Sentry Power Manager (SPM) – Email Escalation Enhancement

Purpose

Email Escalation is a significant enhancement to SPM's Alerting subsystem for allowing SPM administrators to escalate, filter, and set schedules that determine when SPM alerts will be delivered and where those alerts will be targeted.

The enhancement is readily accessible within the SPM graphical user interface and does not require a separately purchased software license key. However, access is available only to administrative-level user accounts running SPM version 6.1 or later, and only after activating the enhancement with a global system setting that enables an alarm policy to send a specific alert to designated recipients.

This technical note provides step-by-step instructions and examples for using the full functionality of SPM's enhanced Email Escalation.

Before You Begin

To use Email Escalation, you will need:

- Sentry Power Manager (SPM), version 6.1 or later.
- An SPM administrative-level user account.
- Enable the enhancement at Global setting at > Email Setup > Email Server > SMTP: Enable.
- Configure the Policy Polling Period at Admin Setup > Advanced Settings > Server Settings.

Overview

Email Escalation improves email notification functionality from earlier SPM releases by providing an enhanced design for setting up email and creating alarm policies. Administrators can define unique alarm policies that will translate active device alarms into customized email alerts for distribution.

Some key areas include:

- The enhancement allows email alerts to be configured by a zone or location.
- Email recipients do not have to be SPM users.
- You can gather designated email recipients into an email group and apply an alarm policy to the group.
- The enhancement places information from the Device Discovery feature and user actions/logins into a report instead of into an email. These reports can be scheduled and emailed like other scheduled tasks in SPM.
- If you have upgraded from an earlier version of SPM, and in that version you had configured the SMTP server, email recipients, and Alarm Status as an Email notification category, the information will auto-populate into the related enhancement windows of SPM 6.1. However, if you are new to SPM with version 6.1, you will have to provide this information manually.

What Is Not Supported

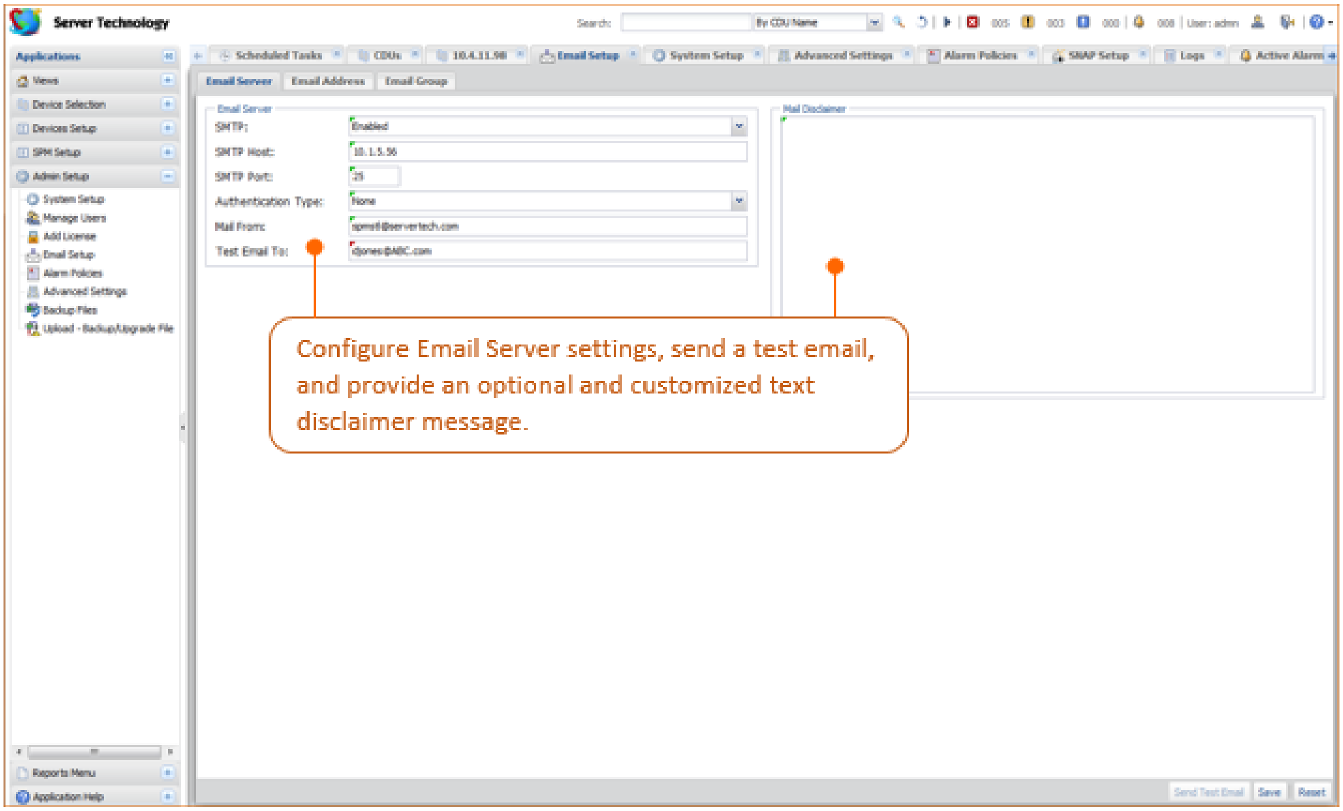
Areas that the Email Enhancement does not cover:

- SPM Hub and Node systems.
- The SPM API.
- Spreadsheet tools external to SPM.
- Consolidation to a single email.

Part 1: Starting with Email Setup

To use the enhancements of Email Escalation in SPM version 6.1 or later, begin with Email Setup. Email Setup provides SMTP server settings, setting of recipient email addresses, and allows the grouping of email recipients.

Log in to SPM and go to **Admin Setup > Email Setup**. The window defaults to the Email Server tab.



Email Server

SMTP: Enabled

SMTP Host: 10.1.5.56

SMTP Port: 25

Authentication Type: None

Mail From: spmsl@servertech.com

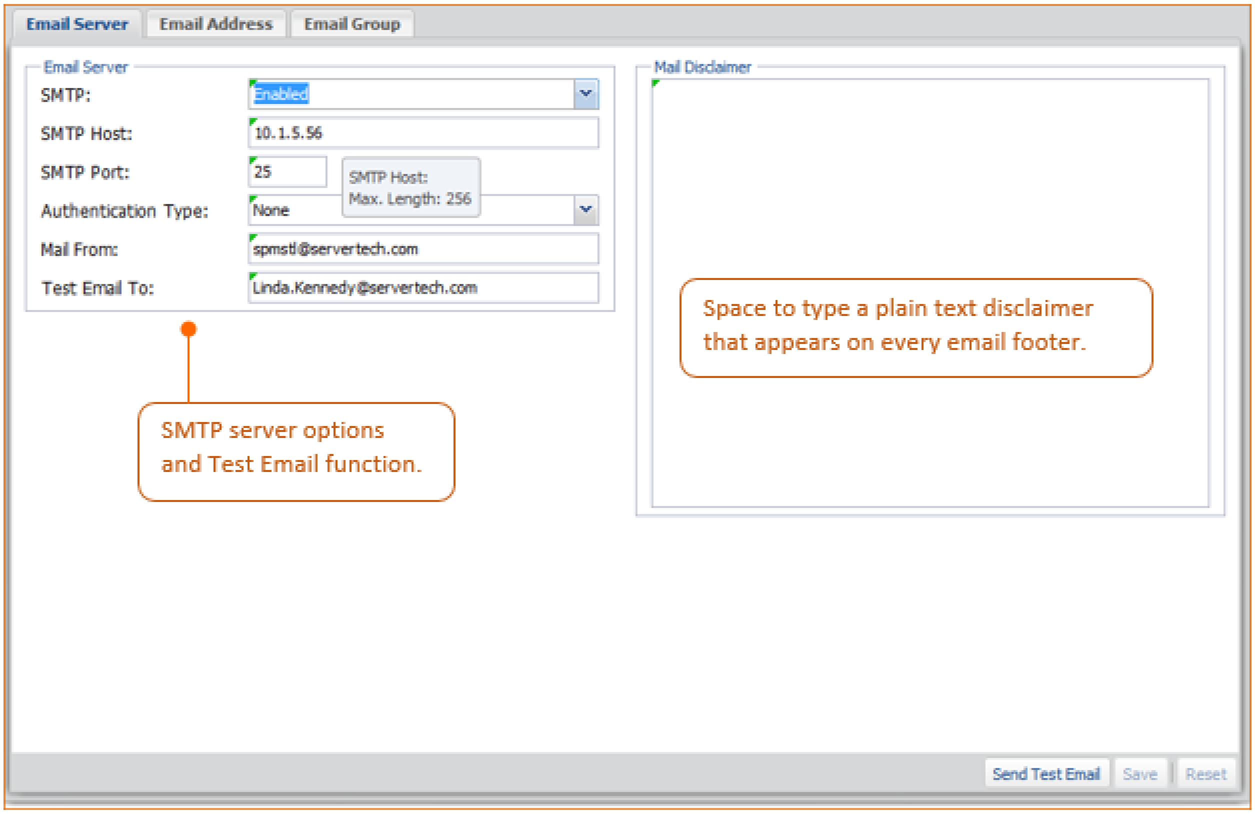
Test Email To: djones@ABC.com

Configure Email Server settings, send a test email, and provide an optional and customized text disclaimer message.

Email Server Tab

The Email Server Tab has several uses:

- Enables the SMTP server (required for Email Setup functionality).
- Specifies the SMTP server host name and SMTP port number (default port is 25).
- Allows selection of the SMTP authentication type (default is none) and provides the sending email address for your SPM system.
- Lets you enter an (optional) plain text customized disclaimer message that will be added to the footer of all sent emails.
- Provides an email test function.



SMTP: Enabled
SMTP Host: 10.1.5.56
SMTP Port: 25
Authentication Type: None
Mail From: spmstl@servertech.com
Test Email To: Linda.Kennedy@servertech.com

SMTP server options and Test Email function.

Space to type a plain text disclaimer that appears on every email footer.

If you have upgraded to SPM 6.1 or later from a previous SPM version, the fields on the Email Server tab will be populated with the same Email Server settings and disclaimer you set up in the Email Notification section of your previous SPM version.

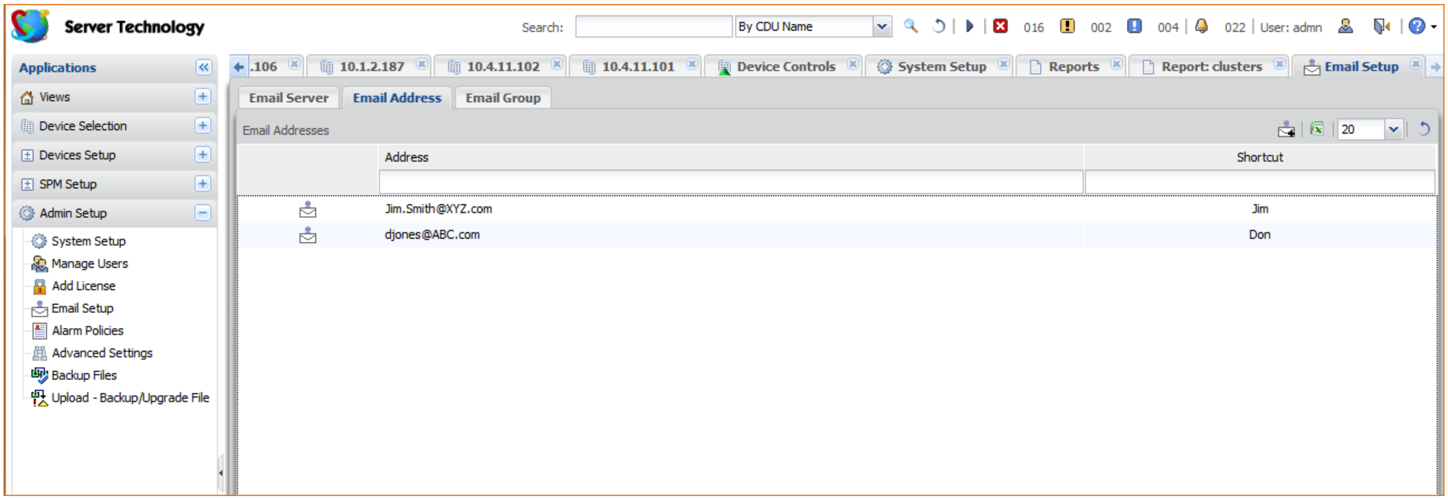
If you are new to SPM with version 6.1 or later, then you will need to complete the fields manually for the Email Server tab. See the window example above for step-by-step instructions.

Test Email

To test the email setup, provide an email recipient and click the **Send Test Email** button.

Email Address Tab

A list of specified email recipients with whom you can send text communication about system activity.



Email Addresses

Address	Shortcut
Jim.Smith@XYZ.com	Jim
djones@ABC.com	Don

If you have upgraded to SPM 6.1 or later from a previous SPM version, the list of recipients on the Email Address tab will be populated with the same email addresses you set up in the Email Notification section of your previous SPM version.

If you are new to SPM with version 6.1 or later, then you will need to add the email addresses manually for the Email Address tab. See the window example above for step-by-step instructions.

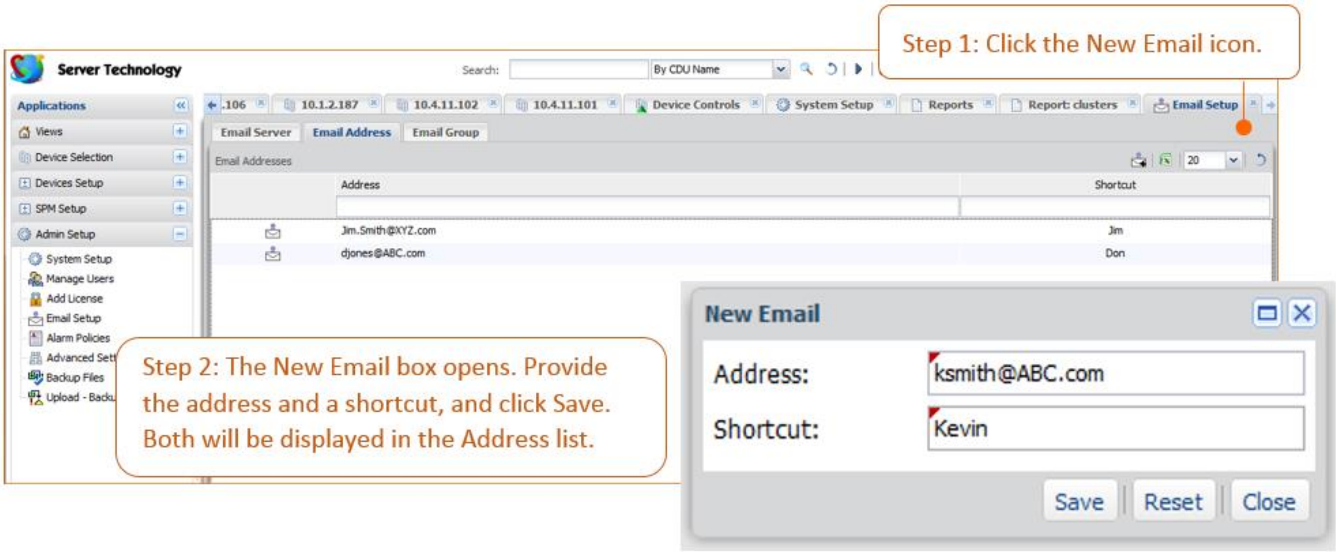
The email addresses in this list, either migrated or added, will be displayed throughout the Email Setup and Alarm Policies areas.

About SMS Messaging

To use SMS text communication and receive notification on mobile phones, convert the 10-digit mobile number to an email address. The format of the email address and the text message rates that apply depend on the mobile provider.

EXAMPLE: If the mobile provider is ATT, convert the following mobile number to an email address as follows: This ATT mobile phone number: 775-555-1234 converted to an email address is 7755551234@txt.att.netType the converted address into one of the Mail To recipient fields.

Adding a New Email Address



Step 1: Click the New Email icon.

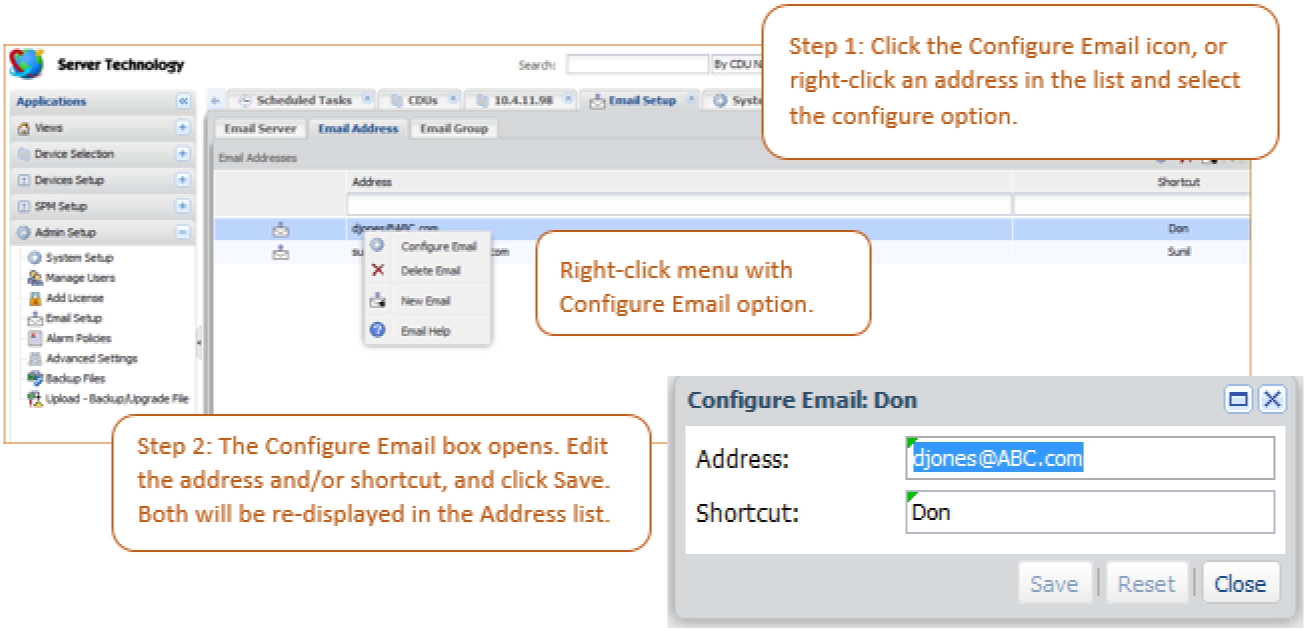
Address	Shortcut
Jim.Smith@XYZ.com	Jim
djones@ABC.com	Don

Step 2: The New Email box opens. Provide the address and a shortcut, and click Save. Both will be displayed in the Address list.

Address: ksmith@ABC.com

Shortcut: Kevin

Configuring an Email Address



Step 1: Click the Configure Email icon, or right-click an address in the list and select the configure option.

Right-click menu with Configure Email option.

Step 2: The Configure Email box opens. Edit the address and/or shortcut, and click Save. Both will be re-displayed in the Address list.

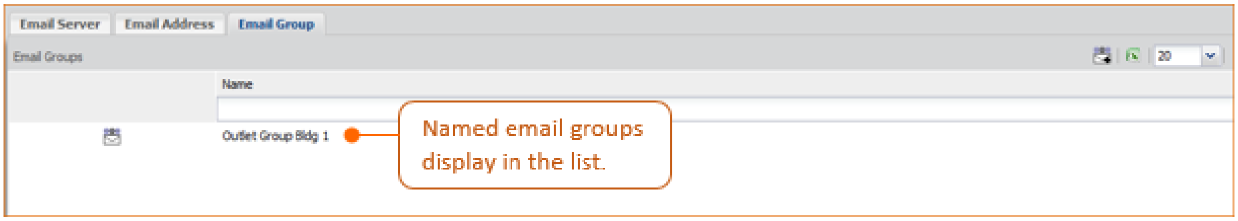
Configure Email: Don

Address: djones@ABC.com

Shortcut: Don

Email Group Tab

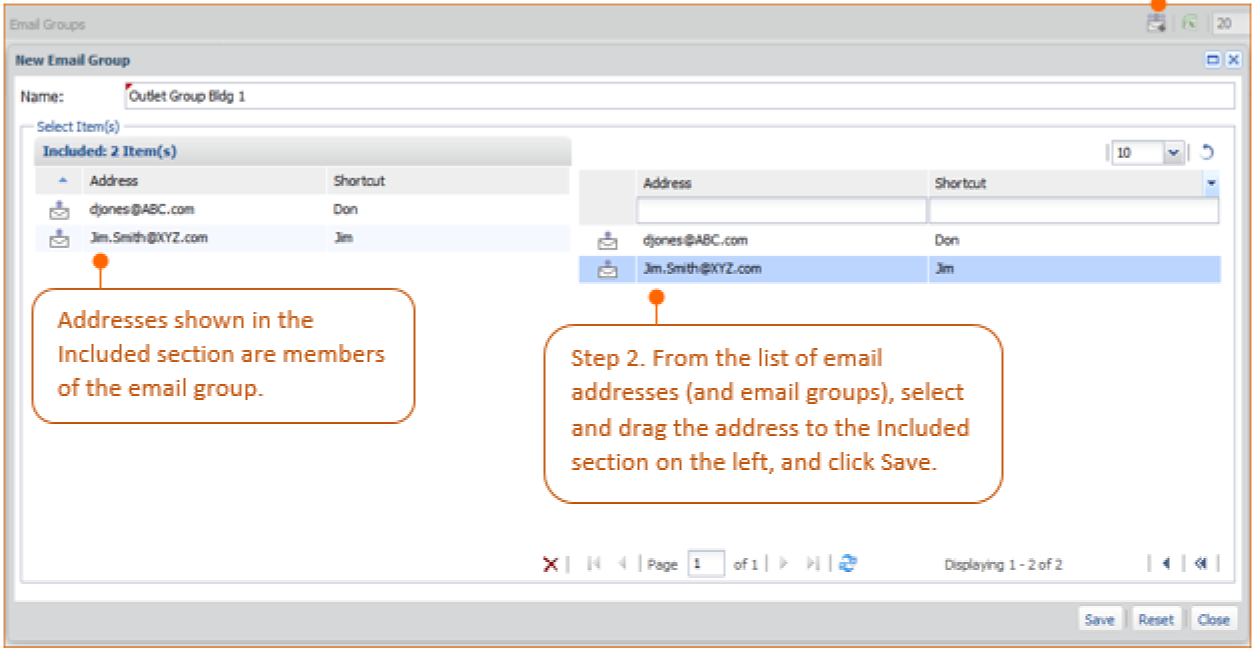
Configuration window that allows one or more individual email addresses to be added to an email group. An alarm policy can be set up to target a specific email group to determine the type of alert the group receives.



Named email groups display in the list.

Adding a New Email Group

Step 1: From the Email Groups list, click the New Email Group icon to open the window below.



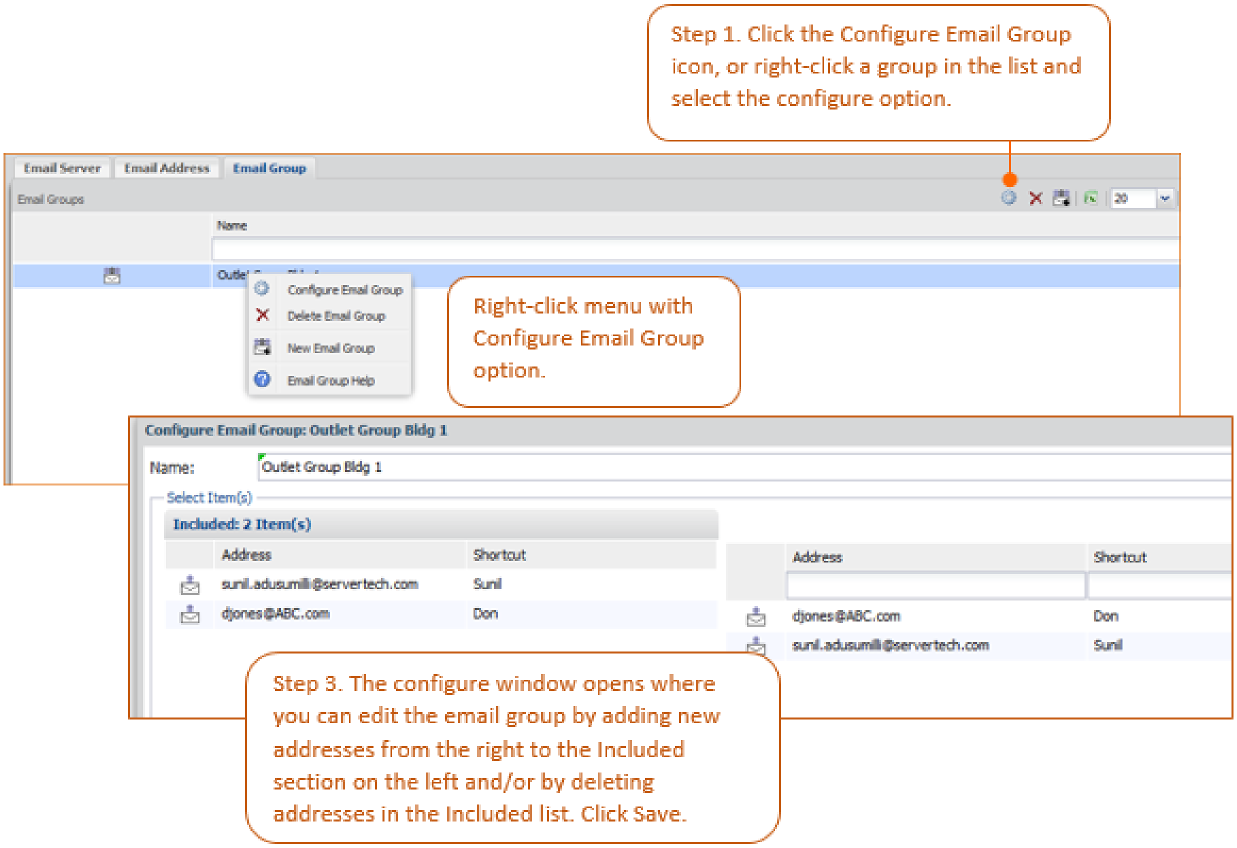
Name: Outlet Group Bldg 1

Address	Shortcut
djones@ABC.com	Don
Jim.Smith@XYZ.com	Jim

Addresses shown in the Included section are members of the email group.

Step 2. From the list of email addresses (and email groups), select and drag the address to the Included section on the left, and click Save.

Configuring an Email Group



Step 1. Click the Configure Email Group icon, or right-click a group in the list and select the configure option.

Right-click menu with Configure Email Group option.

Configure Email Group: Outlet Group Bldg 1

Name: Outlet Group Bldg 1

Select Item(s)

Included: 2 Item(s)

Address	Shortcut
sunil.adusumilli@servertech.com	Sunil
djones@ABC.com	Don

Address	Shortcut
djones@ABC.com	Don
sunil.adusumilli@servertech.com	Sunil

Step 3. The configure window opens where you can edit the email group by adding new addresses from the right to the Included section on the left and/or by deleting addresses in the Included list. Click Save.

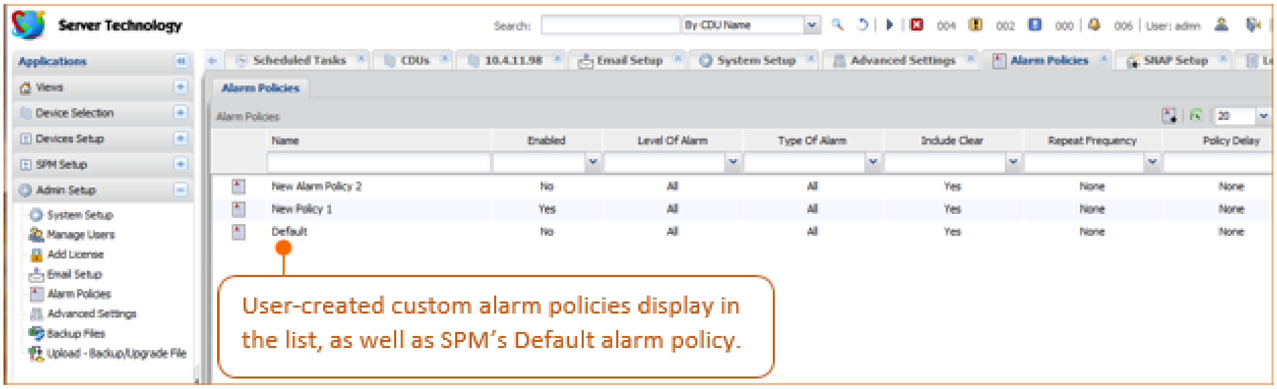
Part 2: Working with Alarm Policies

An alarm policy is a set of rules you specify to drive an active device alarm into an email alert for one or more specified email recipients or email groups.

Multiple emails rules can be applied to the alerts with the ability to delay by email, if desired. The rules can be repeated and filtered based on Critical or All alarms.

The Alarm Policies Window

After Email Setup has been completed as previously described in Part 1, go to **Admin Setup > Alarm Policies**. The Alarm Policies window displays.



Alarm Policies

Name	Enabled	Level Of Alarm	Type Of Alarm	Include Clear	Repeat Frequency	Policy Delay
New Alarm Policy 2	No	All	All	Yes	None	None
New Policy 1	Yes	All	All	Yes	None	None
Default	No	All	All	Yes	None	None

User-created custom alarm policies display in the list, as well as SPM's Default alarm policy.

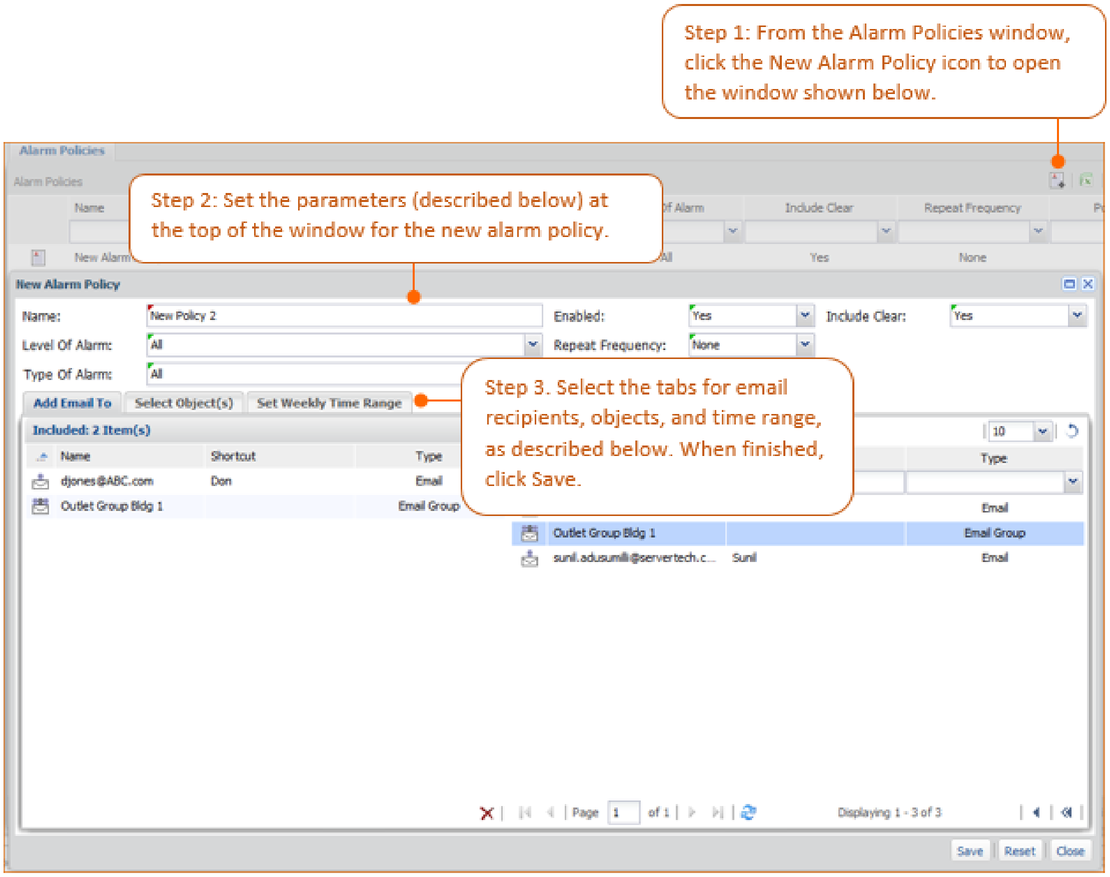
Default Alarm Policy

The Default alarm policy is provided by SPM as a convenient and optional starting place for creating a new alarm, however, it is not required for creating new user-customized policies.

If you choose, the default policy can be configured, renamed, or deleted like any other alarm policy.

The parameters of the default policy are: will be applied to all devices, on, immediate, all levels, no filters, include clear, and include outlet groups.

Creating a New Alarm Policy



Step 1: From the Alarm Policies window, click the New Alarm Policy icon to open the window shown below.

Step 2: Set the parameters (described below) at the top of the window for the new alarm policy.

Step 3. Select the tabs for email recipients, objects, and time range, as described below. When finished, click Save.

Name: New Policy 2
Enabled: Yes
Include Clear: Yes
Level Of Alarm: All
Repeat Frequency: None
Type Of Alarm: All

Included: 2 Item(s)

Name	Shortcut	Type
djones@ABC.com	Don	Email
Outlet Group Bldg 1		Email Group

Name	Shortcut	Type
		Email
Outlet Group Bldg 1		Email Group
sunil.adusumilli@servertech.c...	Sunil	Email

Alarm Policy Parameters

Name: (Required). Provide a name for the new alarm policy.

Level of Alarm: All or Critical. Filters the level of alarm to be sent.

Type of Alarm: Can be filtered based on whether the email is Power only (just power readings), Environment only (temperature/humidity readings), or All (every alarm).

Enabled: Yes or No. Determines whether the policy is active or inactive. Only enabled alarm policies can be deployed.

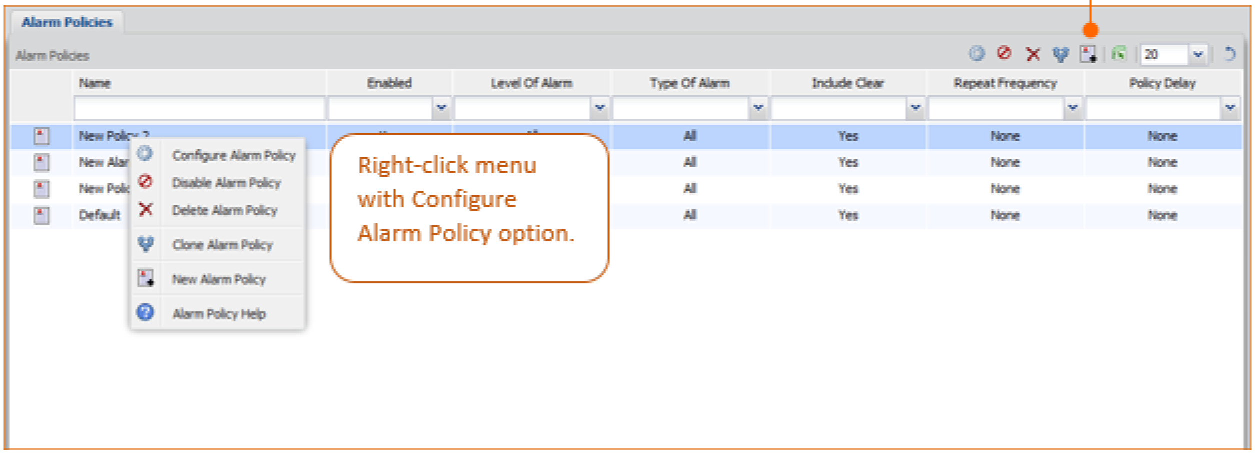
Repeat Frequency: None, or a range from 1 minute to 1 week. Determines that the alert will be sent to the recipient(s) more than once and how often the alert will be repeated. The None option disables the repeat frequency.

Policy Delay: None, or a range from 1 minute to 1 week. Delay is how long after the alarm occurs on the device that an email recipient is notified, and how often the alert is sent between repeat frequency, if set. The None option disables the policy delay.

Include Clear: Yes or No. Clear is an email alert sent to confirm resolution of the device alarm.

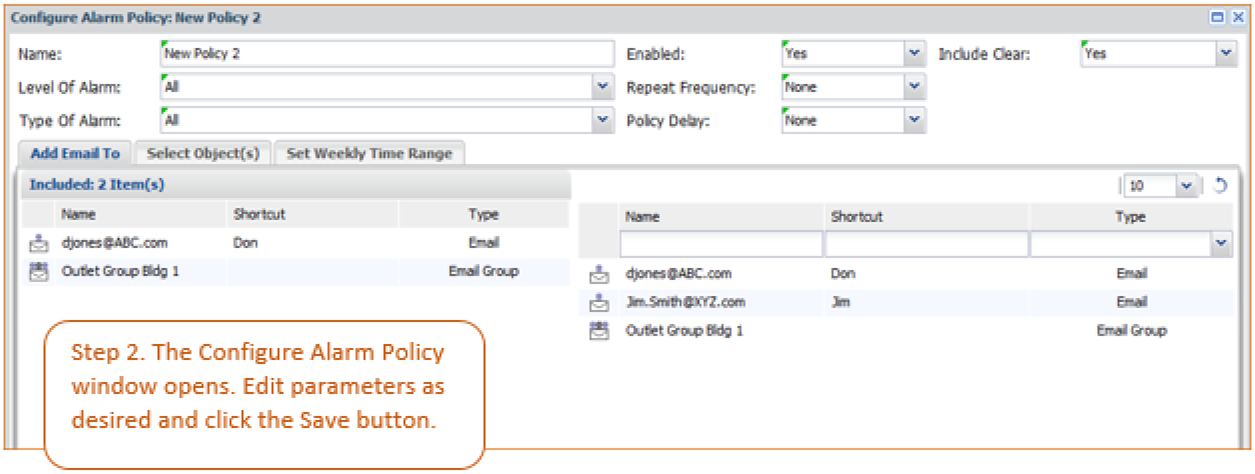
Configuring an Alarm Policy

Step 1. Click the Configure Alarm Policy icon, or right-click an alarm policy in the list and select the configure option.



Name	Enabled	Level Of Alarm	Type Of Alarm	Include Clear	Repeat Frequency	Policy Delay
New Polic 2			All	Yes	None	None
New Alar			All	Yes	None	None
New Poli			All	Yes	None	None
Default			All	Yes	None	None

Right-click menu with Configure Alarm Policy option.



Name: New Policy 2
Enabled: Yes
Include Clear: Yes
Level Of Alarm: All
Repeat Frequency: None
Type Of Alarm: All
Policy Delay: None

Included: 2 Item(s)

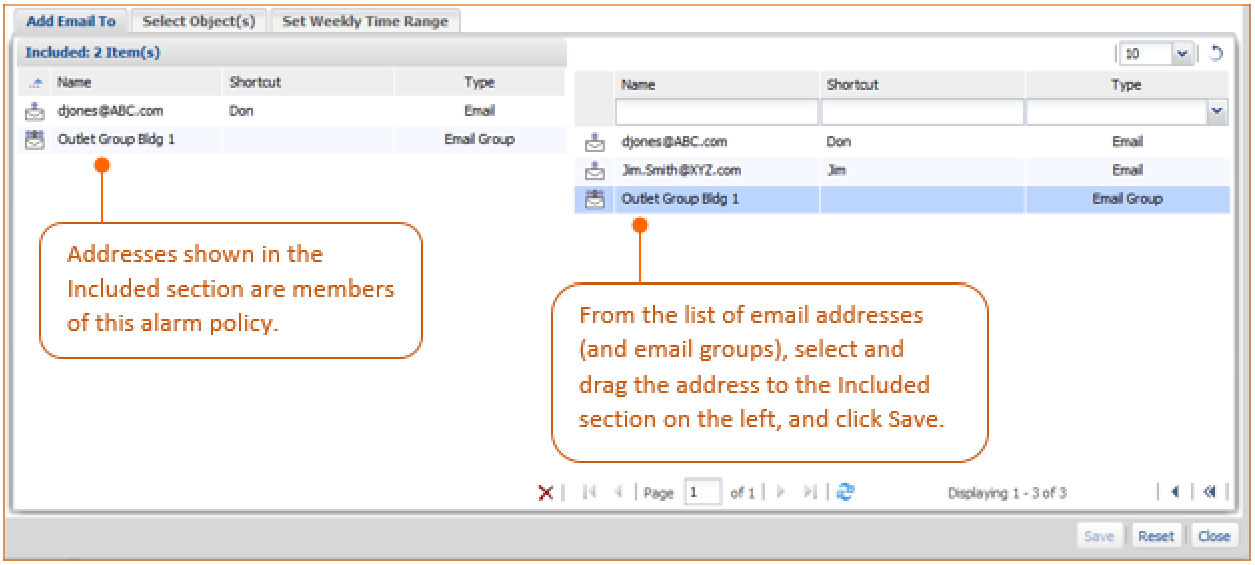
Name	Shortcut	Type
djones@ABC.com	Don	Email
Outlet Group Bldg 1		Email Group

Name	Shortcut	Type
djones@ABC.com	Don	Email
Jim.Smith@XYZ.com	Jim	Email
Outlet Group Bldg 1		Email Group

Step 2. The Configure Alarm Policy window opens. Edit parameters as desired and click the Save button.

Add Email To Tab

This tab provides the email recipient list that is based on the email addresses from the **Email Setup > Email Address** tab. Select any number of individual recipients (or email groups) to be included in the alarm policy.



Included: 2 Item(s)

Name	Shortcut	Type
djones@ABC.com	Don	Email
Outlet Group Bldg 1		Email Group

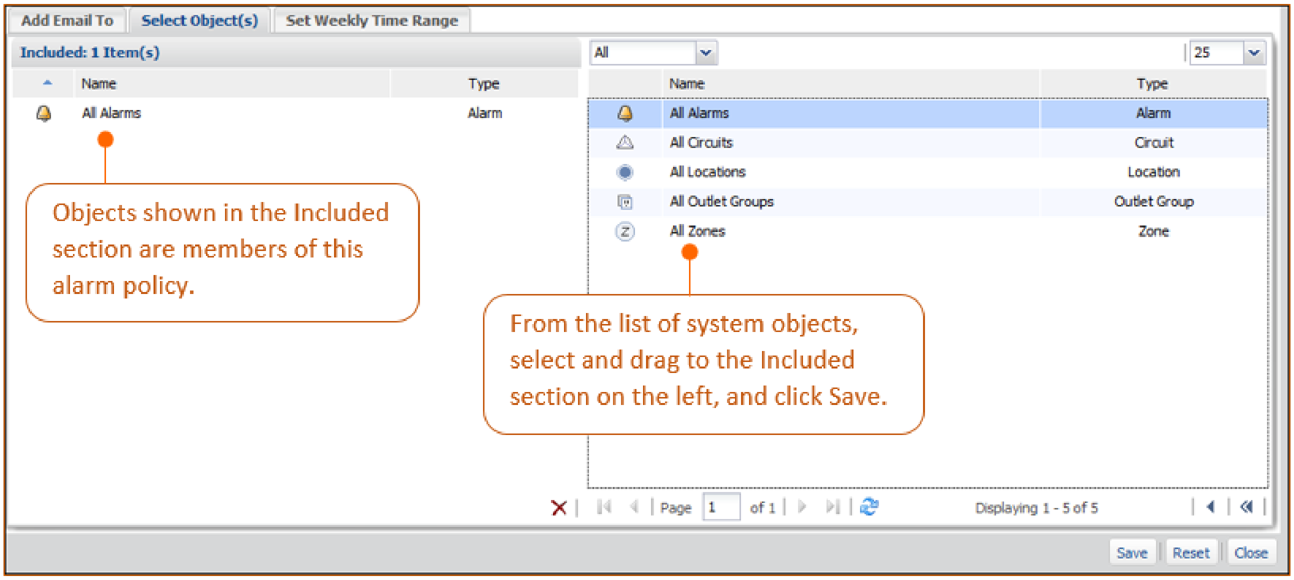
Name	Shortcut	Type
djones@ABC.com	Don	Email
Jim.Smith@XYZ.com	Jim	Email
Outlet Group Bldg 1		Email Group

Addresses shown in the Included section are members of this alarm policy.

From the list of email addresses (and email groups), select and drag the address to the Included section on the left, and click Save.

Select Object(s) Tab

This tab allows you to determine the type of system objects that will be included in the alarm policy. Locations, zones, circuits, and outlet groups can be added to the alarm policy. Cabinets will be added if they belong to a zone or location.



Included: 1 Item(s)

Name	Type
All Alarms	Alarm

Objects shown in the Included section are members of this alarm policy.

Name	Type
All Alarms	Alarm
All Circuits	Circuit
All Locations	Location
All Outlet Groups	Outlet Group
All Zones	Zone

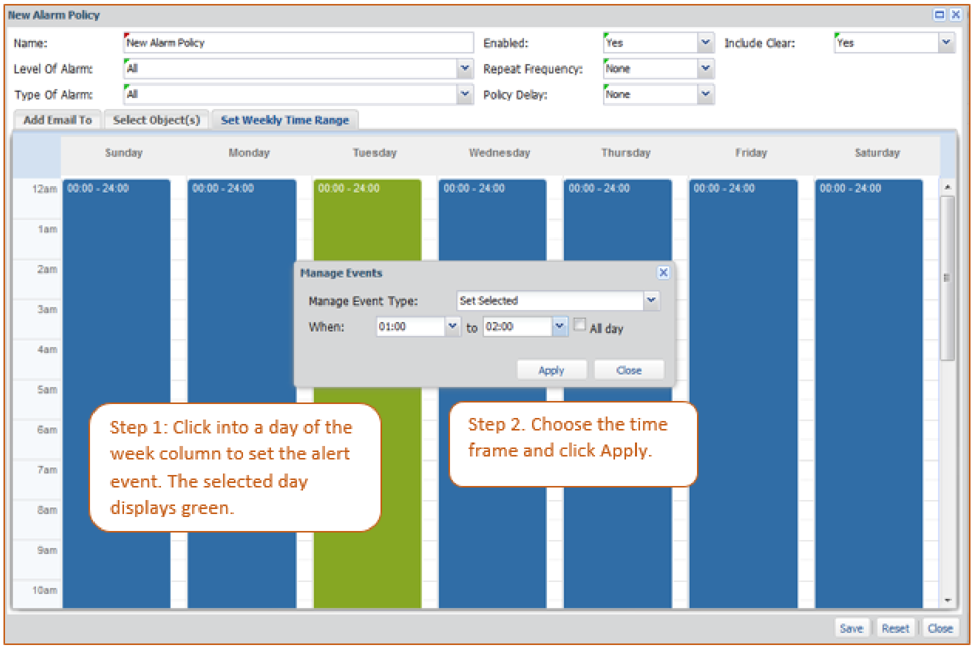
Displaying 1 - 5 of 5

From the list of system objects, select and drag to the Included section on the left, and click Save.

Set Weekly Time Range

This tab allows you to determine the days of the week and time of day for an active alarm policy to be deployed. Weekdays, weekends, and night shift hours can be selected and set (or cleared) by day and 24-hour time period.

To deploy an alarm event:

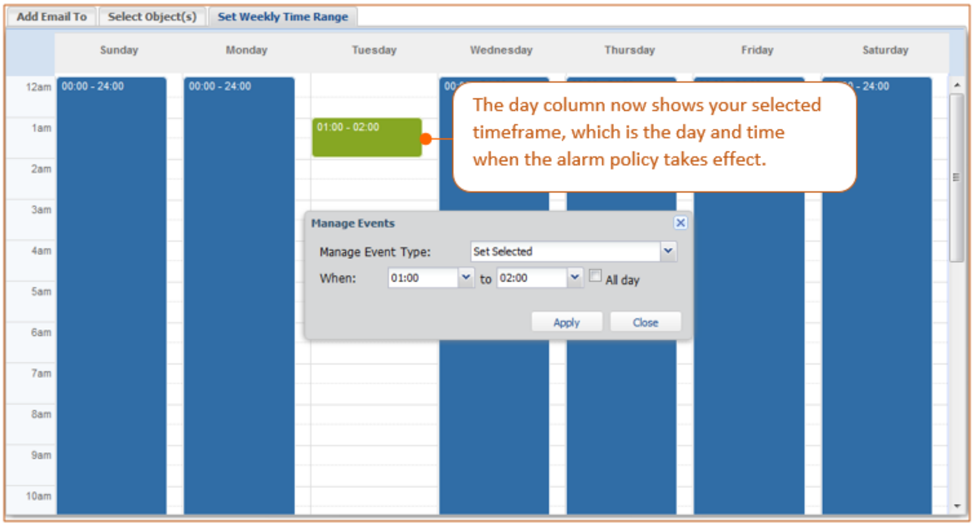


Name: New Alarm Policy
Enabled: Yes
Include Clear: Yes
Level Of Alarm: All
Repeat Frequency: None
Type Of Alarm: All
Policy Delay: None

Manage Event Type: Set Selected
When: 01:00 to 02:00 ☐ All day

Step 1: Click into a day of the week column to set the alert event. The selected day displays green.

Step 2. Choose the time frame and click Apply.

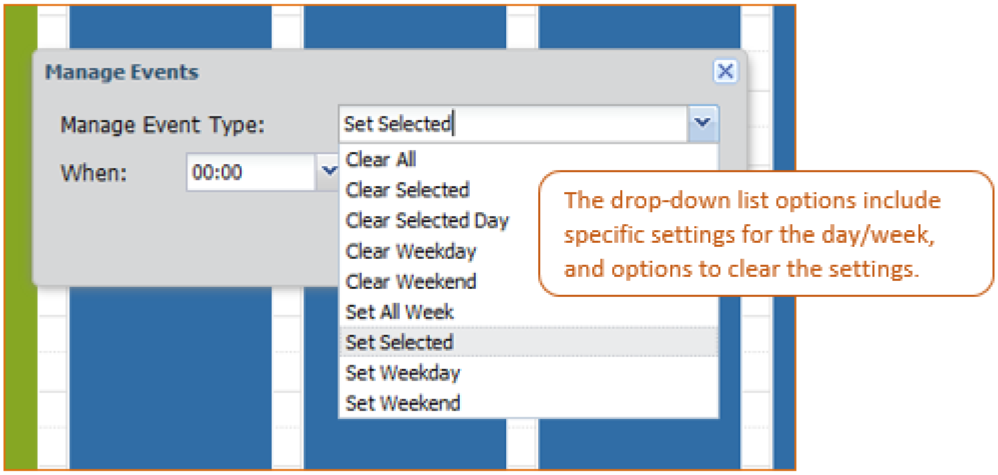


The day column now shows your selected timeframe, which is the day and time when the alarm policy takes effect.

Manage Event Type: Set Selected
When: 01:00 to 02:00 ☐ All day

The day column changes to show the time (start and end) when the alarm policies will take effect and send email alerts as configured.

To manage weekly time range events:



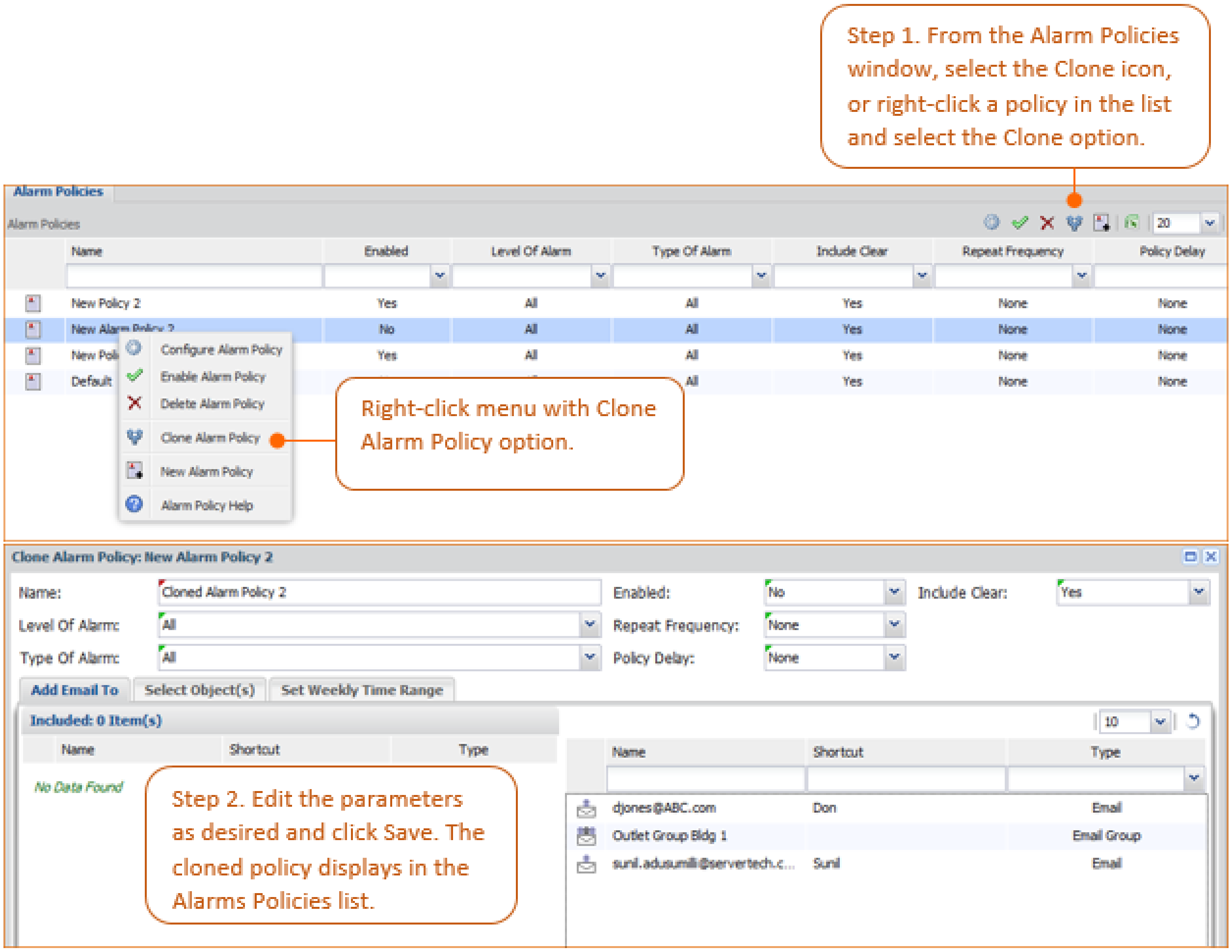
The drop-down list options include specific settings for the day/week, and options to clear the settings.

-

Several options for clearing and setting the weekly time range columns are available on the Manage Events drop-down list.

Cloning an Alarm Policy

A cloned alarm policy allows you to quickly customize a new alarm policy based on an existing policy.



Step 1. From the Alarm Policies window, select the Clone icon, or right-click a policy in the list and select the Clone option.

Alarm Policies

Name	Enabled	Level Of Alarm	Type Of Alarm	Include Clear	Repeat Frequency	Policy Delay
New Policy 2	Yes	All	All	Yes	None	None
New Alarm Policy 2	No	All	All	Yes	None	None
New Poli	Yes	All	All	Yes	None	None
Default			All	Yes	None	None

Right-click menu with Clone Alarm Policy option.

Clone Alarm Policy: New Alarm Policy 2

Name: Cloned Alarm Policy 2
Enabled: No
Include Clear: Yes
Level Of Alarm: All
Repeat Frequency: None
Type Of Alarm: All
Policy Delay: None

Included: 0 Item(s)

Name	Shortcut	Type
No Data Found		

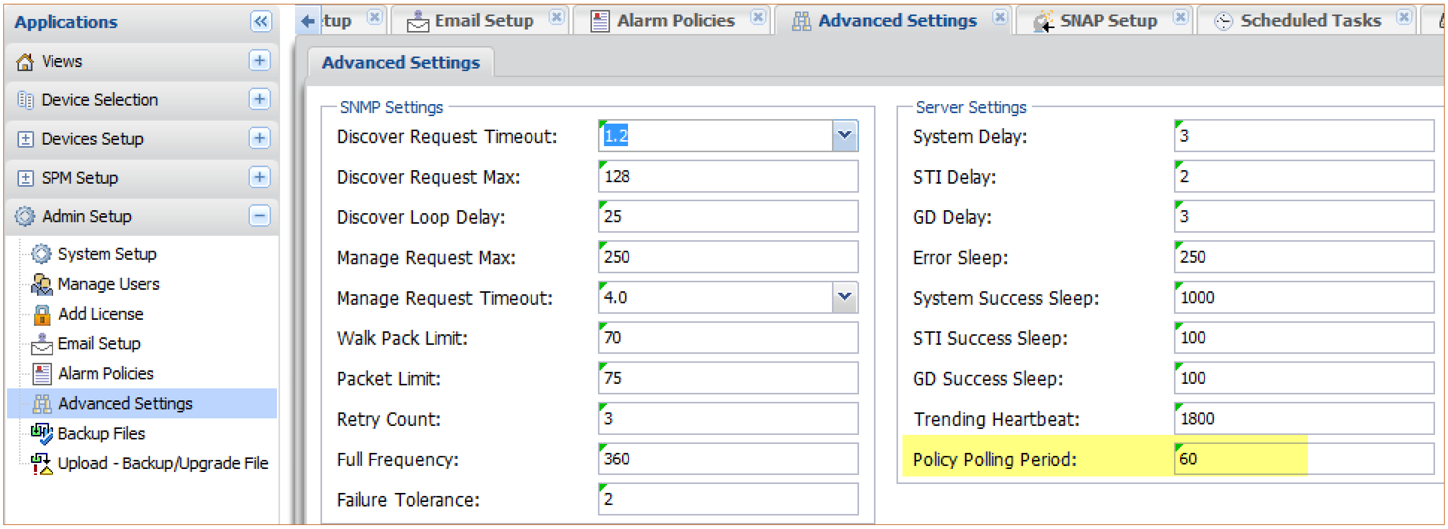
Name	Shortcut	Type
djones@ABC.com	Don	Email
Outlet Group Bldg 1		Email Group
sunil.adusumilli@servertech.c...	Sunil	Email

Step 2. Edit the parameters as desired and click Save. The cloned policy displays in the Alarms Policies list.

Setting the Policy Polling for Alarms

Once every minute, the Active Alarms feature of SPM checks associated alarm policies for alert rules and sends those that match the triggering criteria.

You can configure this 60-second default polling setting at **Admin Setup > Advanced Settings > Server Settings > Policy Polling Period.**



SNMP Settings

Discover Request Timeout: 1.2
Discover Request Max: 128
Discover Loop Delay: 25
Manage Request Max: 250
Manage Request Timeout: 4.0
Walk Pack Limit: 70
Packet Limit: 75
Retry Count: 3
Full Frequency: 360
Failure Tolerance: 2

Server Settings

System Delay: 3
STI Delay: 2
GD Delay: 3
Error Sleep: 250
System Success Sleep: 1000
STI Success Sleep: 100
GD Success Sleep: 100
Trending Heartbeat: 1800
Policy Polling Period: 60

Alarm Message Formats

Alert messages contain the following message formats: Text of the alerts: current reading, timestamp of reading, device name/IP, parent name, thresholds if available.

- last reading
- timestamp of alert creation
- timestamp of when alert is sent (factoring in delays and repeats here)
- parent name
- device name / IP
- thresholds if applicable
- there will be a hyper-link at the end of the message with type and id of the object that will be used to pass through a logon screen and take the user directly to the object with the alarm if used.
- SUBJECT format SPM(<SPM Name>) Policy(<Policy Name>) has (##) notifications
- BODY format (no thresholds) The <object> from <object name> for <sub object> reported <status message> and a reading of <reading value>.
  Alarm created on <created timestamp> with last update on <update timestamp>.
- BODY format (with thresholds; note that not all thresholds are present on all types.)

  The <object> from <object name> for <sub object> reported <status message> and a reading of <reading value>.
  Thresholds: low critical = <low critical>, low warning = <low warning>, high warning = <high warning>, high critical = <high critical>.

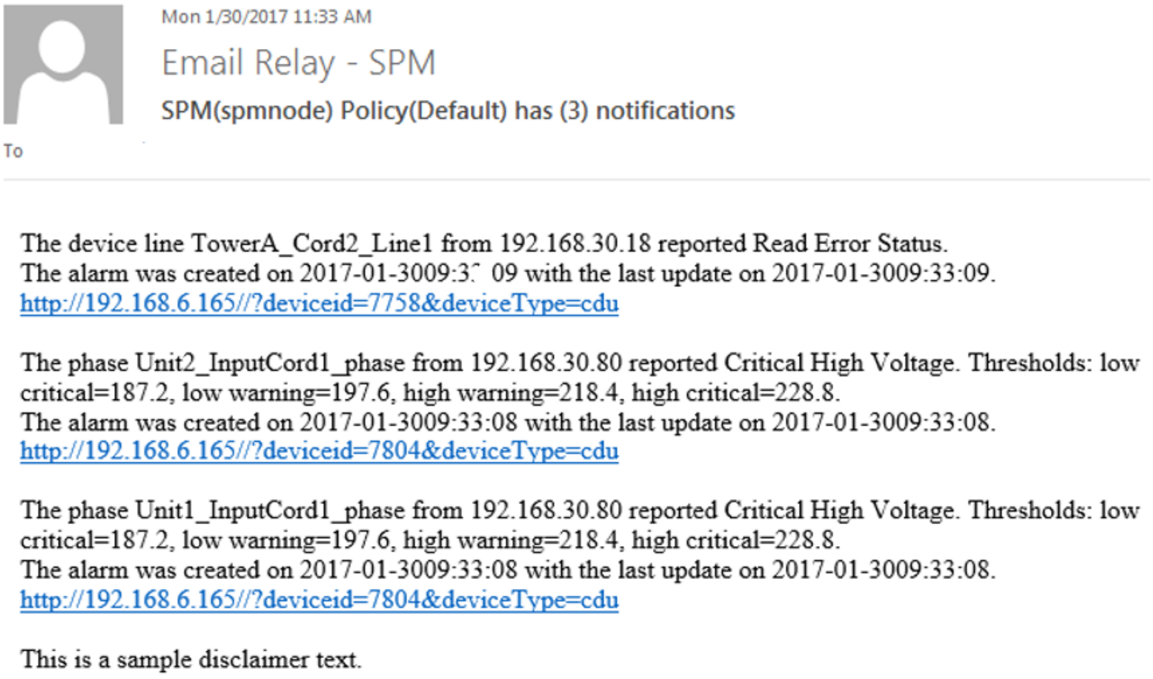
  The created/modified timestamps will only we present on email, added as a separate line after each alert.

  Alarm created on <created timestamp> with last update on <update timestamp>

  BODY has the following appended to the above message formats, but only in email.

  <link back to SPM and object>
  <disclaimer text>

Example of Alarm Message in Email



Mon 1/30/2017 11:33 AM

Email Relay - SPM

SPM(spmnode) Policy(Default) has (3) notifications

To

The device line TowerA_Cord2_Line1 from 192.168.30.18 reported Read Error Status.
The alarm was created on 2017-01-3009:3: 09 with the last update on 2017-01-3009:33:09.
http://192.168.6.165//?deviceid=7758&deviceType=cdu

The phase Unit2_InputCord1_phase from 192.168.30.80 reported Critical High Voltage. Thresholds: low critical=187.2, low warning=197.6, high warning=218.4, high critical=228.8.
The alarm was created on 2017-01-3009:33:08 with the last update on 2017-01-3009:33:08.
http://192.168.6.165//?deviceid=7804&deviceType=cdu

The phase Unit1_InputCord1_phase from 192.168.30.80 reported Critical High Voltage. Thresholds: low critical=187.2, low warning=197.6, high warning=218.4, high critical=228.8.
The alarm was created on 2017-01-3009:33:08 with the last update on 2017-01-3009:33:08.
http://192.168.6.165//?deviceid=7804&deviceType=cdu

This is a sample disclaimer text.

Contact Technical Support

Experience Server Technology's FREE Technical Support

Server Technology understands that there are often questions when installing and/or using a new product. Free Technical Support is provided from 8 a.m. to 5 p.m. PST, Monday through Friday. After-hours service is provided to ensure your requests are handled quickly no matter what time zone or country you are located in.

Server Technology, Inc.

1040 Sandhill Drive	Tel:	1-800-835-1515	Web:	www.servertech.com
Reno, Nevada 89521 USA	Fax:	775-284-2065	Email:	support@servertech.com

Server Technology, the Globe logo, Sentry, Switched CDU, CDU, PRO2, PIPS, POPS, PDU Power Pivot, and StartUp Stick are trademarks of Server Technology, Inc., registered in the US. EZip is a trademark of Server Technology.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Server Technology, Inc. disclaims any proprietary interest in trademarks and trade names other than its own.