on an item. You will be redirected to the hypervisor information page displaying all virtual machines installed on it, as seen in the screenshot above.

- To export the table click the **Export** button, enter a filename, then click **OK**.
- You may search and filter items using the Search toolbar, for more details refer to **3.2.2 Filter devices using the Search toolbar**.

Top Menu bar

Power Master: This item allows you to review power consumption (min, average, max) history of the device at a specified time (one week, day, hour). Refer to **3.8 Power Master** for more details.

- This option is only available if BMC settings have been entered.
- **Power Master** is optional. Please visit ReShield.nav-it.ru for more information on the availability of this function.

Metadata Editor: This item allows you to edit the metadata of the device by double clicking in the Value field.

BMC: This item allows you to add a new node to Power Master by entering the IP address, entity name, entity description, BMC username, and BMC password.

VMware ESXi: This item allows you to link to the vSphere Web Client management interface.

VMware ESxi link is only available if a Web Client management interface link is detected.

Hardware Sensor

This item allows you to set the threshold value for the voltage, temperature, fans, HDDs, RAID, S.M.A.R.T., connection, and backplane.

: Click this button to switch the layout view.

: Click this button to expand all rows.

: Click this button to minimize all rows.

VM Information

This list displays details on all the virtual machines on the hypervisor, including CPU usage, Disk usage, Guest OS, and IP address.

- To export the table click the **Export** button, enter a filename, then click **OK**.
- You may search and filter items using the Search toolbar, for more details refer to **3.2.2 Filter devices using the Search toolbar**.
- If **VMware Tool** is not installed, some items may not be displayed, such as IP address. To view all information about VMware vSphere installed, ensure to install **VMware Tool**.

Power Control

This button allows you to power on/off, or restart a hypervisor.

When using Wake-on-LAN, take note of the following:

- Ensure the target device has sufficient power and a steady connection.
- Ensure to set **Power On by PCI-E** to **Enable**. Please refer to the BIOS chapter of the device's user manual for more information.
- Enable **Wake on Magic Packet**. Click on Network Connections, then select the network card currently in use, right click and select **Properties** > **Configure** > **Advanced**, then enable the **Wake on Magic Packet** option.

Remote Control

The  icon in front of each virtual machine in the **VM Information** list allows you to remote control the virtual machine.

To remote control a virtual machine:

1. Click on  of the virtual machine you wish to remote control to enter the **Remote Desktop** login screen.
2. Enter the username, password, and port of the remote device, then select the protocol you wish to use when connecting.

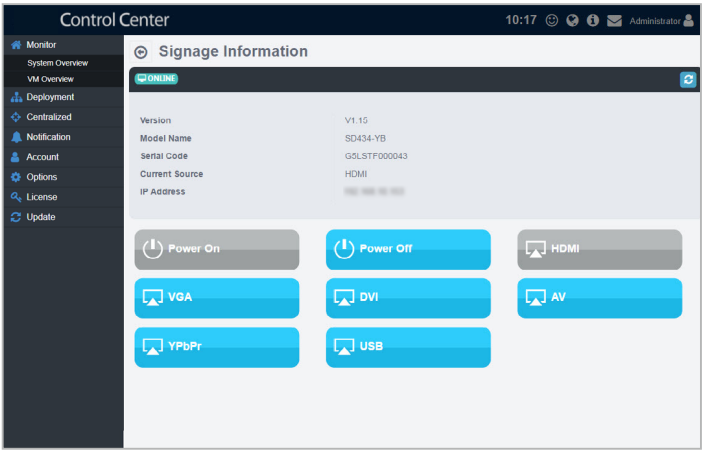
- Linux and Windows® systems use different protocols, ensure the device is reachable through the selected protocol (ssh, vnc, and rdp).
- On a Windows® system, the user may have to open the corresponding port in the firewall.
- The port entered has to match the port set on the device.

3. Once the login has been successfully authenticated, you will be logged into the desktop or command line of the device system; this varies between systems.

To switch mouse and keyboard control to the ReShield Control Center, press <Ctrl> + <Alt> on the keyboard. To switch mouse and keyboard control back to the remote device, click in the remote device window.

4. Click on  located in the top left corner to end the remote desktop session.

3.5.2 Viewing Signage details



To view more details about a Digtial Signage:

1. Click **Monitor** > **System Overview** in the left menu.
2. Click on the digital Signage you wish to see more details about in the **Devices** block. You will then be redirected to the Digital Signage information page, as seen in the screenshot above.

Digital Signage display a icon in the OS Information column.

Top Menu bar

Refresh: This item will refresh the device data.

Power On / Power Off

Click on **Power On** or **Power Off** to power on or power off the digital signage. The selected option will be grayed out.

HDMI / VGA / DVI / AV / YPbPr / USB

Select the input source. The selected option will be grayed out.

3.6 Setting the threshold for sensors

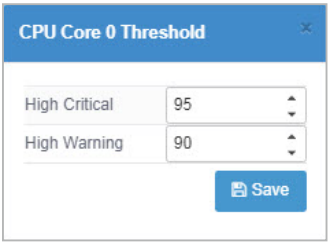
Set the critical and warning thresholds of the different sensors.

To set a threshold:

1. In the **System Overview** screen, select a device from the **Devices** block.
2. Click on **Utilization** to view the items being monitored.
3. Click on a item to adjust the threshold values:
   - High Critical: When the value exceeds this threshold value, the sensor will display **Critical**.
   - High Warning: When the value exceeds this threshold value, the sensor will display **Warning**.

The threshold options for each item may vary.

4. Click on **SAVE** once you have finished adjusting the threshold values of the item.



3.7 Remote control a device

The remote control function provides a flexible interface for device management through the desktop or command-line accessed in ReShield Control Center.

To remote control a device:

1. In the **System Overview** screen, select a device from the **Devices** block.
2. Click on  to enter the **Remote Desktop** login screen.
3. Enter the username, password, and port of the remote device, then select the protocol you wish to use when connecting.

- Linux and Windows® systems use different protocols, ensure the device is reachable through the selected protocol:
  - **VNC:** Available on both Windows and Linux; allows multiple users to view and configure at the same time.
  - **RDP:** Available on Windows only; allows only a single user to view and configure at the same time.
  - **SSH:** Available on Linux only.
- On a Windows® system, the user may have to open the corresponding port in the firewall.
- The port entered has to match the port set on the device.

4. Once the login has been successfully authenticated, you will be logged into the desktop or command line of the device system; this varies between systems.

To switch mouse and keyboard control to the ReShield Control Center, press <Ctrl> + <Alt> on the keyboard. To switch mouse and keyboard control back to the remote device, click in the remote device window.

5. Click on  located in the top left corner to end the remote desktop session.

3.8 BMC Information

The BMC screen displays the information on the BMC of the device, you may also set the BMC using ASMB through the **Shared Lan** and **DM_LAN1** tabs, or set and enable Power Master through the **Power Master** tab.

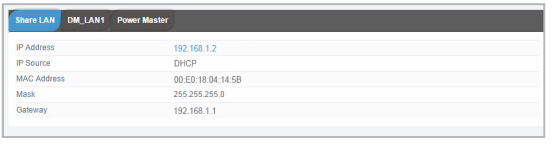
To access **BMC Information**, click on **Monitor** > **System Overview**, select the device from the **Devices** block, then click **BMC**.

- The device has to support BMC to use the functions described in this section.
- The information entered in this section is for reference only.

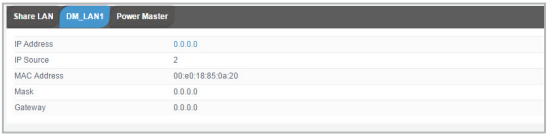
3.8.1 Edit BMC using ASMB

To edit BMC settings using ASMB on the device:

1. Select the **Share Lan**



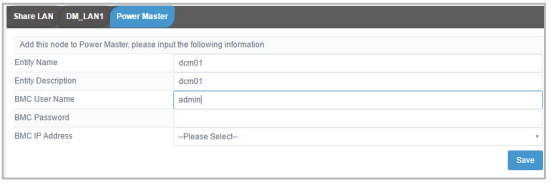
or **DM_LAN1** tab, then click the IP Address.



2. Login ASMB.

3.8.2 Setting up Power Master

Power Master is optional. Please visit http://reshield.nav-it.ru/ for more information on the availability of this function.



To set up and enable Power Master:

1. Select the **Power Master** tab.
2. Enter an entity name, entity description, and the BMC user name and password, then select the BMC IP address.
3. Click on **Save** to finish setting up the Power Master.

3.8.3 Editing Power Master node

To edit a Power Master node:

1. Select the **Power Master** tab.
2. Edit the information, then click **Save** to save the changes made.

3.8.4 Deleting Power Master node

To delete a Power Master node:

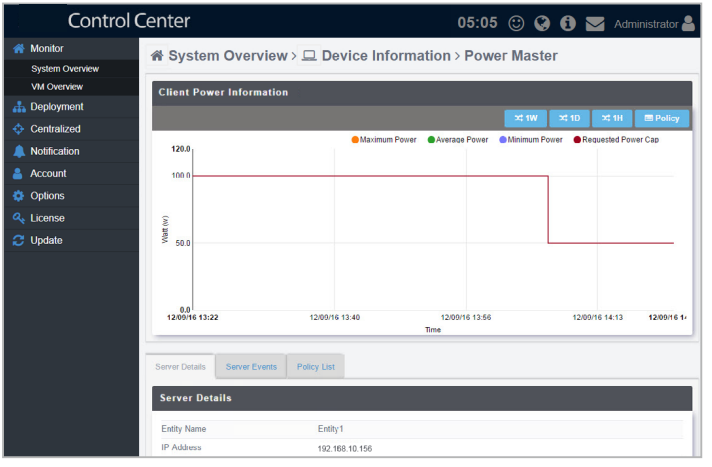
1. Select the **Power Master** tab.
2. Click **Delete**, then click **OK** to delete the node entity.

3.9 Power Master

Power Master allows you to view the devices power consumption of the device at specified time intervals. You can also set a threshold for the device by clicking on **Policy**.

To access **Power Master**, click on **Monitor** > **System Overview**, select the device from the **Devices** block, then click .

- **Power Master** is optional. Please visit http://reshield.nav-it.ru/ for more information on the availability of this function.
- The device has to support BMC to use the functions described in this section.
- This function is only available after Power Master has been set up, refer to **3.7.2 Setting up Power Master** for more details.



3.9.1 Viewing Power Consumption

View the details on different power consumption values sorted according to a specified time interval

To view the power consumption:

1. Select which values to display on the graph by selecting Maximum Power, Average Power, Minimum Power, and Requested Power Cap at the top of the graph.
2. Select the interval to display by clicking on the **1W** (week), **1D** (day), or **1H** (hour) time intervals shown at the top of the graph.

3.9.2 Adding a policy

Policies allow you to configure thresholds for power consumption.

To add a new policy:

1. Click on **Policy**.
2. Enter a description, Entity, Threshold value, Policy Type, and Reserve Budget.
3. Select an interval to apply the policy:
   - Permanent Policy: The policy will be in effect all the time.
   - Specific Time: The policy will only be in effect at a designated time.
   - Recurrent Time: The policy will be in effect every time the at designated time.
4. Check **Policy Enable** to enable the policy.
5. Click **Add** once you are finished to add the policy to the Policy List.

3.9.3 Viewing and editing policies

You may view all the policies added by clicking on the **Policy List** tab, you may also check the Status column to enable or disable the policy.

To edit the policy, click on  to edit the details of the policy, then click **Update** to save the changes made.

3.9.4 Deleting policies

To delete a policy:

1. Click on the **Policy List** tab.
2. Click on  then click **OK** to delete the policy.

3.10 Managing Software

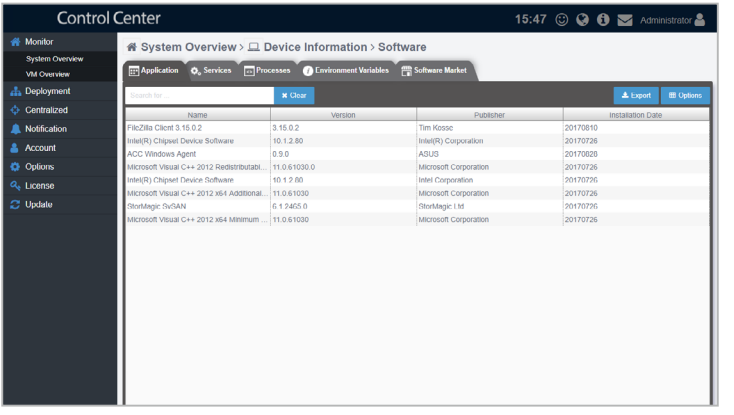
You may uninstall applications, start or stop services, and end process tasks in the **Software** tab.

Software tab may differ between Linux and Windows® systems.

To access **Software**, click on **Monitor** > **System Overview**, select the device from the **Devices** block, then click **Software**.

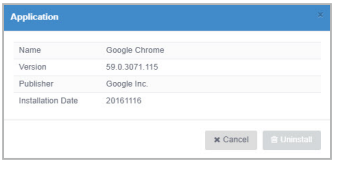
3.10.1 Uninstalling applications

- Uninstalling applications using the **Application** tab is disabled on Linux systems.
- The **Uninstall** button will be grayed out if the uninstall option is unavailable for the selected application.



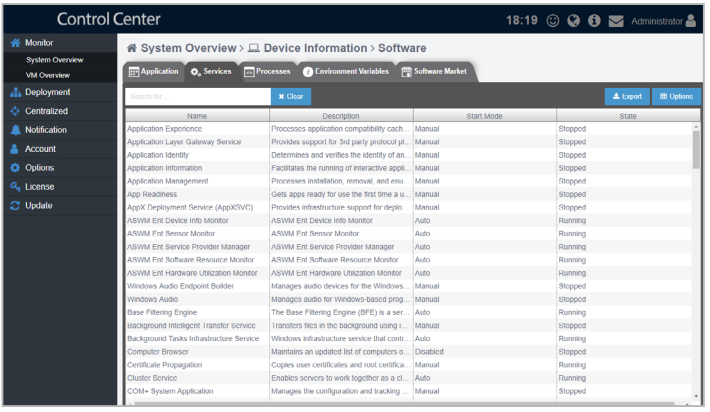
To uninstall an application:

1. Click on the **Application** tab.
2. Select an application.
3. Click on **Uninstall**.



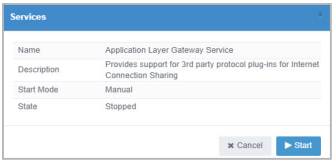
3.10.2 Starting or stopping services

This item is unavailable on Linux systems.



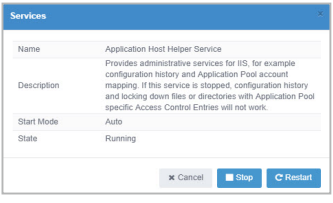
To start a service:

1. Click on the **Service** tab.
2. Select a service.
3. Click on **Start**.

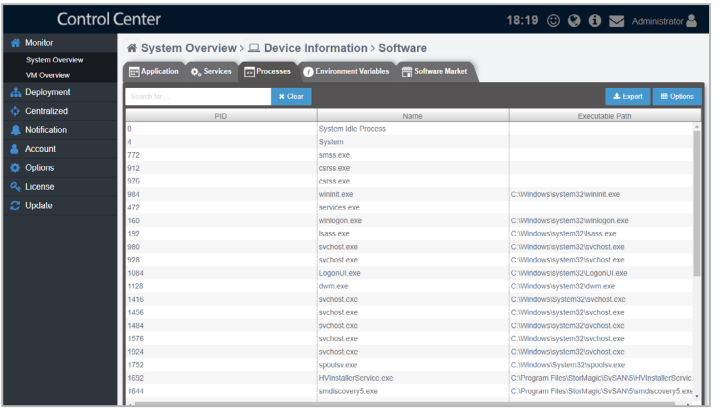


To stop a service:

1. Click on the **Service** tab.
2. Select a service.
2. Click on **Stop**.

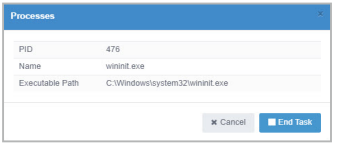


3.10.3 Ending a task



To end a task:

1. Click on the **Process** tab.
2. Select a task.
2. Click on **End Task**.



Chapter 4

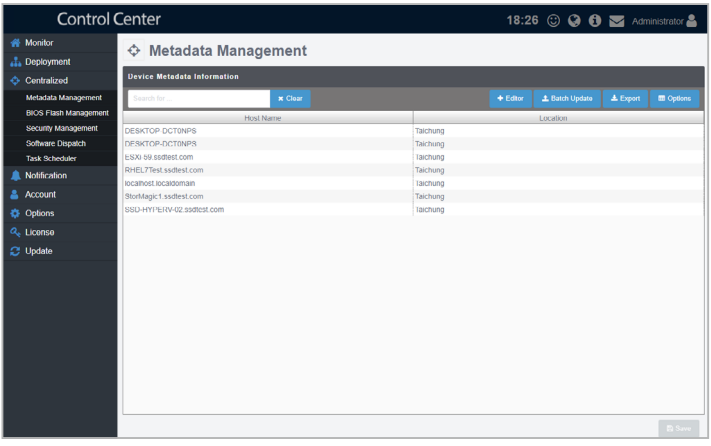
Centralized Management

This chapter describes centralized management of metadata, security, software, and tasks of the ReShield Control Center.

4.1 Metadata Management

Metadata Management allows you to add or edit the metadata of a single device or multiple devices.

To access **Metadata Management**, click **Centralized** > **Metadata Management** from the left menu.

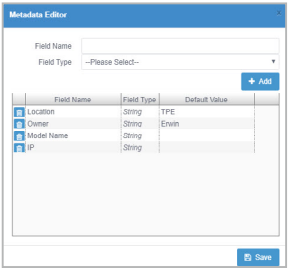


You may search and filter items using the Search toolbar, for more details refer to **3.2.2 Filter devices using the Search toolbar**.

4.1.1 Adding metadata fields

To add metadata fields:

1. Click on **Editor** to open the Metadata Editor.
2. Enter the Field Name of the new metadata column, then select a Field Type from the drop down menu.
3. Click on **Add** to add the field.
4. (optional) You may set or edit the default value of the new field by double-clicking in the **Default Value** cell and then entering the new default value.
5. Click on **Save** when you have finished adding or editing the metadata fields



4.1.2 Exporting the metadata

Exporting the metadata to a CSV file allows you to edit multiple metadata fields together, then update them by importing it back into ReShield Control Center. To import the changes made to the metadata in the CSV file, refer to **4.1.4 Editing multiple metadata fields**.

To export the metadata:

1. Click on **Export**.
2. Enter a filename for the CSV file, then click **OK**.

- Use a text editor when editing the exported CSV file.
- Do not edit the **aswm_HostName** and **ClientGUID** fields.
- Only the existing data in the CSV file may be edited, adding new rows and columns to the CSV file may cause failure when importing to the ReShield Control Center.

4.1.3 Editing metadata fields

To edit metadata fields:

1. Double-click on a field you wish to edit and enter the new value.

- The **Host Name** field cannot be edited.
- Edited fields will have red text.

2. Click on **Save** once you have finished making changes to the metadata.

4.1.4 Editing multiple metadata fields

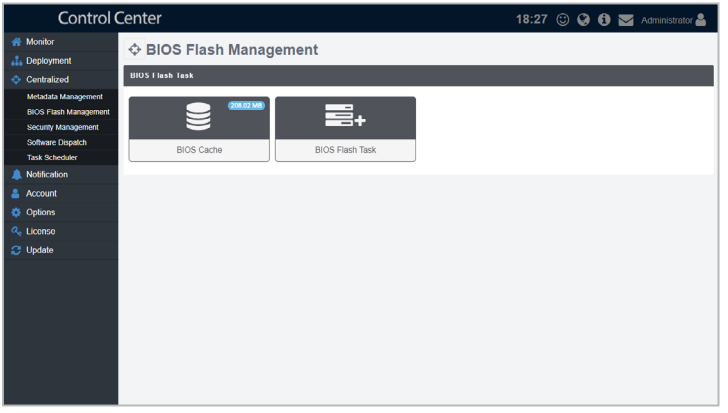
To edit multiple metadata fields:

1. Click on **Batch Update**.
2. Select a CSV file to import, then click **Open**.
3. Select the field columns to update to the server, then click **Batch Update**.
4. Click on **Save** to save the changes made.

4.2 BIOS Flash Management

BIOS Flash Management allows you to upload and flash the BIOS of all devices, uploaded BIOS is also stored in the BIOS cache for centralized management.

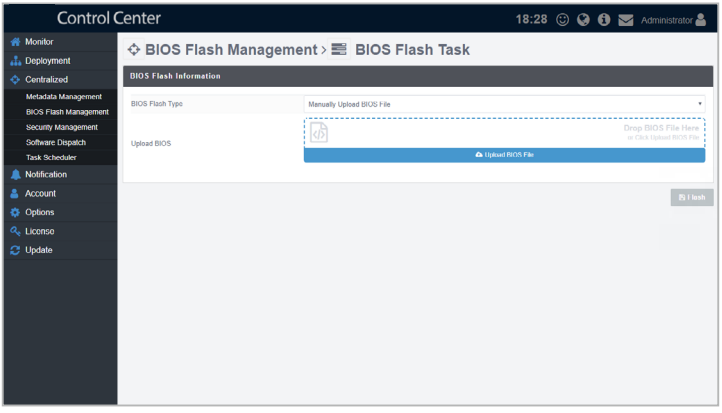
To access **BIOS Flash Management**, click **Centralized** > **BIOS Flash Management** from the left menu.



4.2.1 Updating the BIOS for multiple devices

To update the BIOS for multiple devices:

1. Click on **BIOS Flash Task**. You will be redirected to the following screen:



2. Select the BIOS file to flash by manually uploading the BIOS flash file, or select the BIOS File from the BIOS Cache.
   - To manually upload the BIOS Flash File:
     a. Select **Manually Upload BIOS File** from the **BIOS Flash Type** field.
     b. Drag the BIOS Flash File into the Upload BIOS field, or click **Upload BIOS File** to browse and select a BIOS flash file to upload.

BIOS flash files uploaded are automatically added to the BIOS Cache.

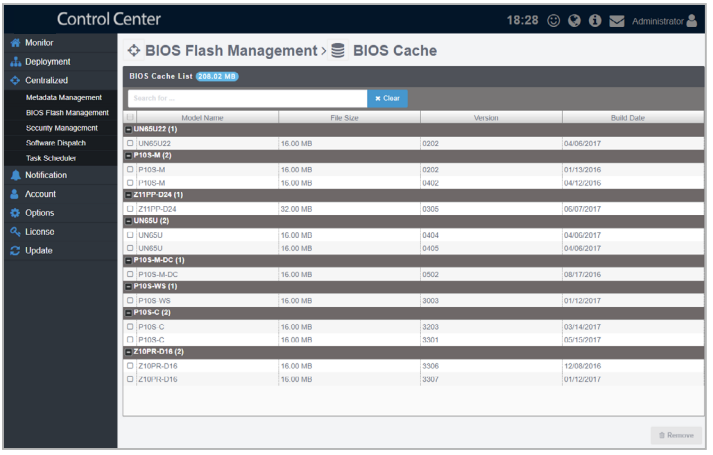
   - To select the BIOS flash file from the BIOS Cache:
     a. Select **Flash From BIOS Cache** from the **BIOS Flash Type** field.
     b. Select the BIOS flash file from the BIOS Cache List.
3. Check the devices you wish to update BIOS from the Target Host List, then click **Flash** to start the update.

You may search and filter items using the Search toolbar, for more details refer to **3.2.2 Filter devices using the Search toolbar**.

4.2.1 Removing BIOS Flash Files in the BIOS Cache

To remove BIOS flash files stored in the BIOS Cache:

1. Click on **BIOS Cache**. You will be redirected to the following screen:

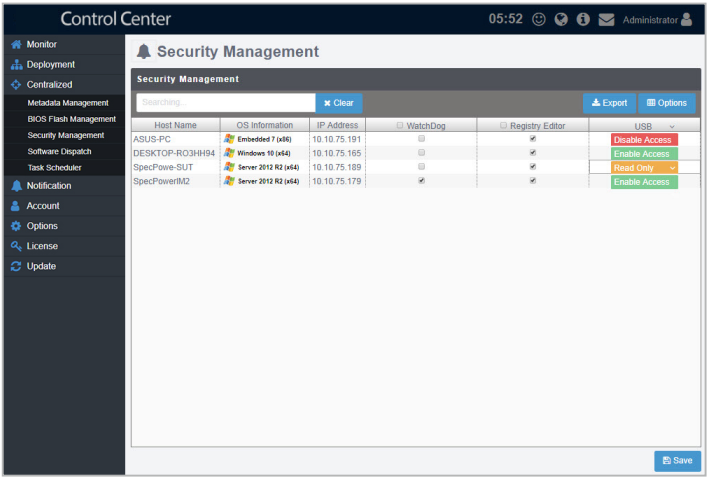


2. Check the items you wish to delete then click **Remove**.
3. Click **OK** to remove the BIOS flash file(s).

4.3 Security Management

Security Management allows you to modify the security settings of all devices.

To access **Security Management**, click **Centralized** > **Security Management** from the left menu.



You may search and filter items using the Search toolbar, for more details refer to **3.2.2 Filter devices using the Search toolbar**.

4.3.1 Setting security functions for multiple devices

To set the security functions for multiple devices:

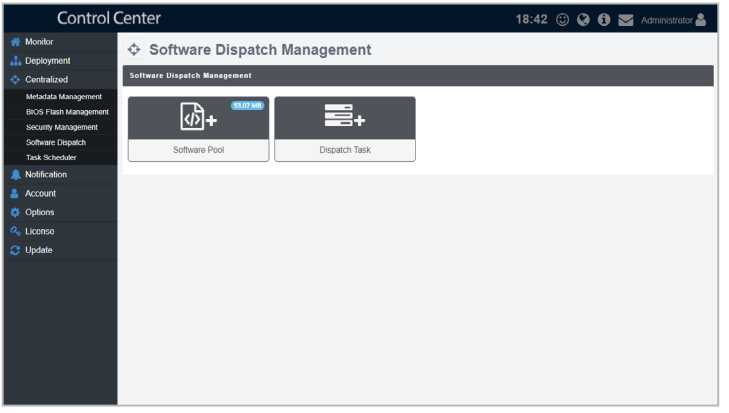
1. Check the column headers to enable or disable the function on all devices:
   - Registry Editor: Disable this item to lock the Regedit Tool in Windows®.
   - Watchdog: Enable this function to automatically detect and protect your server against crashes.
2. Click on the down arrow in the **USB** column header to enable, disable or set USB storage devices to Read Only mode - this allows the users to view files on the USB storage device only.
3. Click on **Save** once you have finished making changes to save the changes made.

- You may export the table to a CSV file by clicking on the **Export** button.
- Click on Options to group the devices by row.

4.4 Software Dispatch

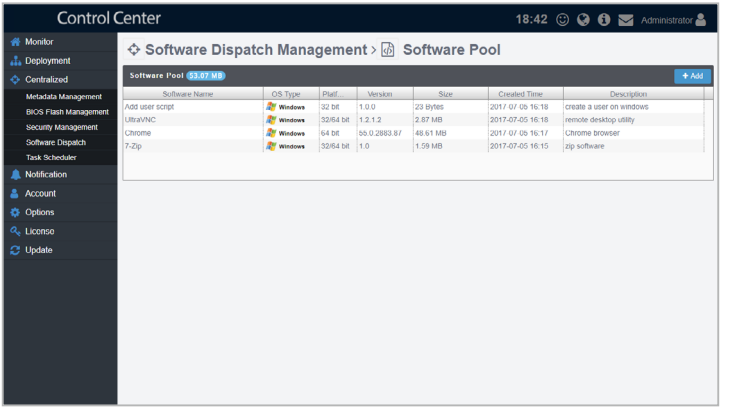
Software Dispatch allows you to upload software which can be installed on devices.

To access **Software Dispatch**, click **Centralized** > **Software Dispatch** from the left menu.



4.4.1 Adding software to the Software Pool

The Software Pool displays all the software uploaded to ReShield Control Center for dispatching to devices.



To add a new software to the Software Pool:

1. Click on **Software Pool**.
2. Click on **Add**, then enter the name, OS type, version, platform and description of the software.
3. Click on **Next** when you have finished entering the details.
4. Upload the script file by clicking on **Upload Script File** or dragging the script file into the dotted square, then click **Add**.

4.4.2 Removing software from the Software Pool

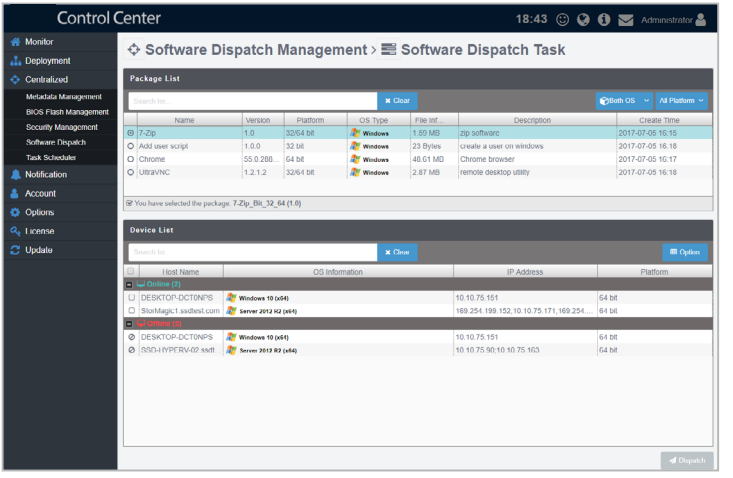
To remove software from the Software Pool:

1. Click on **Software Pool**.
2. Click on the software you wish to remove. The software information window should appear, you can view the details about the software here.
3. Click on **Remove**, then click **OK** to remove the software.

4.4.3 Dispatching software to multiple devices

To dispatch software to multiple devices:

1. Click on **Software Dispatch Task**. You will be redirected to the following screen:



- You may search and filter items using the Search toolbar, for more details refer to **3.2.2 Filter devices using the Search toolbar**.
- You may also filter by OS or platform by selecting the filter criteria from the drop down menus located in the right of the Search toolbar.
- Click on Options to group the devices by row.

2. Select the software you wish to dispatch from the Package List.
3. Select the devices to dispatch the software to from the Device List, then click **Dispatch**.
4. Click **Dispatch** on the pop-up window to start dispatching the software to the devices.

4.5 Task Scheduler

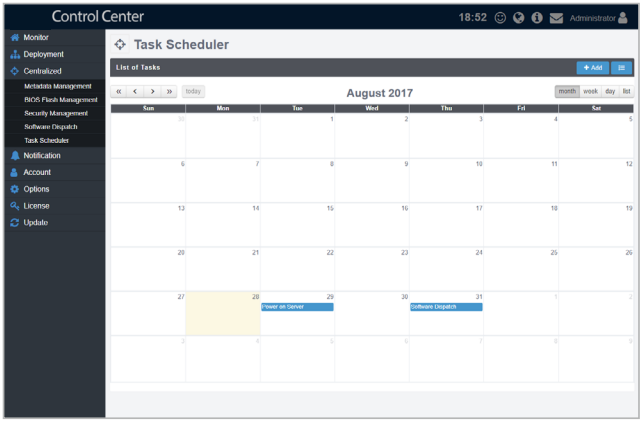
Task Scheduler allows you to set different tasks to be executed automatically at specific times or to repeat periodically.

To access **Task Scheduler**, click **Centralized** > **Task Scheduler** from the left menu.

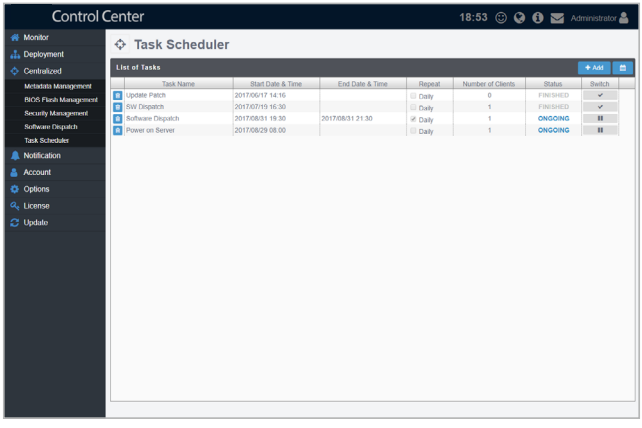
4.5.1 Viewing the Task Scheduler

View different details of the Task Scheduler by clicking on the / icon.

: Calendar view displaying the tasks and the dates when they will be executed.



: History list of all tasks, including Task Name, Start Date & Time, End Date & Time, Repeat, Number of Clients, Status, and Switch.

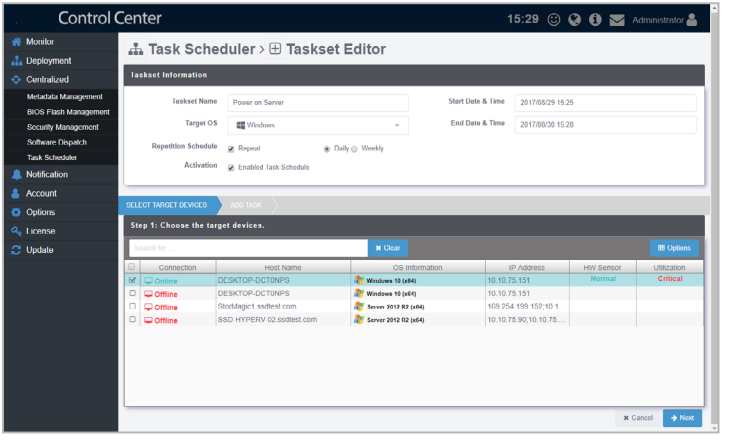


4.5.2 Changing the Calendar view layout

You may switch between different layouts in the calendar view

«	View previous year
»	View next year
<	View previous month
>	View next month
today	Move to the current day. The current day will be highlighted on the calendar.
month	Display month view
week	Display week view
day	Display day view
list	Display list of all tasks in the selected month and year.

4.5.3 Adding a new scheduled task



To add a new scheduled task:

1. Click on **Add**.
2. Enter the TaskSet Name, then select a Start Date & Time.
3. Select **Windows** or **Linux** in the **Target OS** field.
4. (optional) Check **Repeat**, then select **Daily** to repeat the task daily, or **Weekly** to repeat the task weekly.
5. (optional) You may select an end date and time.

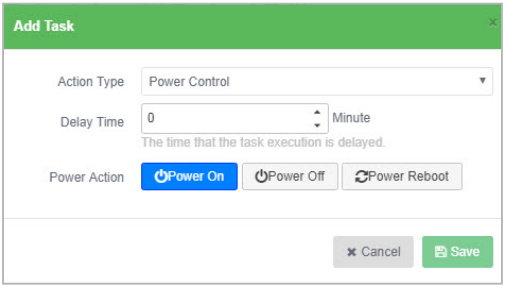
The end date and time option only appears when **Repeat** has been checked.

6. Check **Enabled Task Schedule** to enable and activate the task.

7. Once the Target Type has been selected, a list of all devices matching the Target Type will be displayed. Select the devices to apply the task to, then click **Next**.

You may search and filter items using the Search toolbar, for more details refer to **3.2.2 Filter devices using the Search toolbar**.

8. Click on **Add** in the middle-right of the screen to add a new task.



9. Select an action type. Each action type contains different options, see the table below for a list of the action types and the options available:

Action Type	Options
Power Control	Power On: Power on the device Power Off: Power off the device Power Reboot: Reboot the device
Service Control	Service Name: Enter the name of the service Start: Activate the service Stop: Stop the service Restart: Restart the service
Software Dispatch	Platform Type: Select from 32Bit, 64Bit, or 32_64Bit to filter the software options. Package Name: Select an item from the **Software Pool** to be installed. The options will vary according to the Bit type selected in **Platform Type**.
Security Control	Security Type: • **WatchDog** StatusWatchDog: Enable / Disable • **Registry Tool** StatusRegistry: Enable / Disable • **USB Control** StatusUsbAccess: Enable Access / Disable Access / Read Only

Linux only supports **Power Control** and **Security** action types.

10. Set the **Delay Time** (in minutes). This function is used to set a delay time before the task is executed.

When adding multiple tasks, ensure to set a Delay Time for each task to ensure the tasks are executed properly.

11. Once you have finished with setting the task, click on **Save**. The newly added task will be displayed in a timeline, you may click and drag the items in the timeline to rearrange the scheduled tasks. Clicking on will delete the task.
12. When you are finished, click on the **Save** at the bottom of the screen.

4.5.4 Editing a scheduled task

To edit a scheduled task:

1. Click on the task you wish to edit on the calendar in Calendar view.

   OR

   Click on the task you wish to edit from the list in History view.
2. Edit the details then click **Update** at the bottom of the screen when you have finished editing.
3. Click **Update** on the pop-up window to confirm the changes made.

4.5.5 Deleting a scheduled task

To delete a scheduled task:

1. Click on the task you wish to edit on the calendar in Calendar view.

   OR

   Click on the task you wish to edit from the list in History view.
2. Click **Delete** at the bottom of the screen, then click **Delete** on the pop-up window to delete the scheduled task.

Chapter 5

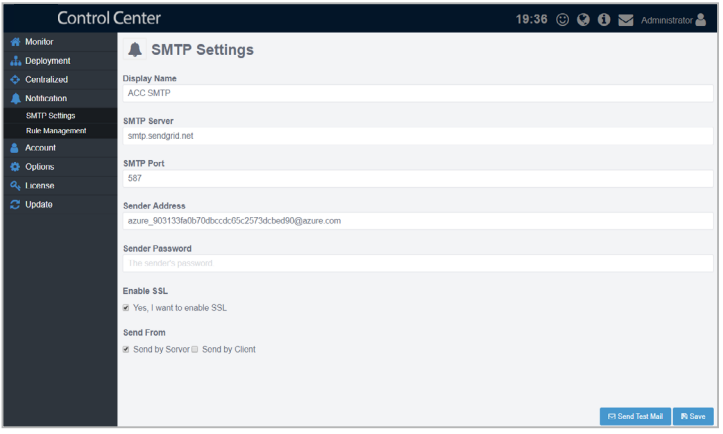
This chapter describes setting the notifications and SMTP Server

Notification Settings

5.1 Setting up the SMTP Server

The information entered in this section is for reference only.

Set up the SMTP (Simple Mail Transfer Protocol) for ReShield Control Center to allow feedback on system failures and alerts to be sent via email to the system administrator.

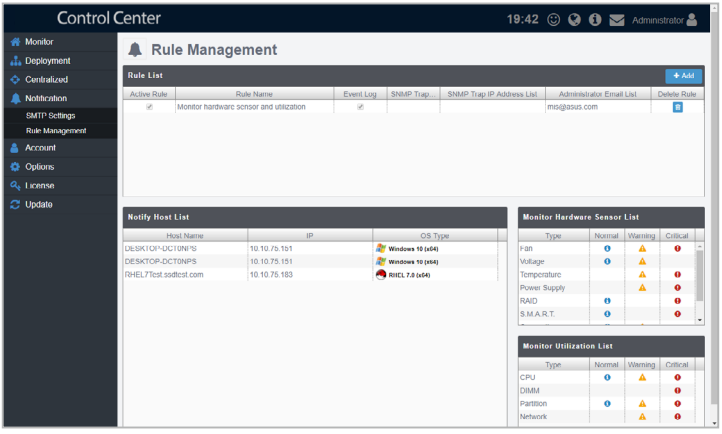


To set up the SMTP Server:

1. Click **Notification** > **SMTP Settings** to navigate to the settings page.
2. Enter the display name, SMTP server, SMTP port, sender address, and password.
3. Check **Yes, I want to enable SSL** to enable SSL.
4. Select the devices to use the SMTP server:
   - **Send by Server:** Client devices will send the notification information to the server first, the server will then send the notification email.
   - **Send by Client:** Notification emails will be sent from the client device.
5. Click on **Send Test Mail** to check the status of the SMTP. If the SMTP is functioning properly, you should receive an email.
6. Click **Save** to save the changes made, after confirming the SMTP is functioning.

5.2 Rule Management

Rule management allows you to add or delete rules on notifications. When a device is in warning or critical status, an email will be sent to the system administrator.



5.2.1 Adding rules for notifications

To add a rule:

1. Click **Add**.
2. Enter a rule name, then select the devices to apply the rule to. Click **Next**.
3. Select conditions (type and status of hardware or utilization sensors) to send notifications, then click **Next**.

- The checkbox checked when selecting the hardware sensor or utilization type and status will send notifications when the status shifts from the other two statuses to the status checked. For example, checking **Normal** will send notifications when the status changes from **Warning** or **Critical** to **Normal**.
- To set the status thresholds for the Utilization Type, please refer to **3.6 Setting the threshold for sensors**.

4. (optional) Check **Event Log** to select if the event log should be sent in the email.

5. (optional) Check **SNMP Trap** to automatically send notifications to the administrators when a warning or critical event occurs.
6. (optional) Enter the email addresses the notification should be sent to, then click **Save**.

Ensure to set up the SMTP server settings before using the email function. For more information please refer to **5.1 Setting up the SMTP Server**.

When entering multiple emails, use a semicolon ' **;** ' to separate the emails.

5.2.2 Deleting notification rules

To delete a notification rule:

1. Select a rule in the **Rule List** you wish to delete, then click on  in the **Delete Rule** column.
2. Click **Delete** to delete the rule.

Chapter 6

This chapter describes how to add and edit accounts for different users.

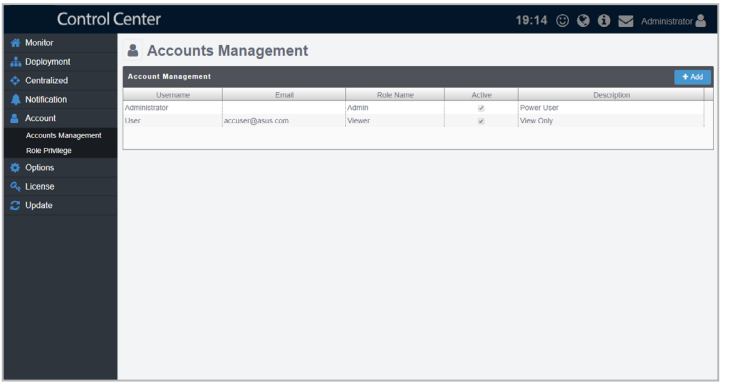
Account Management

6.1 Account Management

The account management function displays all user accounts on ReShield Control Center, and allows you to add, edit, or delete user accounts.

To access **Account Management**:

- Click **Account** > **Account Management** from the left menu.
- Click **Account Information** in the top right corner, then select **Settings**.



6.1.1 Adding new accounts

To add new accounts:

1. Click on **Add**.
2. Enter the username, password, email, and description of the new account.
3. Select a role in the Role Name field.

For more details on adding new roles, please refer to 6.2 Role Privilege.

4. Check **Enable the account** in the **Active Account** field to enable the account.
5. Click **Save** once you have finished entering the account details.

The maximum of users is 12. With the possibility of simultaneous work.

6.1.2 Editing accounts

To edit an account:

1. Click on the account you wish to edit from the Account Management block.
2. Modify the account, then click **Save** to save the changes made to the account.
3. Click **OK** to confirm the update to the account details.

6.1.3 Deleting accounts

To delete an account:

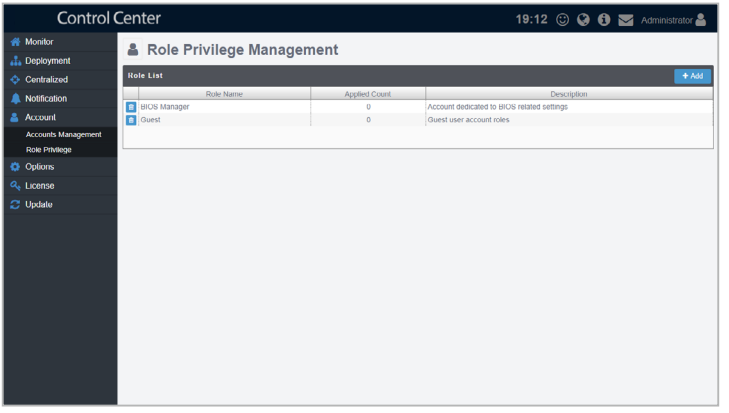
1. Double-click on the account you wish to delete.
2. Click on **Delete**, then click **Delete** in the pop-up window to delete the account.

The Administrator account may not be deleted.

6.2 Role Privilege

The Role Privilege function displays all roles on ReShield Control Center, and allows you to add, edit, or modify permissions of different roles that you may assign to users.

To access **Role Privilege**, click **Account** > **Role Privilege** from the left menu.



6.2.1 Adding new roles

To add new roles:

1. Click on **Add**.
2. Enter the role name, and description of the new role.
3. Select and check the permissions to enable for the role in the Privilege Configuration block.

You may search and filter items using the Search toolbar, for more details refer to **3.2.2 Filter devices using the Search toolbar**.

4. Click **Add** once you have finished setting the role privileges.

6.2.2 Editing roles

To edit a role:

1. Click on the role you wish to edit from the Role List block.
2. Modify the role, then click **Update**.
3. Click **Update** in the pop-up window to confirm the update to the role.

6.2.3 Deleting roles

- To delete a role from the Role Privilege window:
  1. Click the icon next to the role you wish to delete.
  2. Click **Delete** to delete the role.

Accounts associated with the role will also be deleted.

- To delete a role from the Role Configuration window:
  1. Click on the role you wish to delete from the Role List block.
  2. Click on **Delete**, then click on Delete in the pop-up window to delete the role.

Accounts associated with the role will also be deleted.

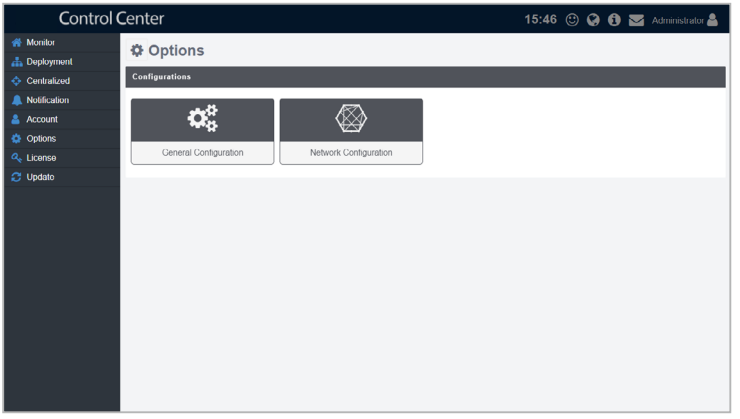
Chapter 7

This chapter describes system configuration options, and License information.

Server Configurations

7.1 General and Network Configurations

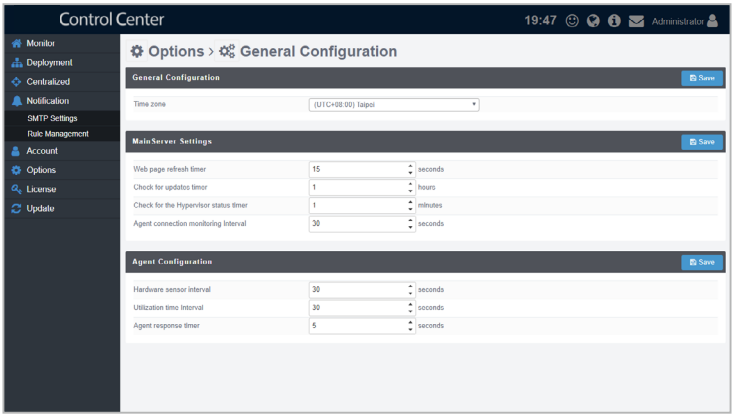
The General and Network configurations can be accessed through the Options screen and allows you to configure different settings for the MainServer, agents, and network.



7.1.1 General Configuration

The General Configuration screen allows you to configure different settings for the MainServer and agents.

To access **General Configuration**, click **Options** then select **General Configuration** from the Options screen.



Changes made to each section will only be applied after clicking the **Save** button in each section respectively.

General Configuration List

Set the Timezone of the ReShield Control Center by selecting a timezone from the dropdown list.

MainServer Settings List

Adjust the intervals for web page refreshment, system update detection, and Hypervisor/agent status check via the mainserver.

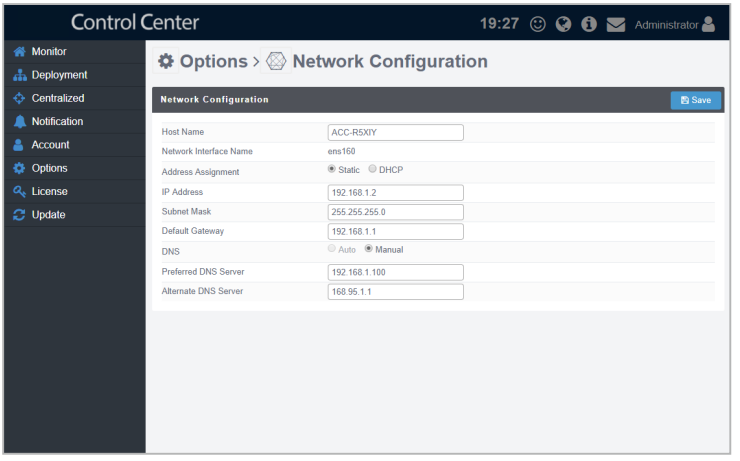
Agent Configuration List

Configure the interval at which agents will respond to server requests, or set the interval at which the agent will monitor the hardware and utilization sensors.

7.1.1 Network Configuration

The Network Configuration screen allows you to configure network settings.

To access **Network Configuration**, click **Options** then select **Network Configuration** from the Options screen.

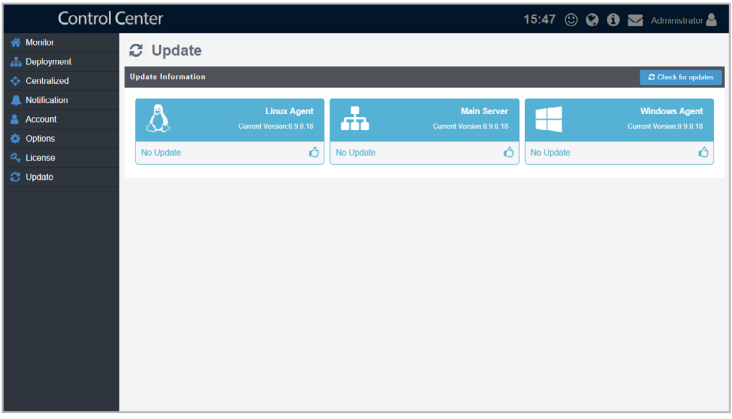


Network Configuration

Set the network configurations automatically (DHCP), or manually (Static). If you select **Static**, you will need to enter the IP Address, Host Name, Subnet Mask, Gatweway Address, and DNS server.

7.2 Checking for system updates

The Update screen will display available updates for the Linux Agent, Windows Agent, and Main Server, you may manually refresh the updates screen by clicking on **Check Refresh**. Clicking on an update will automatically update the server and agent without needing to restart the system.

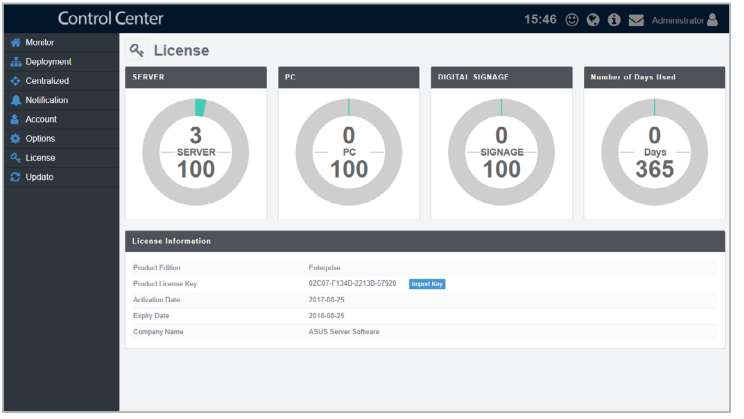


Ensure to add *http //reshield.nav-it.ru/** to your firewall exceptions list to enable update checks.

7.3 License Information

This screen displays the license information of your ReShield Control Center, this includes your license key, activation date, expiry date and edition.

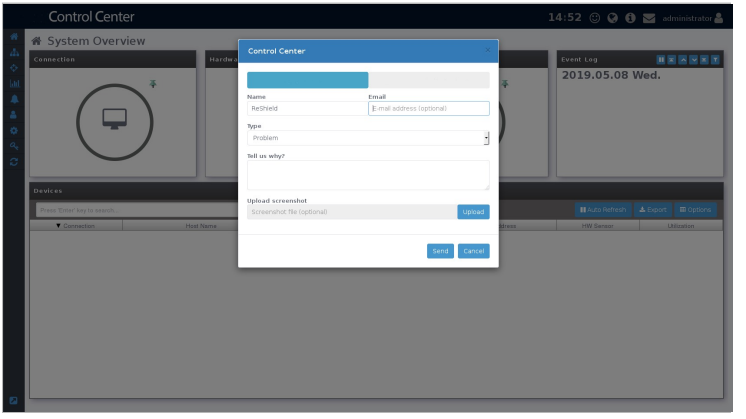
If you have a product license key, you may also import and activate your license key by clicking on **Import Key**. For more information on license keys, refer to http://reshield.nav-it.ru/.



7.4 ReShield ProDesk

ReShield ProDesk is a tool to automate technical support and inventory for all manufactured products of the company.

It is possible to get access to the appeal to technical support by the button in the upper corner. We analyze every call in detail and immerse ourselves in every question. We are always looking for the most optimal and systematic solution to the problem.



Appendix

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

Appendix

System Requirements

Hardware Host Server Requirements

Virtual machine hypervisors	Oracle VirtualBox 5.1.x VMware ESXi 5.x Microsoft Hyper-V 3.0
Virtual machine resources (200 clients capability)	4 vCPU 8 GB memory 100 GB disk space
Minimum VM requirement (50 clients capability)	2 vCPU 4 GB memory 100 GB disk space
Networking	HTTP / HTTPS SMTP SNMP Connection among devices
Supported Internet browsers	Browsers with HTML5 support Google Chrome Firefox Apple Safari

Managed Clients Requirements

Supported client OS	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows 7 Windows 8.1 Windows 10 Windows Embedded 7 RedHat 6.4~6.8 CenOS 6.4~6.8 Scientific Linux 6.4~6.8
Requirement on Client Systems	Windows .NET Framework 3.5 Linux sysstat, smartmontools, wireless-tools, ethtool, ipmitool, Open IPMI driver, ASMB