Patch Management

Getting Started Guide

November 17, 2023

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About this Guide

Welcome to Qualys Patch Management! We'll help you get acquainted with the Qualys solutions for patching your systems using the Qualys Cloud Security Platform.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access online support information at www.qualys.com/support/.

Patch Management Overview

Qualys Patch Management provides a comprehensive solution to manage vulnerabilities in your system and deploy patches to secure these vulnerabilities as well as keep your assets upgraded. The Qualys Vulnerability Management, Detection, and Response (VMDR) module enables you to discover, assess, prioritize, and identify patches for critical vulnerabilities. The Patch Management module helps you save time and effort by automating patch management on Windows, Linux, and Mac assets using a single patch management application. It provides instant visibility on patches available for your asset and allows you to automatically deploy new patches as and when they are available.

- The Windows Cloud Agent downloads the required patches from external sources. However, patches that require authentication cannot be downloaded by the agent. You can manually download and install such patches on the assets. Qualys Patch Management will then identify these patches as installed.

- The Linux Cloud Agent access the patches from the YUM repository and deploys the patches to the Linux assets in Patch Management.

- The same Qualys Cloud Mac Agent that is currently used for vulnerability management can now be used to detect and patch Mac OS patches as well as Mac 3rd party application patches. You can just enable Patch management on MAC agents in a single click, and you do not need to go through the never-ending approval process of installing one more agent. For more information, see this blog.

To experience MacOS support, contact your Technical Account Manager (TAM) to get the compatible Mac agent binary 4.25 or later for x64, x86_64, and binary 4.26 or later for arm64 architecture.

Qualys Subscription and Modules required

You would require Patch Management (PM) module enabled for your account.

System support

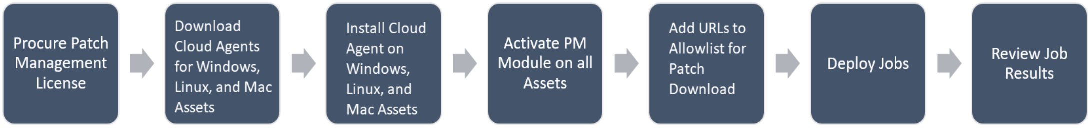
Patch Management supports installing patches on Windows, Linux, and Mac systems.

Refer to the Qualys Patch Management Supported Product Versions guide to know more about:

- Supported Windows Products
- Supported Linux Operating Systems
- Supported Mac Products

Patch Management Process Workflow

Refer to the following workflow to get started with Patch Management.


Procure Patch Management License
Download Cloud Agents for Windows, Linux, and Mac Assets
Install Cloud Agent on Windows, Linux, and Mac Assets
Activate PM Module on all Assets
Add URLs to Allowlist for Patch Download
Deploy Jobs
Review Job Results

Agent Installation and Configuration

Installing Cloud Agent for PM

Adding URLs to Allowlist for Patch Download

Creating and enabling PM in a CA Configuration Profile

User Roles and Permissions for Patch Management

Note: It's an important step to use tags to grant access to assets. Refer to the 'How are tags used to grant access to assets?' section from User Roles and Permissions for Patch Management.

Deploy Patches

Creating Assessment profiles for Windows and Mac Assets

Reviewing Missing and Installed Windows Patches

Reviewing Missing and Installing Linux Patches

Reviewing Missing and Installed Mac Patches

Deploying Patch Jobs on Assets

- Managing Patch Jobs for Windows Assets

- Managing Patch Jobs for Linux Assets

- Managing Patch Jobs for Mac Assets

Reviewing Job Results

Rollback Windows Patches

Rolling Back Patches from Windows Assets

Reviewing Job Results

Patch Management Features

Qualys Patch Management provides a comprehensive solution for patching assets with the following features:

Deploy Patches for Windows, Linux and Mac Assets

You can deploy patch jobs for Windows, Linux, and Mac assets. Ensure that you have installed Cloud Agent on all assets on which you want to deploy patch jobs.

See the following User Scenarios:

User Scenario: Deploying security patch jobs for Microsoft

User Scenario: Deploying security patches for RHEL assets

User scenario: Installing critical patches for Chrome and Internet Explorer

Schedule Run-Once or Recurring Jobs

You can schedule Run-Once and Recurring jobs. Run-Once jobs are the default type of jobs for Patching. You can schedule these jobs for Windows, Linux and Mac assets:

- To run jobs immediately after they are enabled.

- To run jobs once or on a recurring basis.

- To run jobs in the future once or on a recurring basis.

Clone and Edit Windows, Linux, and Mac Jobs

You can clone a patch job, which lets you quickly copy an existing job and create a new one from it with minimal edits. Creating a job in less time means you can promptly patch your mission-critical assets to mitigate the vulnerabilities, which reduces the risk of attack.

View Patch Details

You can view the Windows, Linux, and Mac patch details, such as Patch title, Patch Category, Vendor Severity, and Patch Status.

View Job Details

You can view the job details from the **Jobs** tab. You can see the list of patch jobs for Windows, Linux, and Mac. You can see all the jobs created in your subscription, but you can view or edit only those jobs you have created, or you are the Co-Author for them. If you are a Co-author of a respective job, you can edit the job only if you have edit permission. You can see the job's status on the Jobs page, such as (Enabled, Disabled, and Assets Responded), name, owner, and schedule. In addition to these details, you can also see the total number of patches, assets, and tags added to the job, if any.

View Asset Details

You can view the asset details for all assets in your account for which you activated Patch Management from the Cloud Agent module.

- You can see the missing and installed patches for all the successfully scanned Windows and Mac assets

- You can see only missing patches for all the successfully scanned Linux assets.

- You can review missing and installed patches for Windows, Linux, and Mac assets.

- You can use QQL to automate patch selection for Windows and Linux deployment jobs.

Generate Reports

You can generate the following reports from Patch Management. A full or trial Patch Management license is required to generate the reports.

- Patch Reports for Windows and Linux Assets

- Job Progress Reports

- Aggregated Job Progress Report - Windows

- Patch Insights Report

Roll Back Patches from Windows Assets

You can roll back the patches from Windows assets by using selected tags for assets contained in your scope. When you select an asset tag, corresponding child tags get automatically selected.

Additional information:

User Scenario: Rolling back an older version of Internet Explorer browser

Remove Deprecated Patches from the Job

Sometimes, the already published patches are deprecated by the vendor due to various reasons, such as performance issues with the given fix, vulnerability, and so on. Patch Management does not deploy such deprecated patches even if a deprecated patch is already associated with a job. Another aspect is to ensure that no discrepancy is caused in the number of patches applied on an asset as a part of a deployment job. To ensure this, you must remove the deprecated patches from the job.

Create Custom Dashboards and Widgets

You can create custom dashboard and widgets for Windows, Linux, and Mac assets. For more information, see the *Customizable Dynamic Dashboards* section from Get Started with Patch Management topic and Patch Management Widgets.

Enable Vendor Acquired Windows Patch for Windows Jobs

If you are a Patch Manager, Patch User, or Patch Security role user, you can enable, add, and edit vendor-acquired patches to Windows deployment jobs.

Patch from VMDR

Based on the VMDR Prioritization report shown in the VMDR application, you can identify the vulnerabilities that need to be remediated first for Windows, Linux, and Mac assets. By clicking Patch Now from VMDR, you can initiate the process of patching the vulnerabilities.

View Aggregated Jobs Progress

You can view the aggregated job progress for multiple jobs in one place. With the help of aggregated job progress insights, you can identify whether patches that are part of single or multiple jobs are installed or failed for the asset.

Additional Resources

Using Tags to Grant Access to Assets

Note: Refer to the ‘How are tags used to grant access to assets?’ section from the User Roles and Permissions for Patch Management topic.

An asset tag is a tag assigned to one or more assets. Tag scopes define what assets the user can view when creating a job or when the user goes to the Assets tab in patch management. Assigning a tag to an asset enables you to grant users access to that asset by assigning the same tag to the user's scope.

Best Practices for Qualys Patch Management

The best practices facilitate effectively deploying patches on your assets. By effective patch deployment, we mean that remediating your assets from vulnerabilities is achieved by running optimum patch jobs with a lesser number of reboots and by avoiding hindrance in the end user’s day-to-day work.

Fallback to free version

Patch Management will revert to the Free version after your Trial or Full subscription expires. Existing scan intervals of less than 24 hours will get converted to intervals of 24 hours. Your existing jobs will be disabled and you can re-enable them once you renew your subscription.

The free version allows you to create assessment profiles with a minimum scan interval of 24 hours and see a list of missing and installed patches on the assets in your environment. It doesn’t allow creating deployment/rollback jobs.

User Scenarios

User Scenario: Deploying security patch jobs for Microsoft

Microsoft releases crucial security patches on a regular basis. To automate the job deployment for these patches, you can create a job to run on the 2nd Tuesday of every month.

To automate the patch installation, create a monthly recurring deployment job with the following parameters:

1. Navigate to **Jobs** > **Windows** > **Create Job**, and click **Deployment Job**.

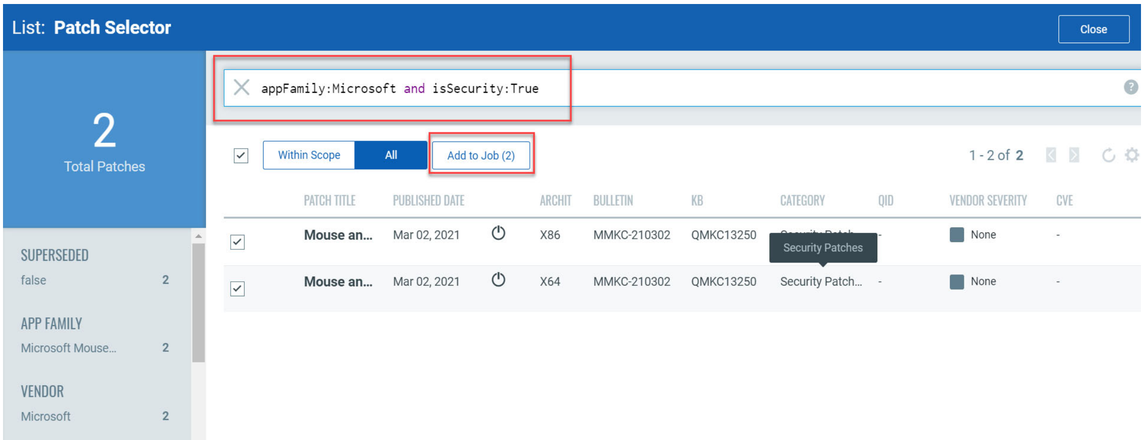
2. Enter the job title as ***Microsoft Security Patches*** and click **Next**.

3. Select assets or asset tags on which you want to apply the patches.

4. *(Optional)* Select **Add Exclusion Asset Tags** to exclude the assets from the deployment job that have **All/Any** of the selected asset tags.

5. To select patches to apply to the assets, choose the **Select Patch** option, and then click the **Take me to patch selector** link to select patches.

6. On the Patch Selector page, in the search query, enter **`appfamily:windows and isSecurity: True`** and select the patches from the search results.



```
appFamily:Microsoft and isSecurity:True
```

2
Total Patches

SUPERSEDED	
false	2
APP FAMILY	
Microsoft Mouse...	2
VENDOR	
Microsoft	2

	PATCH TITLE	PUBLISHED DATE		ARCHIT	BULLETIN	KB	CATEGORY	QID	VENDOR SEVERITY	CVE
☑	Mouse an...	Mar 02, 2021	⏻	X86	MMKC-210302	QMKC13250	Security Patches	-	None	-
☑	Mouse an...	Mar 02, 2021	⏻	X64	MMKC-210302	QMKC13250	Security Patch...	-	None	-

Note: You can add maximum 2000 patches to a single job.

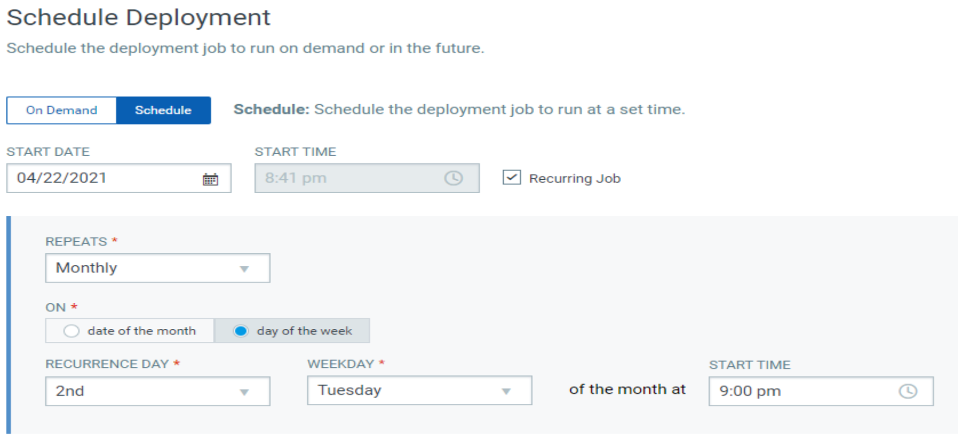
7. Click **Add to Job** and then click **Close**.

8. On the Select Patches page, click **Next**.

9. On the Schedule Deployment page, click **Schedule**.

10. Select the start date and time, and select the **Recurring Job**.

11. Set **Repeats** as ***Monthly***, select **day of a week**, and ***2nd Tuesday*** of the month at ***9:00 PM***.



Schedule Deployment

Schedule the deployment job to run on demand or in the future.

Schedule: Schedule the deployment job to run at a set time.

START DATE: 04/22/2021

START TIME: 8:41 pm

☑ Recurring Job

REPEATS *: Monthly

ON *: ○ date of the month ● day of the week

RECURRENCE DAY *: 2nd

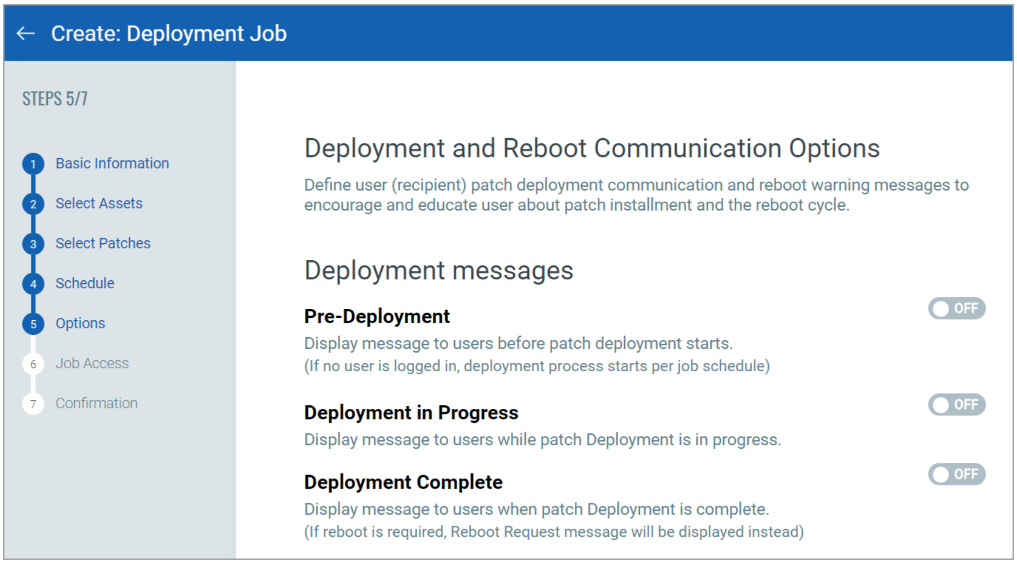
WEEKDAY *: Tuesday

of the month at

START TIME: 9:00 pm

12. *(Optional)* Set the Patching window if you want to restrict the agent to start the job within the specified patch window (e.g., start time + 6 hours). The job gets timed out if it does not start within this window.

13. Based on your preference, configure how to notify the users about the patch deployment. Configure the pre-deployment messages, deferring the patch deployment certain number of times.



Deployment and Reboot Communication Options

Define user (recipient) patch deployment communication and reboot warning messages to encourage and educate user about patch installment and the reboot cycle.

Deployment messages

Pre-Deployment OFF

Display message to users before patch deployment starts.
(If no user is logged in, deployment process starts per job schedule)

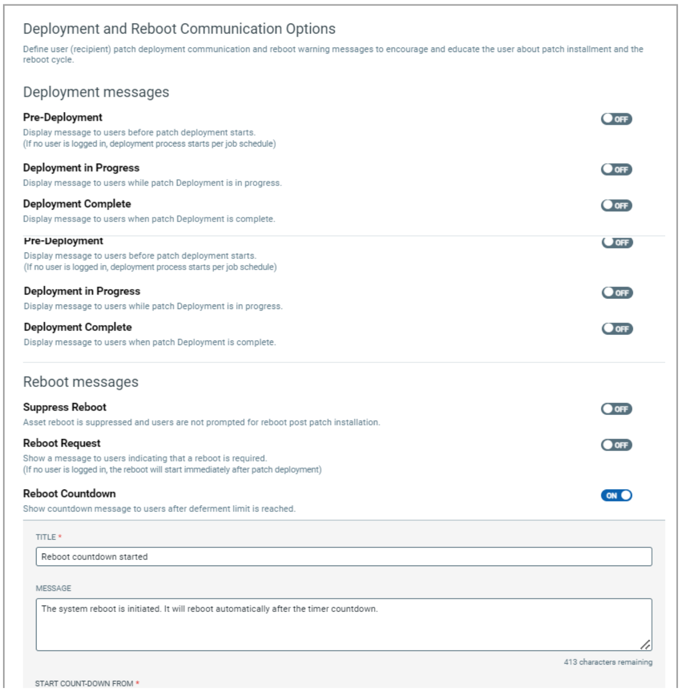
Deployment in Progress OFF

Display message to users while patch Deployment is in progress.

Deployment Complete OFF

Display message to users when patch Deployment is complete.
(If reboot is required, Reboot Request message will be displayed instead)

We recommend that you fill out both the message and description fields for these options.



Deployment and Reboot Communication Options

Define user (recipient) patch deployment communication and reboot warning messages to encourage and educate the user about patch installment and the reboot cycle.

Deployment messages

Pre-Deployment OFF
Display message to users before patch deployment starts.
(If no user is logged in, deployment process starts per job schedule)

Deployment in Progress OFF
Display message to users while patch Deployment is in progress.

Deployment Complete OFF
Display message to users when patch Deployment is complete.

Pre-Deployment OFF
Display message to users before patch deployment starts.
(If no user is logged in, deployment process starts per job schedule)

Deployment in Progress OFF
Display message to users while patch Deployment is in progress.

Deployment Complete OFF
Display message to users when patch Deployment is complete.

Reboot messages

Suppress Reboot OFF
Asset reboot is suppressed and users are not prompted for reboot post patch installation.

Reboot Request OFF
Show a message to users indicating that a reboot is required.
(If no user is logged in, the reboot will start immediately after patch deployment)

Reboot Countdown ON
Show countdown message to users after deferment limit is reached.

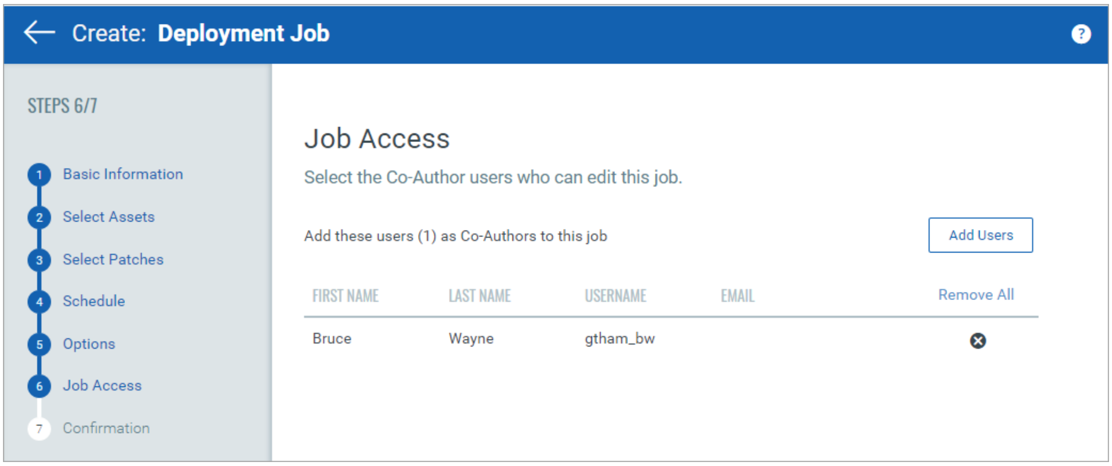
TITLE *
Reboot countdown started

MESSAGE
The system reboot is initiated. It will reboot automatically after the timer countdown.

413 characters remaining

START COUNT-DOWN FROM *

14. Finally based on the permissions assigned to other users, choose Co-Authors who can edit this job.



Job Access

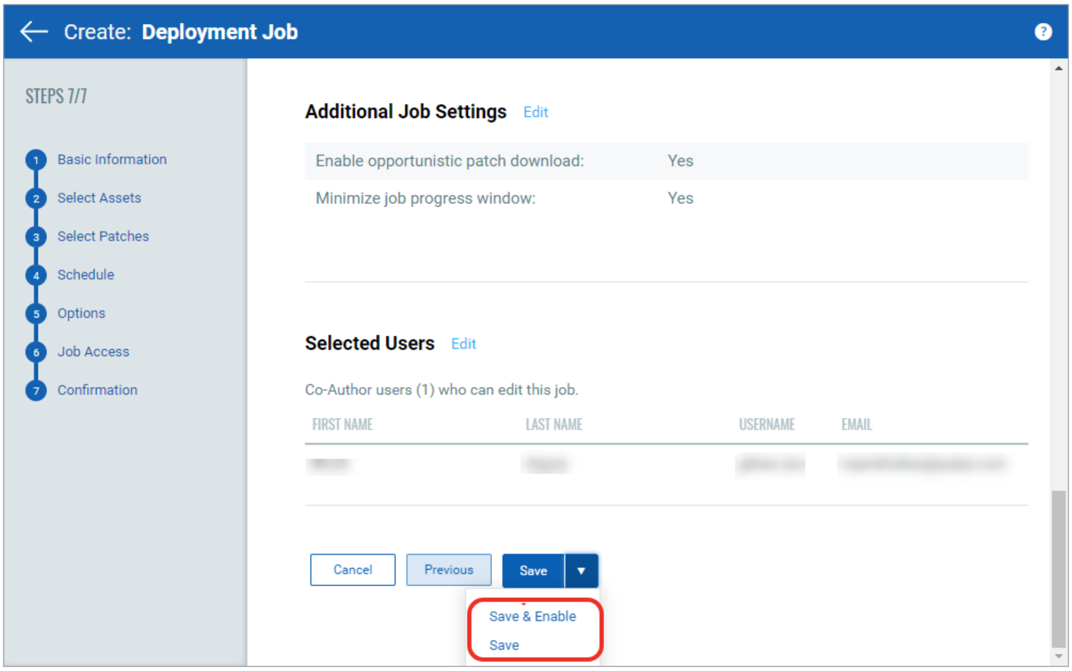
Select the Co-Author users who can edit this job.

Add these users (1) as Co-Authors to this job

FIRST NAME	LAST NAME	USERNAME	EMAIL
Bruce	Wayne	gtham_bw	

15. Next, review the configuration.

Job can either be created in ENABLED state by using the **Save & Enable** option or in DISABLED state by using the default **Save** button.



Additional Job Settings

Enable opportunistic patch download:	Yes
Minimize job progress window:	Yes

Selected Users

Co-Author users (1) who can edit this job.

FIRST NAME	LAST NAME	USERNAME	EMAIL
[redacted]	[redacted]	[redacted]	[redacted]

Note: The Patch Manager user can change the job status (enable/disable), delete and edit the job.

User Scenario: Deploying security patches for RHEL assets

RedHat releases security patches on a frequent basis. To automate the patch installation, create a deployment job with the following parameters:

1. Navigate to **Jobs** > **Linux** > **Create Job**.

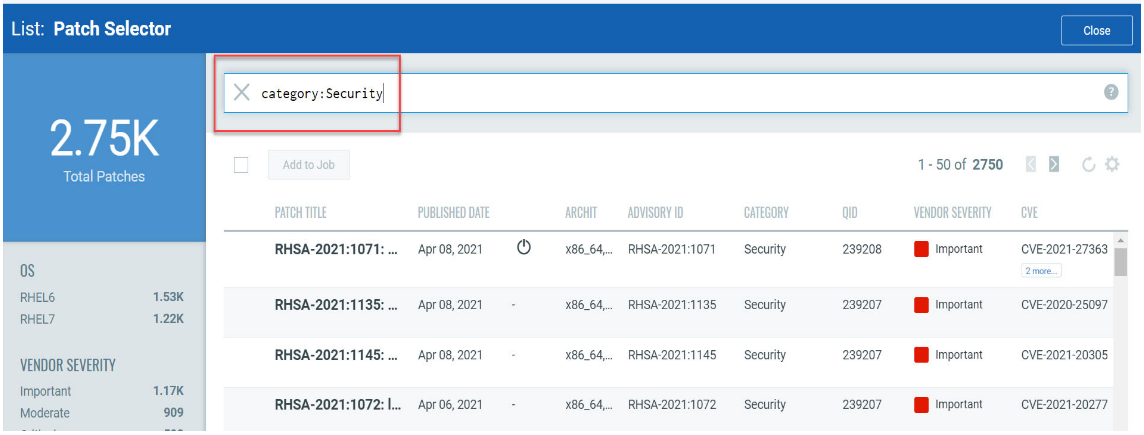
2. Enter the job title as ***RHEL Security Patches*** and click **Next**.

3. Select assets or asset tags on which you want to apply the patches.

4. *(Optional)* Select **Add Exclusion Asset Tags** to exclude the assets from the deployment job that have **All/Any** of the selected asset tags.

5. To select patches to apply to the assets, choose the **Select Patch** option and then click **Take me to patch selector** link to select patches.

6. On the Patch Selector page, in the search query, enter **`category: security`** and select the patches.



List: **Patch Selector**

`category:Security`

2.75K
Total Patches

OS

RHEL6	1.53K
RHEL7	1.22K

VENDOR SEVERITY

Important	1.17K
Moderate	909

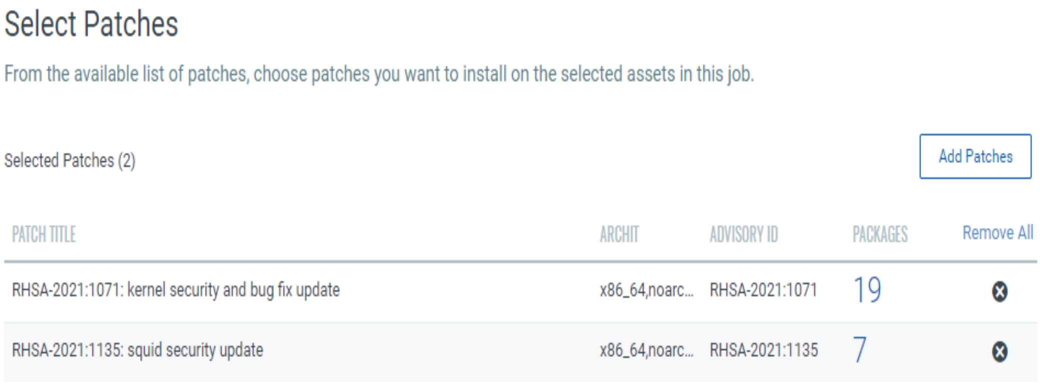
1 - 50 of **2750**

PATCH TITLE	PUBLISHED DATE		ARCHIT	ADVISORY ID	CATEGORY	QID	VENDOR SEVERITY	CVE
RHSA-2021:1071: ...	Apr 08, 2021	⏻	x86_64,...	RHSA-2021:1071	Security	239208	🟥 Important	CVE-2021-27363 2 more...
RHSA-2021:1135: ...	Apr 08, 2021	-	x86_64,...	RHSA-2021:1135	Security	239207	🟥 Important	CVE-2020-25097
RHSA-2021:1145: ...	Apr 08, 2021	-	x86_64,...	RHSA-2021:1145	Security	239207	🟥 Important	CVE-2021-20305
RHSA-2021:1072: l...	Apr 06, 2021	-	x86_64,...	RHSA-2021:1072	Security	239207	🟥 Important	CVE-2021-20277

Note: You can add maximum 2000 patches to a single job.

7. Click **Add to Job** and then click **Close**.

8. On the Select Patches page, click **Next**.



Select Patches

From the available list of patches, choose patches you want to install on the selected assets in this job.

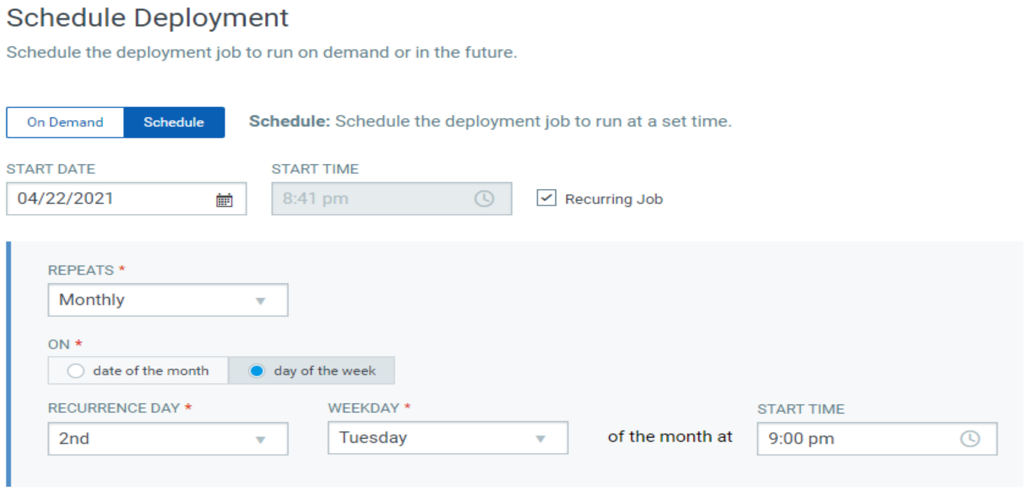
Selected Patches (2)

PATCH TITLE	ARCHIT	ADVISORY ID	PACKAGES	Remove All
RHSA-2021:1071: kernel security and bug fix update	x86_64,noarc...	RHSA-2021:1071	19	⊗
RHSA-2021:1135: squid security update	x86_64,noarc...	RHSA-2021:1135	7	⊗

9. On the Schedule Deployment page, click **Schedule**.

10. Select the start date and time, and select **Recurring Job**.

11. Set **Repeats** as ***Monthly***, select **day of a week**, and ***1st Monday*** of the month at ***9:00 PM***.



Schedule Deployment

Schedule the deployment job to run on demand or in the future.

Schedule: Schedule the deployment job to run at a set time.

START DATE: 04/22/2021

START TIME: 8:41 pm

☑ Recurring Job

REPEATS *: Monthly

ON *: ○ date of the month ● day of the week

RECURRENCE DAY *: 2nd

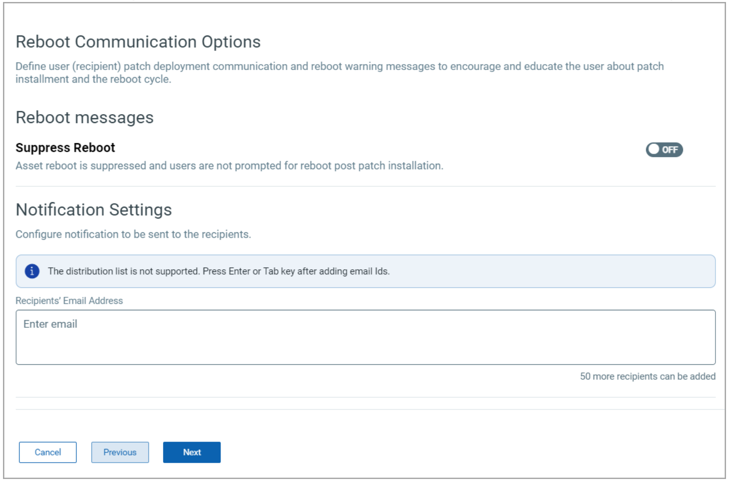
WEEKDAY *: Tuesday

of the month at

START TIME: 9:00 pm

12. *(Optional)* Set the Patching window if you want to restrict the agent to complete the job within the specified patch window (e.g., start time + 6 hours). The job will timed out if it does not complete within this window.

13. Based on your preference, configure reboot communication options. Enable the Continue patching even after a package failure occurs for a patch option so that if one of the package in the patch fails to install, other packages are installed successfully.



Reboot Communication Options

Define user (recipient) patch deployment communication and reboot warning messages to encourage and educate the user about patch installment and the reboot cycle.

Reboot messages

Suppress Reboot OFF

Asset reboot is suppressed and users are not prompted for reboot post patch installation.

Notification Settings

Configure notification to be sent to the recipients.

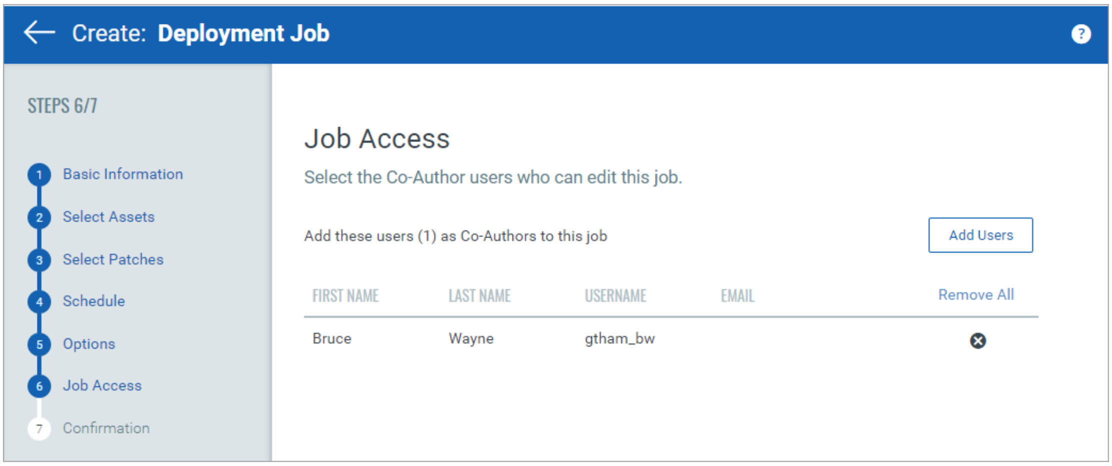
The distribution list is not supported. Press Enter or Tab key after adding email Ids.

Recipients' Email Address

Enter email

50 more recipients can be added

14. Finally based on the permissions assigned to other users, choose Co-Authors who can edit this job.



Job Access

Select the Co-Author users who can edit this job.

Add these users (1) as Co-Authors to this job

FIRST NAME	LAST NAME	USERNAME	EMAIL
Bruce	Wayne	gtham_bw	

15. Next, review the configuration.

Job can either be created in ENABLED state by using the **Save & Enable** option or in DISABLED state by using the default **Save** button.

Note: The Patch Manager super user can change the job status (enable/disable), delete and edit the job.

User Scenario: Rolling back an older version of Internet Explorer browser

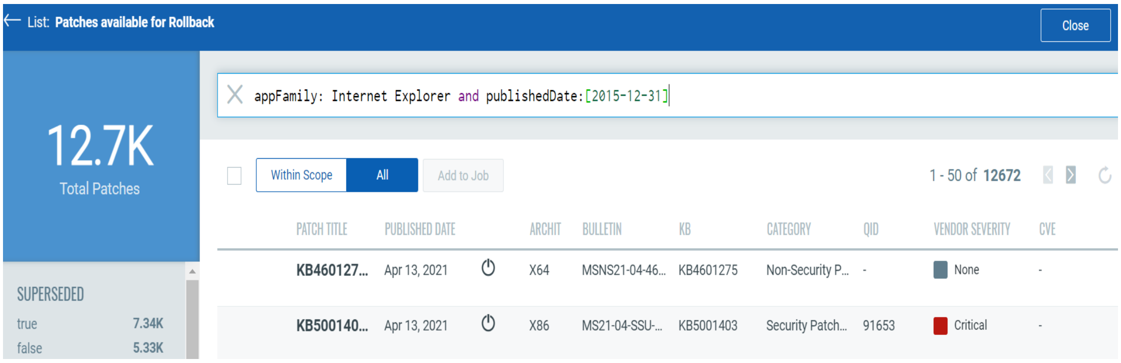
Using an older version of the web browser can cause security issues. You can roll back an older version of Internet Explorer browser that might have released before 2016.

1. Navigate to **Jobs** > **Windows** > **Create Job**, and click **Rollback Job**.

2. Provide a job title, and then select assets or asset tags from which you want to roll back the patches.

3. Select patches to roll back from the assets. Use the patch selector link to select patches.

4. On the Patches available for Rollback page, in the search query, enter **`appfamily: Internet Explorer and publishedDate: [2015-12-31]`**.



List: **Patches available for Rollback**

Close

```
appFamily: Internet Explorer and publishedDate:[2015-12-31]
```

12.7K
Total Patches

SUPERSEDED

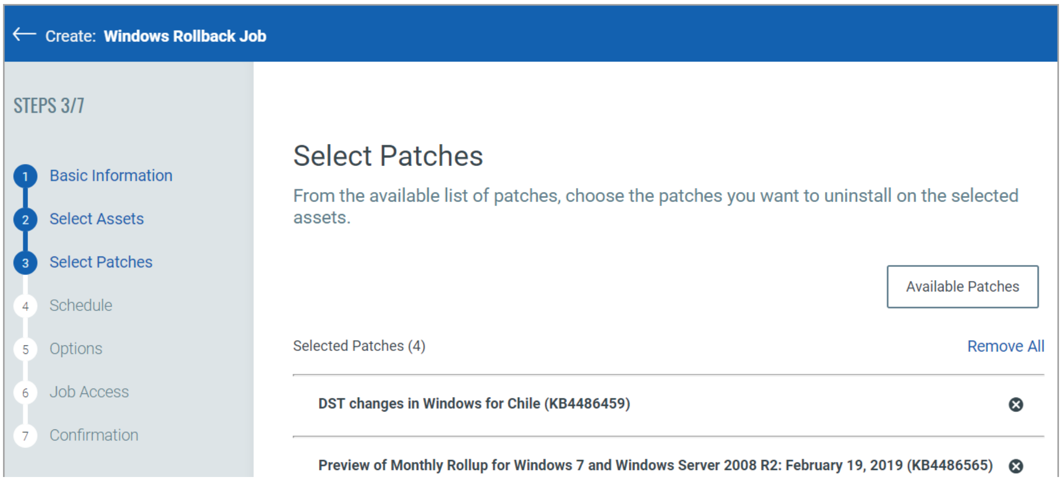
true	7.34K
false	5.33K

Within Scope | All | Add to Job

1 - 50 of **12672**

PATCH TITLE	PUBLISHED DATE		ARCHIT	BULLETIN	KB	CATEGORY	QID	VENDOR SEVERITY	CVE
KB460127...	Apr 13, 2021	⏻	X64	MSNS21-04-46...	KB4601275	Non-Security P...	-	■ None	-
KB500140...	Apr 13, 2021	⏻	X86	MS21-04-SSU-...	KB5001403	Security Patch...	91653	🟥 Critical	-

Note: You can add maximum 2000 patches to a single job.



Create: **Windows Rollback Job**

STEPS 3/7

1 Basic Information
2 Select Assets
3 Select Patches
4 Schedule
5 Options
6 Job Access
7 Confirmation

Select Patches

From the available list of patches, choose the patches you want to uninstall on the selected assets.

Available Patches

Selected Patches (4) Remove All

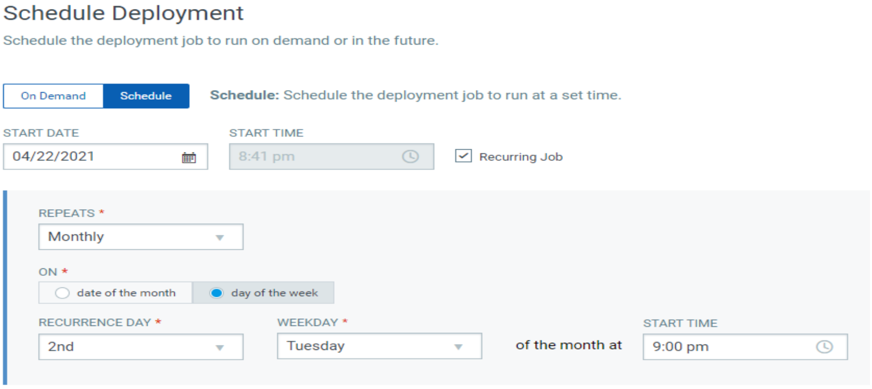
DST changes in Windows for Chile (KB4486459) ⊗

Preview of Monthly Rollup for Windows 7 and Windows Server 2008 R2: February 19, 2019 (KB4486565) ⊗

5. Click **Add to Job** and then click **Close**.

6. On the Select Patches page, click **Next**.

7. On the Schedule Deployment page, click **On Demand**.



Schedule Deployment

Schedule the deployment job to run on demand or in the future.

On Demand | Schedule

Schedule: Schedule the deployment job to run at a set time.

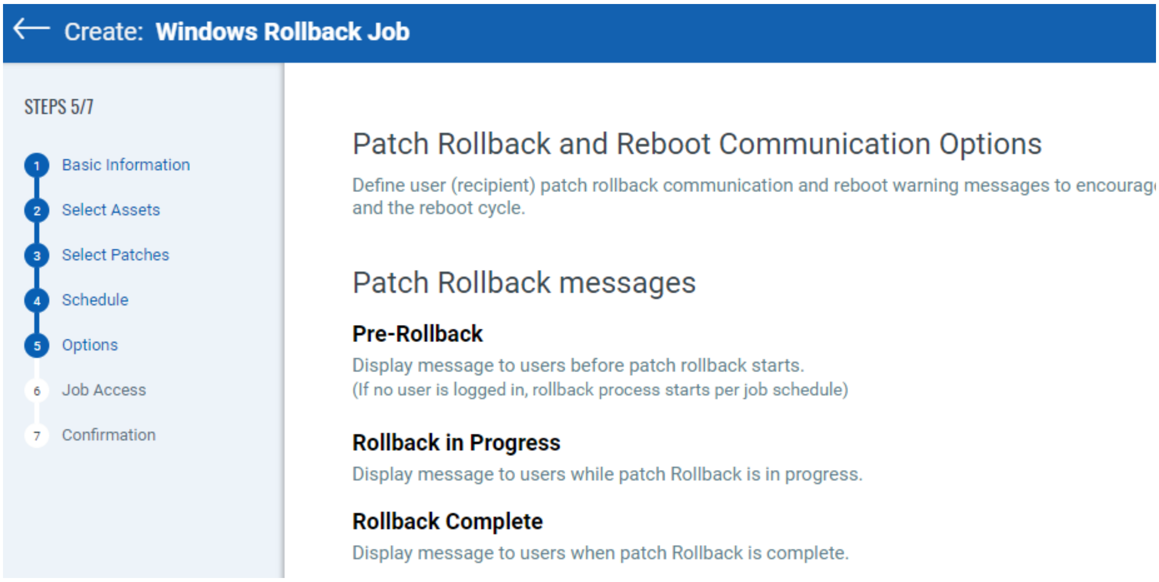
START DATE: 04/22/2021
START TIME: 8:41 pm
☑ Recurring Job

REPEATS *: Monthly

ON *: ○ date of the month ● day of the week

RECURRENCE DAY *: 2nd
WEEKDAY *: Tuesday
of the month at
START TIME: 9:00 pm

8. Based on your preference, configure how to notify the users about the patch deployment. Configure the pre-deployment messages, deferring the patch deployment certain number of times.



Patch Rollback and Reboot Communication Options

Define user (recipient) patch rollback communication and reboot warning messages to encourag and the reboot cycle.

Patch Rollback messages

Pre-Rollback

Display message to users before patch rollback starts.
(If no user is logged in, rollback process starts per job schedule)

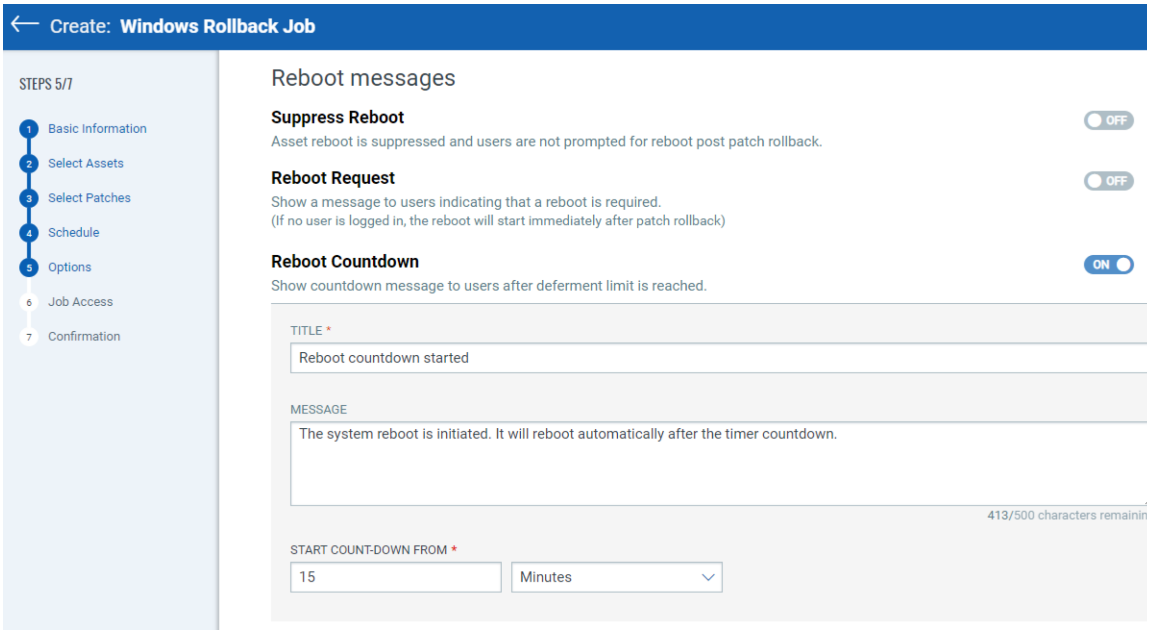
Rollback in Progress

Display message to users while patch Rollback is in progress.

Rollback Complete

Display message to users when patch Rollback is complete.

9. Finally, you can prompt the user or choose suppress reboot when asset reboot is required post patch installation.



Reboot messages

Suppress Reboot OFF

Asset reboot is suppressed and users are not prompted for reboot post patch rollback.

Reboot Request OFF

Show a message to users indicating that a reboot is required.
(If no user is logged in, the reboot will start immediately after patch rollback)

Reboot Countdown ON

Show countdown message to users after deferment limit is reached.

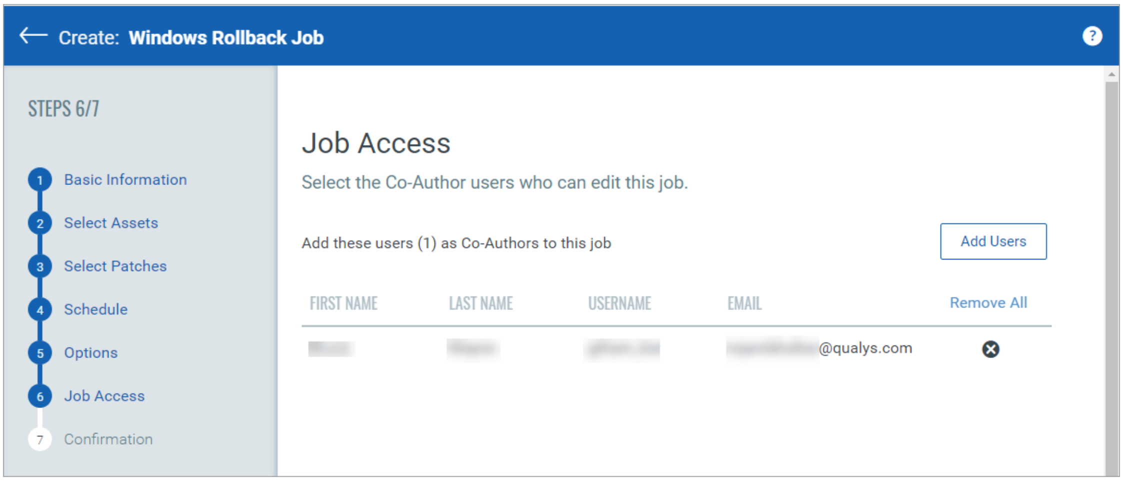
TITLE *
Reboot countdown started

MESSAGE
The system reboot is initiated. It will reboot automatically after the timer countdown.

413/500 characters remainin

START COUNT-DOWN FROM *
15 Minutes

10. Finally based on the permissions assigned to other users, choose Co-Authors who can edit this job.



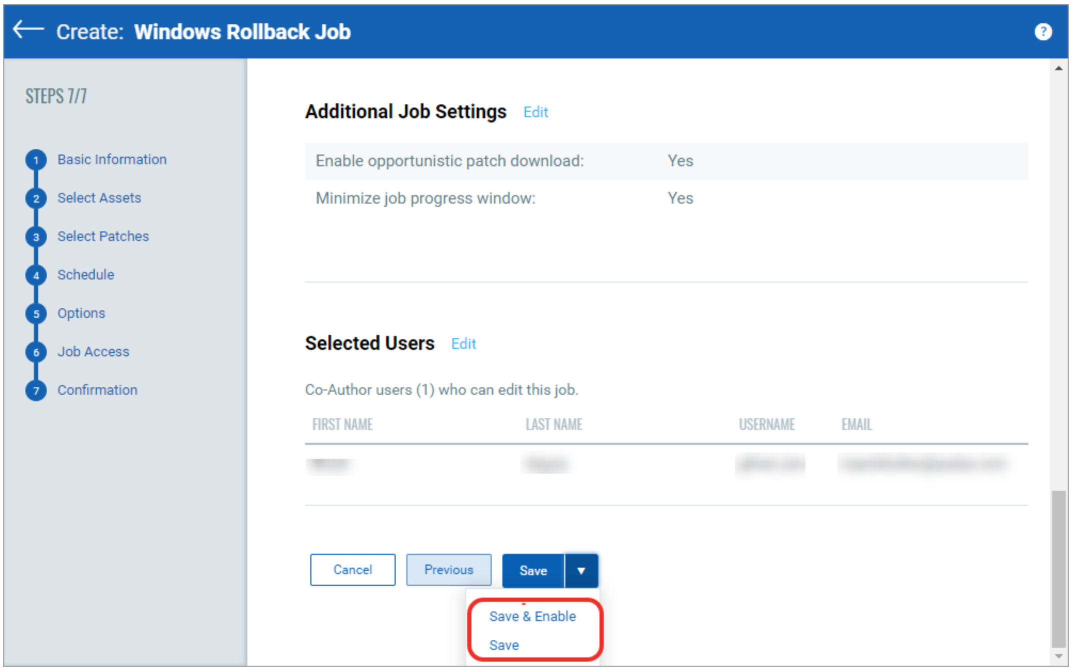
Job Access

Select the Co-Author users who can edit this job.

Add these users (1) as Co-Authors to this job

FIRST NAME	LAST NAME	USERNAME	EMAIL
[redacted]	[redacted]	[redacted]	[redacted]@qualys.com

11. Next, review the configuration. Job can either be created in ENABLED state by using the **Save & Enable** option or in DISABLED state by using the default **Save** button.



Additional Job Settings

Enable opportunistic patch download: Yes

Minimize job progress window: Yes

Selected Users

Co-Author users (1) who can edit this job.

FIRST NAME	LAST NAME	USERNAME	EMAIL
[redacted]	[redacted]	[redacted]	[redacted]

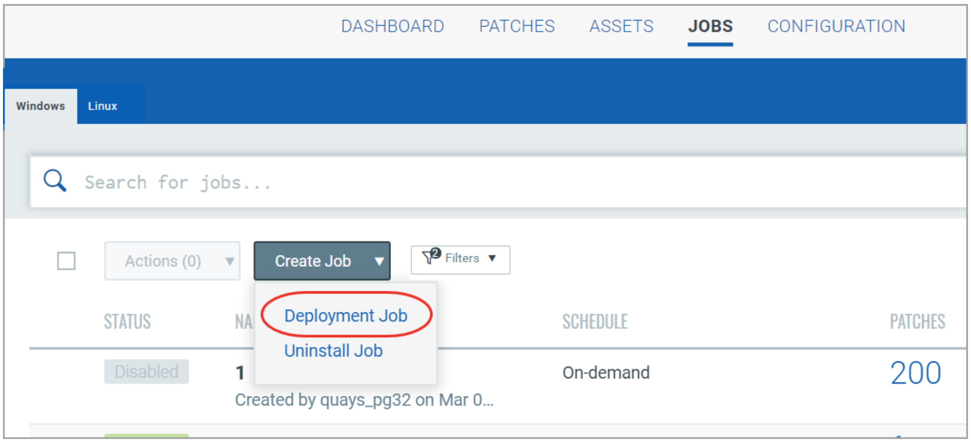
You must enable the disabled job in order to run it. To enable a disabled job, simply go to the **Jobs** tab, then from the **Quick Actions** menu of a job, click **Enable**. The **Save & Enable** option should be chosen only when you are confident that job is correctly configured, because this job will begin executing as soon as you "Save" the job.

Note that the Patch Manager user can change the job status (enable/disable), delete and edit the job.

User scenario: Installing critical patches for Chrome and Internet Explorer

To ensure that the browsers receive the critical updates, you can create a daily recurring job to ensure critical patches are deployed.

1. Navigate to **Jobs** > **Windows** > **Create Job**, and click **Deployment Job**.

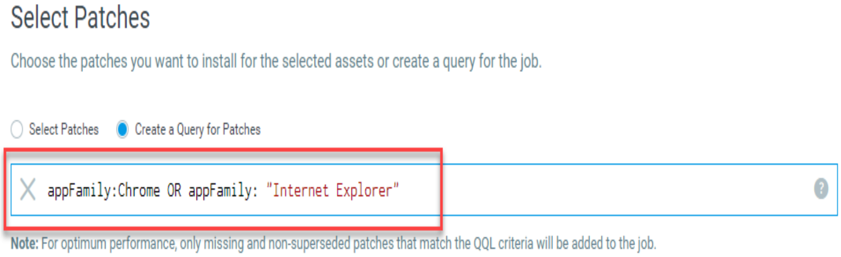


2. Enter the job title as ***Browser Security Patches*** and click **Next**.

3. Select assets or asset tags on which you want to apply the patches.

4. (Optional) Select **Add Exclusion Asset Tags** to exclude the assets from the deployment job that have ALL/ANY of the selected asset tags.

5. To select patches to apply to the assets, choose **Create a Query for Patches**. Enter **`appFamily:Chrome or appFamily:“Internet Explorer”`**.


Select Patches

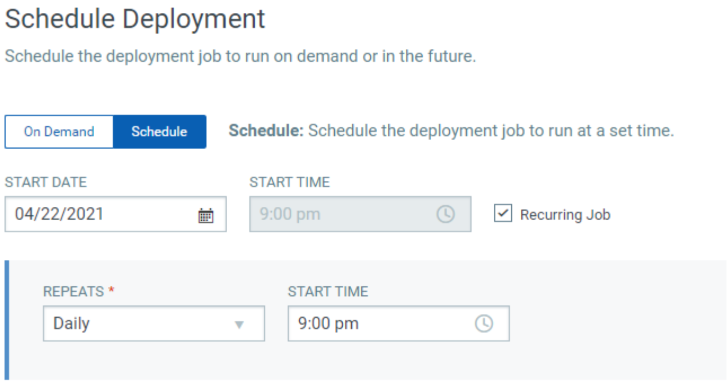
Choose the patches you want to install for the selected assets or create a query for the job.

○ Select Patches ● Create a Query for Patches

appFamily:Chrome OR appFamily: "Internet Explorer"

Note: For optimum performance, only missing and non-superseded patches that match the QQL criteria will be added to the job.

6. Create the following job schedule:



Schedule Deployment

Schedule the deployment job to run on demand or in the future.

Schedule: Schedule the deployment job to run at a set time.

START DATE: 04/22/2021

START TIME: 9:00 pm

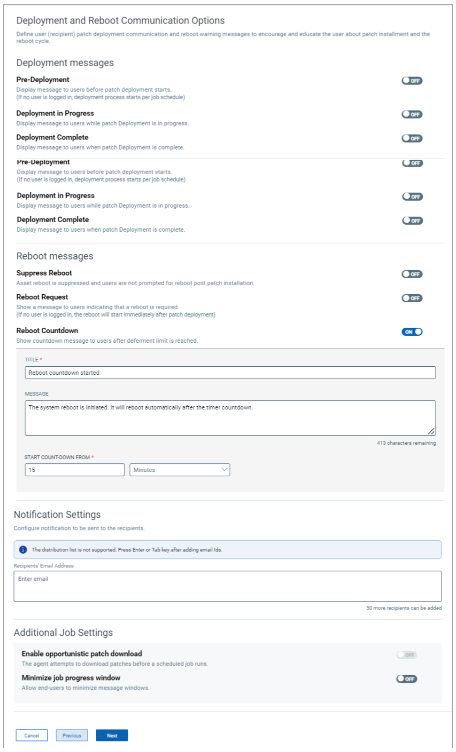
☑ Recurring Job

REPEATS *: Daily

START TIME: 9:00 pm

7. *(Optional)* Set the Patching window if you want to restrict the agent to start the job within the specified patch window (e.g., start time + 6 hours). The job will time out if it does not start within this window.

8. Based on your preference, configure how to notify the users about the patch deployment. Configure the pre-deployment messages, deferring the patch deployment certain number of times.



Deployment and Reboot Communication Options

Define user (recipient) patch deployment communication and reboot warning messages to encourage and educate the user about patch installment and the reboot cycle.

Deployment messages

Pre-Deployment: OFF
Display message to users before patch deployment starts.
(If no user is logged in, deployment process starts per job schedule)

Deployment in Progress: OFF
Display message to users while patch Deployment is in progress.

Deployment Complete: OFF
Display message to users when patch Deployment is complete.

Pre-Deployment: OFF
Display message to users before patch deployment starts.
(If no user is logged in, deployment process starts per job schedule)

Deployment in Progress: OFF
Display message to users while patch Deployment is in progress.

Deployment Complete: OFF
Display message to users when patch Deployment is complete.

Reboot messages

Suppress Reboot: OFF
Asset reboot is suppressed and users are not prompted for reboot post patch installation.

Reboot Request: OFF
Show a message to users indicating that a reboot is required.
(If no user is logged in, the reboot will start immediately after patch deployment)

Reboot Countdown: ON
Show countdown message to users after deferment limit is reached.

TITLE *: Reboot countdown started

MESSAGE: The system reboot is initiated. It will reboot automatically after the timer countdown.

413 characters remaining

START COUNT-DOWN FROM *: 15 Minutes

Notification Settings

Configure notification to be sent to the recipients.

The distribution list is not supported. Press Enter or Tab key after adding email Ids.

Recipients' Email Address: Enter email

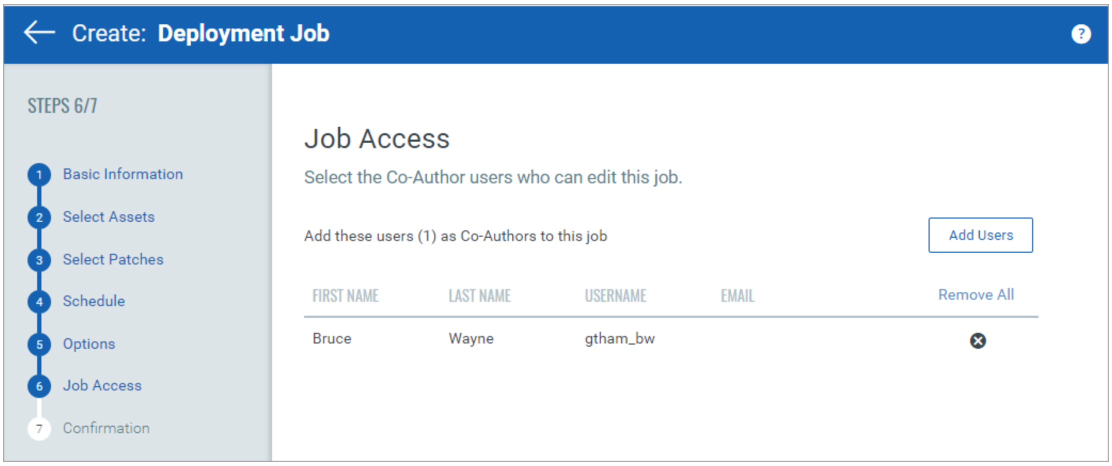
50 more recipients can be added

Additional Job Settings

Enable opportunistic patch download: OFF
The agent attempts to download patches before a scheduled job runs.

Minimize job progress window: OFF
Allow end-users to minimize message windows.

9. Finally based on the permissions assigned to other users, choose Co-Authors who can edit this job.



Job Access

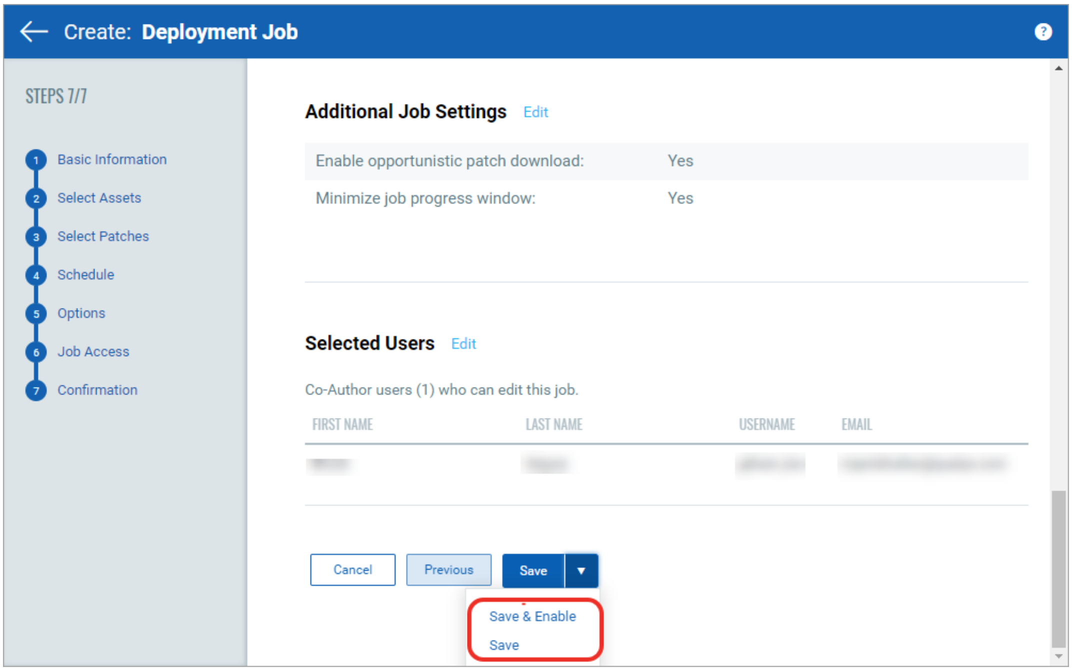
Select the Co-Author users who can edit this job.

Add these users (1) as Co-Authors to this job

FIRST NAME	LAST NAME	USERNAME	EMAIL
Bruce	Wayne	gtham_bw	

10. Next, review the configuration.

Job can either be created in ENABLED state by using the **Save & Enable** option or in DISABLED state by using the default **Save** button.



Additional Job Settings

Enable opportunistic patch download: Yes

Minimize job progress window: Yes

Selected Users

Co-Author users (1) who can edit this job.

FIRST NAME	LAST NAME	USERNAME	EMAIL
[redacted]	[redacted]	[redacted]	[redacted]

Note: The Patch Manager super user can change the job status (enable/disable), delete and edit the job.