

# AUTOMATE OPERATING SYSTEMS PATCHES AND SECURITY PATCHES USING AWS SSM

## KEY POINTS

### Important

Beginning December 22, 2022, Systems Manager provides support for *patch policies*, which are the new and recommended method for configuring your patching operations. Using a single patch policy configuration, you can define patching for all accounts in all Regions in your organization, for only the accounts and Regions you choose, or for a single account-Region pair. For more information, see [Using Quick Setup patch policies](#).

### Note

AWS doesn't test patches before making them available in Patch Manager. Also, Patch Manager doesn't support upgrading major versions of operating systems, such as Windows Server 2016 to Windows Server 2019, or SUSE Linux Enterprise Server (SLES) 12.0 to SLES 15.0.

For Linux-based operating system types that report a severity level for patches, Patch Manager uses the severity level reported by the software publisher for the update notice or individual patch. Patch Manager doesn't derive severity levels from third-party sources, such as the [Common Vulnerability Scoring System](#) (CVSS), or from metrics released by the [National Vulnerability Database](#) (NVD).

## Integrates With AWS Services

### Integrations

Patch Manager integrates with the following other AWS services:

- **AWS Identity and Access Management (IAM)** – Use IAM to control which users, groups, and roles have access to Patch Manager operations. For more information, see [How AWS Systems Manager works with IAM](#) and [Configure instance permissions required for Systems Manager](#).
- **AWS CloudTrail** – Use CloudTrail to record an auditable history of patching operation events initiated by users, roles, or groups. For more information, see [Logging AWS Systems Manager API calls with AWS CloudTrail](#).
- **AWS Security Hub** – Patch compliance data from Patch Manager can be sent to AWS Security Hub. Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status. It also monitors the patching status of your fleet. For more information, see [Integrating Patch Manager with AWS Security Hub](#).
- **AWS Config** – Set up recording in AWS Config to view Amazon EC2 instance management data in the Patch Manager Dashboard. For more information, see [Viewing patch Dashboard summaries](#).

## STEP 1 :- Visit AWS System Manager Dashboard.

The screenshot shows the AWS Systems Manager Patch Manager dashboard. On the left is a navigation sidebar with sections: 'AWS Systems Manager Manager', 'Quick Setup', 'Operations Management' (containing Explorer, OpsCenter, CloudWatch Dashboard, Incident Manager), 'Application Management' (containing Application Manager, AppConfig, Parameter Store), and 'Change Management' (containing Change Manager, Automation, Change Calendar, Maintenance Windows). The main content area has a dark header with 'Management & Governance' and 'AWS Systems Manager Patch Manager'. Below this, it says 'Manage patch compliance across the organization' and provides a brief description of Patch Manager. A 'Patch your instances' section on the right explains how to expedite patching and includes a 'Create patch policy' button and a 'Start with an overview' link. A 'How it works' section in the center shows three steps: 'Create patch policy', 'View dashboard', and 'View compliance reports'. On the far right, there are links for 'Use cases and blog posts' and 'More resources'.

## STEP 2 :- Patch Manager

The screenshot shows the 'Patch Manager' interface, specifically the 'Patch baselines' tab. At the top, there are buttons for 'Patch now' and 'Create patch policy'. Below this is a navigation bar with tabs: 'Dashboard', 'Compliance reporting', 'Patch baselines' (selected), 'Patches', and 'Settings'. The main content area is titled 'Patch baselines (17)' and includes a search bar and buttons for 'View details', 'Edit', 'Delete', and 'Create patch baseline'. A table lists the patch baselines:

	Baseline ID	Baseline name	Description	Operating system
<input type="radio"/>	<a href="#">pb-0cb0c4966f86b059b</a>	AWS-AlmaLinuxDefaultPatchBaseline	Default Patch Baseline for Alma Linux Provided by AWS.	AlmaLinux
<input type="radio"/>	<a href="#">pb-0c10e657807c7a700</a>	AWS-AmazonLinuxDefaultPatchBaseline	Default Patch Baseline for Amazon Linux Provided by AWS.	Amazon Linux
<input type="radio"/>	<a href="#">pb-0be8c61cde3be63f3</a>	AWS-AmazonLinux2DefaultPatchBaseline	Default Patch Baseline for Amazon Linux 2 Provided by AWS.	Amazon Linux 2
<input type="radio"/>	<a href="#">pb-0028ca011460d5eaf</a>	AWS-AmazonLinux2022DefaultPatchBaseline	Default Patch Baseline for Amazon Linux 2022 Provided by AWS.	Amazon Linux 2022
<input type="radio"/>	<a href="#">pb-05c9c9bf778d4c4d0</a>	AWS-AmazonLinux2023DefaultPatchBaseline	Default Patch Baseline for Amazon Linux 2023 Provided by AWS.	Amazon Linux 2023

### STEP 3 :- Creating Patch Baseline

## Create patch baseline

### Patch baseline details

Name

You can use letters, numbers, periods, dashes, and underscores in the name.

Description - *optional*

Operating system

Select the operating system you want to specify approval rules and patch exceptions for.

Amazon Linux

### Approval rules for operating systems

Create auto-approval rules to specify that certain types of operating system patches are approved automatically.

#### Operating system rule 1

Remove rule

Products

Select patches by product

Select products

AmazonLinux2018.03

Classification

Select patches by classification

Select classifications

Security

Bugfix

Severity

Select patches by severity

Select severities

Critical

Important

Auto-approval

Specify how to select updates for automatic approval

☒ Approve patches after a specified number of days

☐ Approve patches released up to a specific date

Specify the number of days

2

 days

Compliance reporting - *optional*

Specify the severity level to report for patches that match this rule.

Critical

Include nonsecurity updates

☐ Select this box to also install nonsecurity patches that meet the approval rules.

Add rule

9 remaining

Fi

## STEP 4 :- Creating Patch Policy.

AWS Systems Manager

Quick Setup

▼ Operations Management

▼ Application Management

▼ Change Management

▼ Node Management

▼ Shared Resources

Systems Manager > Quick Setup > Create configuration

Create patch policy

Patch your instances

This Quick Setup configuration type makes it easy to setup patch scanning and patch installation for your EC2 and on-premises instances, regardless of whether you want to do so across all instances in your AWS Organization or select instances within a specific account and Region. For more details about Patch Manager and Patch Policies, follow this link. [Learn more](#)

Configuration name

Amazon\_Linux\_Custom\_Patching

The configuration name can have up to 113 characters. Configuration names are case sensitive. Valid characters: A-Z, a-z, 0-9, \_ space, and - (hyphen)

Scanning and installation

Patch operation

Scans the targets and compares their installed patches against a list of approved patches in the patch baseline. Select to scan or to scan and install missing patches.

☐ Scan

☒ Scan and install

Scanning schedule

☒ Use recommended defaults

Patch Manager scans your nodes daily at 1:00 AM UTC.

☐ Custom scan schedule

Create a custom scanning schedule.

Installation schedule

☐ Use recommended defaults

Patch Manager will install patches once a week at 2:00 AM UTC on Sunday.

☒ Custom install schedule

Create a custom install schedule.

Installation frequency

Daily

Every day at 12:00 UTC

☒ Wait to install updates until first CRON interval.

☐ Reboot if needed

Reboot node if required after patch installation. Rebooting after each installation is recommended.

Patch baseline

Patch baselines include rules for auto-approving patches within days of their release, in addition to a list of approved and rejected patches. [Learn more](#)

☐ Use recommended defaults

The default patch baseline defined for each operating system supported by AWS.

☒ Custom patch baseline

Select a custom patch baseline. Custom patch baselines must be in the home AWS Region specified for Quick Setup (us-east-2) and can be up to 3,336 bytes.

▼ View or change baselines

Custom patch baselines must be in the home AWS Region specified for Quick Setup (us-east-2).

Operating system	Select baseline	Baseline ID
Alma Linux	AWS-AlmaLinuxDefaultPatchBaseline	pb-0c512885f94eceb9e
Amazon Linux	Amazon	pb-098993567f516cdfc
Amazon Linux 2	Q	pb-07e6d4e9bc703f2e3
Amazon Linux 2022	AWS-AmazonLinuxDefaultPatchBaseline	pb-0d02b7674ff76a48d
Amazon Linux 2023	Default Patch Baseline for Amazon Linux Provided by AWS.	
CentOS	Custom baselines	pb-0366438d3e092e1d3
Debian Server	Amazon	pb-0574b43a65ea646ed
macOS	AWS-CentOSDefaultPatchBaseline	pb-0d215380aec1af2f0
Oracle Linux	AWS-DebianDefaultPatchBaseline	pb-0f9cdf0b6da47181
Raspberry Pi OS	AWS-MacOSDefaultPatchBaseline	pb-0bf2738c5e3b55542
Red Hat Enterprise Linux (RHEL)	AWS-OracleLinuxDefaultPatchBaseline	pb-07335117835e9e63a
Rocky Linux	AWS-RaspbianDefaultPatchBaseline	pb-0e9c1ce8d831d57e0
SUSE Linux Enterprise Server (SLES)	AWS-RedHatDefaultPatchBaseline	pb-056dd3ed0db4e2121
Ubuntu Server	AWS-RockyLinuxDefaultPatchBaseline	pb-0123fdb36e334a3b2
Windows Server	AWS-SuseDefaultPatchBaseline	pb-052a2e04b3b354d69
	AWS-UbuntuDefaultPatchBaseline	pb-020d361a05defe4ed
	AWS-DefaultPatchBaseline	



## Patching log storage

### ☒ Write output to S3 bucket

Store patching operation logs in an Amazon S3 bucket. Patching operation output in the console is truncated after 48,000 characters.

#### S3 URI

Select the S3 bucket for storing patching logs. Only buckets in the current Region can be selected.

[View](#)[Browse S3](#)

## Targets

Choose the nodes that the patch policy is deployed to.

Choose between deploying to the current Region or a custom set of Regions.

### ☐ Current Region

Deploy configuration to the current Region.

### ☒ Choose Regions

Choose the Regions you want to deploy this configuration to.

#### Target Regions

Choose the Regions you want to deploy this patch policy to.

##### ☐ All Regions

- ☒ us-east-1 (N. Virginia)
- ☒ us-east-2 (Ohio)
- ☐ us-west-1 (N. California)
- ☐ us-west-2 (Oregon)
- ☐ sa-east-1 (Sao Paulo)
- ☐ eu-central-1 (Frankfurt)
- ☐ eu-west-1 (Ireland)
- ☐ eu-west-2 (London)
- ☐ eu-west-3 (Paris)
- ☐ eu-north-1 (Stockholm)
- ☐ ca-central-1 (Central)
- ☐ ap-south-1 (Mumbai)
- ☐ ap-northeast-2 (Seoul)
- ☐ ap-southeast-1 (Singapore)
- ☐ ap-southeast-2 (Sydney)
- ☐ ap-northeast-1 (Tokyo)

Choose how you want to target instances

### ☒ All managed nodes

Deploy the patch policy to all managed nodes in the current account.

### ☐ Specify node tag

Specify a tag key-value pair to select nodes in your account.

## Rate control

Specify the concurrency rate and error rate to run your patch policy with.

### Concurrency

Provide the number or percentage of nodes to run the patch policy on at the same time.

[Percentage of nodes](#)

The percent of nodes must be between 1 and 100.

### Error threshold

Provide the number or percentage of nodes to permit errors on before the patch policy fails.

[Percentage of nodes](#)

The percent of nodes must be between 0 and 100.

## Instance profile options

☒ Add required IAM policies to existing instance profiles attached to your instances.



### Enabling this option changes default behavior

By default, Quick Setup creates IAM policies and instance profiles with the permissions needed for the configuration you choose. The instance profiles created by Quick Setup are then attached only to instances that do not have an instance profile attached. If you enable this option, Quick Setup will also add IAM policies to instances with instance profiles attached.

The following policies will be attached:

- AmazonSSMMangedInstanceCore
- aws-quicksetup-patchpolicy-baselineoverrides-s3