Patch Management

Getting Started Guide
Version 1.5

June 28, 2021

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 and Linux 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.

Note: Qualys Patch Management 1.5 supports Linux assets for Patch Management.

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 and *Linux systems.

Note: * Currently, you can deploy patch jobs only on Linux assets for RHEL version 6 and 7.

Patch Management Process Workflow

Follow these steps to get started with Patch Management.

Agent Installation and Configuration

Install Cloud Agents (using the CA app)

Enable PM in a CA configuration Profile (using the CA app)

User Roles and Permissions

Deploy Patches

Create a custom assessment profile (Optional)

Review missing and installed patches

Deploying Patches Jobs on Windows Assets

Deploying Patches Jobs on Linux Assets

Review patch deployment results (success / failure)

Create a custom assessment profile (Optional)

Review missing and installed patches

Uninstalling Patches from Windows Assets

Review patch uninstall results (success / failure)

Patch Management features

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

- Deploy patches for Windows and Linux assets
- Schedule run-once or recurring jobs for Windows and Linux assets
- Clone and edit Windows and Linux jobs
- View patches, assets, and job details for Windows and Linux systems
- Review missing and installed patches for Windows assets
- Download Windows patches from the vendor site
- Create custom Assessment Profile for Windows assets
- Use QQL to automate patch selection for Windows deployment job
- Export patch data for Windows assets
- Uninstall patches from Window assets
- Create custom dashboards and widgets for Windows assets

User Roles and Permissions

Role-Based Access Control (RBAC) gives you the flexibility to control access to Patch Management features based on the roles of the individual users.

Each user is assigned a pre-defined user role which determines what actions the user can take. These roles are exclusive to the Patch Management module only. The roles defined in other modules have NO correlation with that defined in Patch Management.

We have the following five out-of-the-box (OOTB) roles for PM users. Each role, except Patch Security, is an incremental role to the previous one. Let's understand the user roles and permissions.

Roles	Description
Patch Reader	Default role that allows users to view: - Assigned jobs - Assessment profiles - Dashboards
Patch Dashboard Author	- Includes the Patch Reader permissions - Allows a user to develop dashboards - Does not allow the user to manage patching jobs
Patch User	- Includes the Patch Dashboard Author permissions - Allows users to manage patching activities - Build dashboards for reporting information
Patch Manager	- Includes all permissions except create job advisory
Patch Security	- This role is mutually exclusive from the other roles. - Meant for Security experts or Security operations (SecOps) - Allows the user to select patches and create a partially configured job which needs to be assigned to a Patch User or Patch Manager to add a job owner - Cannot edit any job

Note: We do not recommend that you create custom roles for the Patch Management users by assigning or removing permissions available through the default roles. Such customization of roles or change of permissions might cause the user roles to not work as per the design.

For Patch Management, we refer to the Global Dashboard Permissions to determine what operations a user can perform on the Unified Dashboard. The Global Dashboard Permissions will only allow the Patch Manager, Patch User, and Patch Dashboard Author to create, edit, and delete their own dashboards. For permissions to edit, delete other users' dashboard and print or download a dashboard, contact SuperUser or Administrator.

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/uninstall jobs.

Installing Cloud Agents on Assets

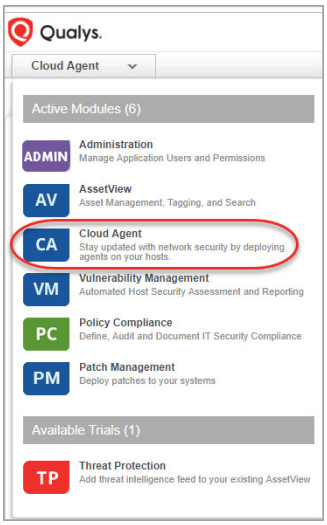
Patch Management allows you to manage your Windows and Linux assets. You must install and configure Cloud Agents to enable Patch Management to deploy patches jobs.

Agent installations are managed on the Cloud Agent (CA) app.

Let's get started!

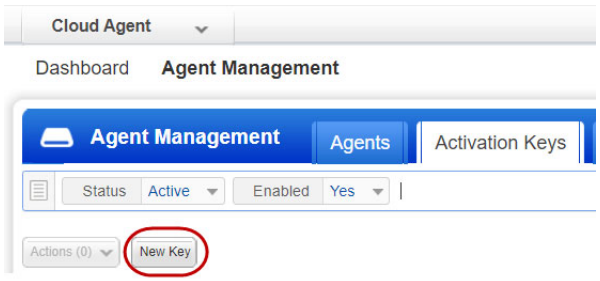
Choose CA (Cloud Agent) from the app picker.

As a first time user, you'll land directly on the Getting Started page.

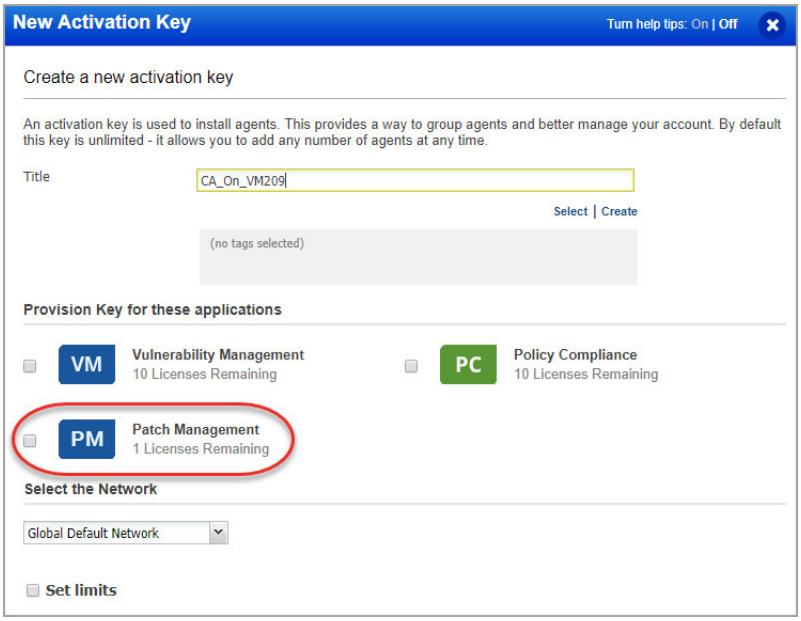


What are the steps?

Create an activation key. Go to Activation Keys, click the **New Key** button. Give it a title, provision for the PM application and click **Generate**.

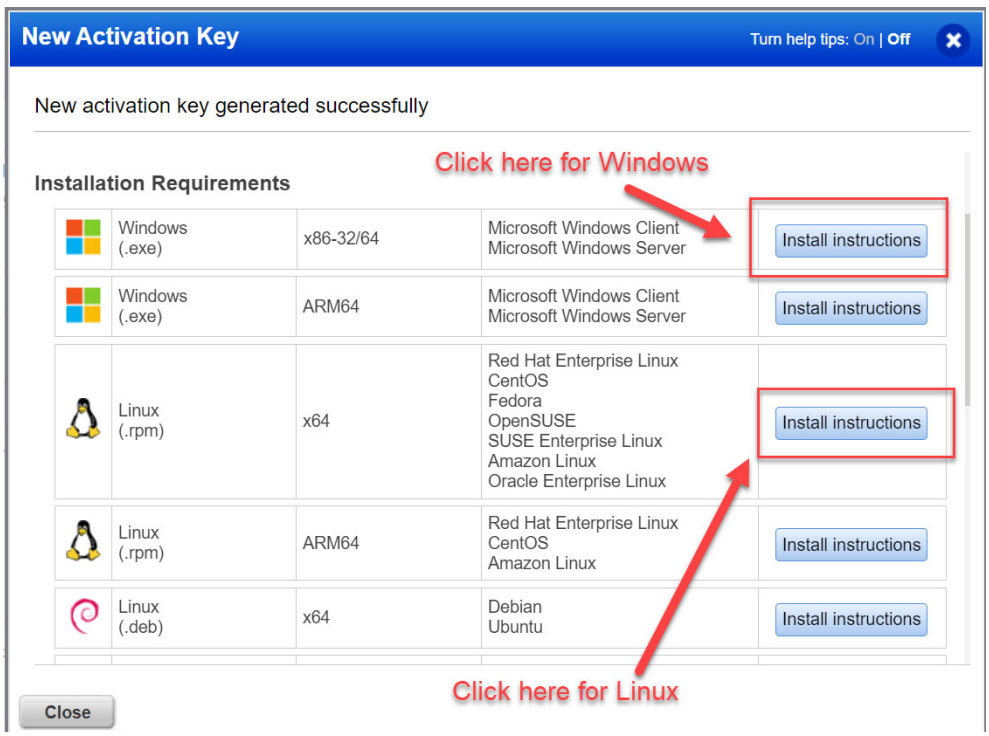


As you can see, you can provision the same key for any of the other applications in your account.



Downloading Installer

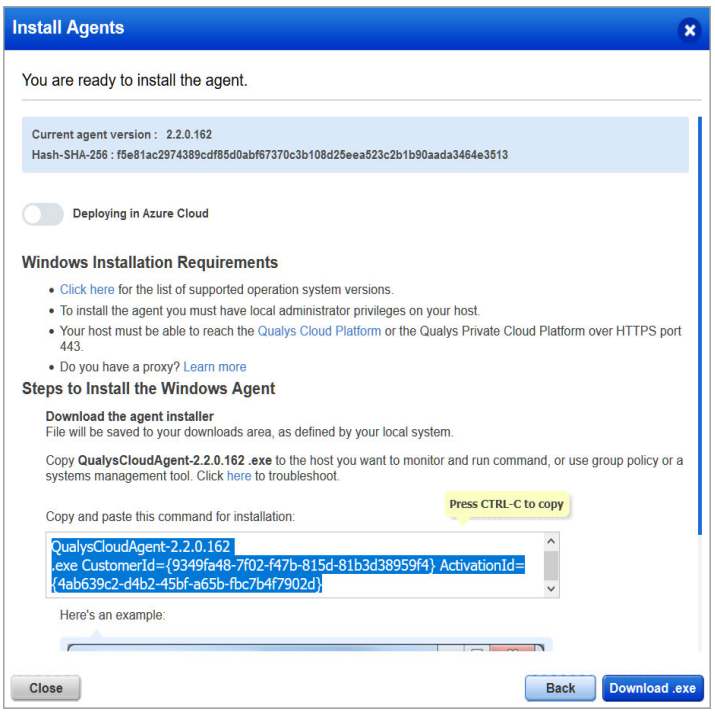
Click **Install instructions** next to **Windows (.exe)** or **Linux (.rpm)**.



Review the installation requirements and click **Download**.

You'll run the installer on each system from an elevated command prompt, or use a systems management tool or Windows group policy. Your agents should start connecting to our cloud platform

For Windows agent:



For Linux agent, to enable patch installation on Linux assets, note the following:

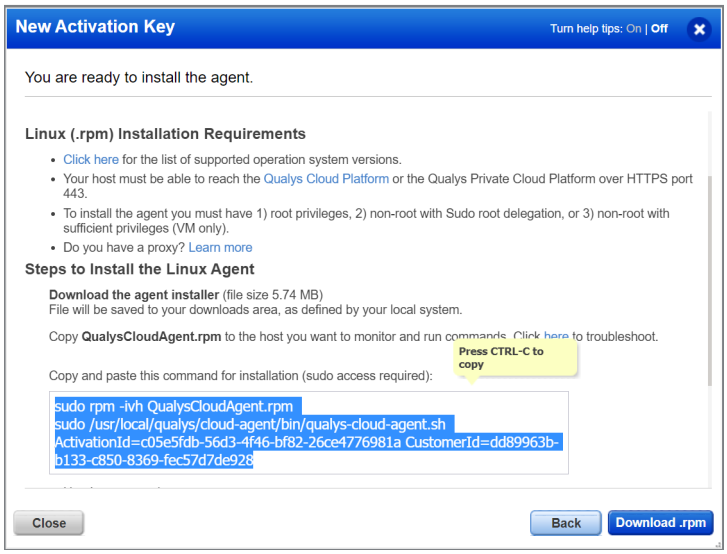
- Supported YUM file version 3.2.29.

- YUM file must be configured with debugloglevel >= 2 Default is 2.

- (Optional) The YUM file is configured with correct proxy settings.

- The endpoint is subscribed for active Red Hat subscriptions.

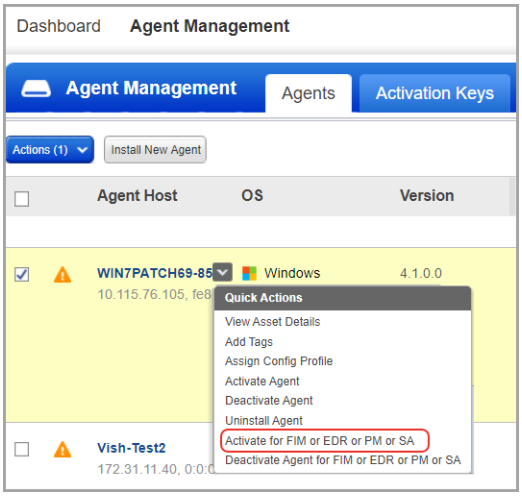
- The Agent must be running with root user or as sudo user. You can configure users by using the Agent configuration tool.



Your host must be able to reach your Qualys Cloud Platform (or the Qualys Private Cloud Platform) over HTTPS port 443. On the Qualys Cloud Platform, go to Help > About to see the URL your host needs to access. For more information about connectivity requirements/proxy settings refer to the platform specific Cloud Agent Installation Guides available on https://www.qualys.com/documentation/.

Note: Ensure that you whitelist the required URLs to allow the Cloud Agent to download the Windows patches on your host. Click here to view the list of URLs.

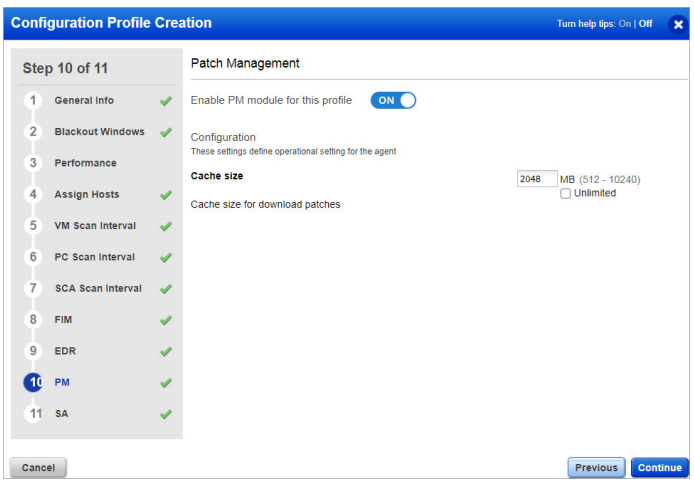
Activating your agents for PM



Go to the **Agents** tab, and from the **Quick Actions** menu of an agent, click **Activate for FIM or EDR or PM or SA**. (Bulk activation is supported using the **Actions** menu).

Enabling PM in a CA configuration profile

You can create a new profile or edit an existing one. The PM module is enabled by default.



The **Cache size** setting determines how much space the agent should allocate to store downloaded patches on the asset. The default allocated size is 2048 MB. If you are planning on using the opportunistic download, where an agent downloads patches before deployment, it is recommended to increase the cache size, or to allow for Unlimited Cache size. Note that the agent will clear the cached files after deployment.

You're ready!

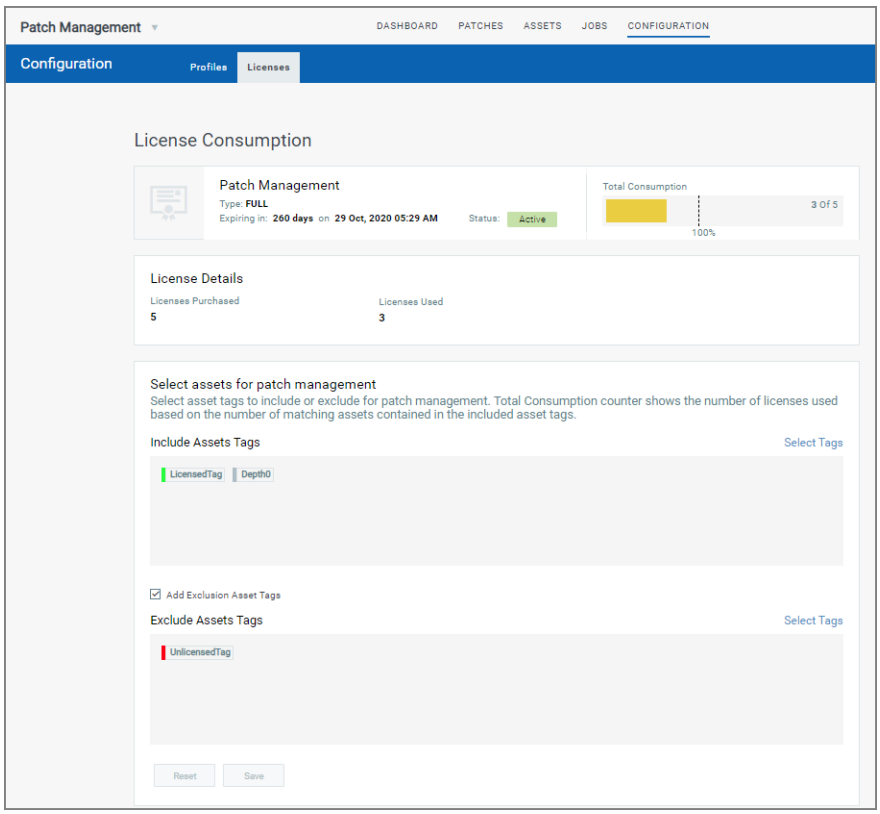
Select PM from the application picker and then create a deployment job to start installing patches on your assets.

Managing PM Licenses

The Licenses tab, enabled only for paid subscribers, shows the number of licenses consumed by Patch Management (PM). You can include asset tags to allow patch installing and uninstalling on the assets contained in those asset tags. The Total Consumption counter may exceed 100% if the number of assets activated for PM are more than the number of PM licenses you have. Assets in the excluded asset tags are not considered for patch management and you cannot deploy patches on those assets.

Note: In case the Total Consumption counter exceeds 100%, licenses will be consumed based on the asset activation time stamp in ascending order.

Only admin and super users can manage licenses. Sub-users can only view the license information.



Using Tags to Grant Access to Assets

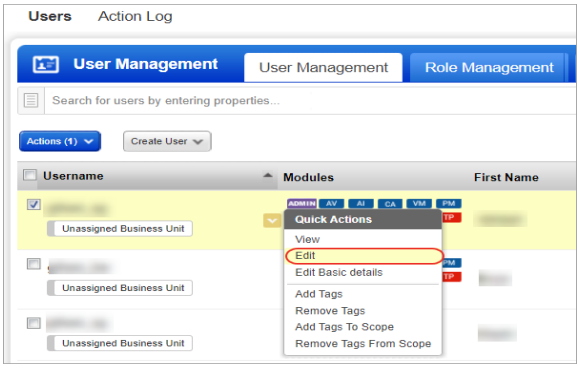
An asset tag is a tag assigned to one or more assets. Tag scopes define what assets the user can view when creating a job or when user go to **Assets** tab in patch management.

Assigning a tag to an asset enables you to grant users access to that asset by assigning the same tag to the users scope. Want to define tags? It's easy - just go to the **Asset Management** (AM) application.

To assign asset tags to the user,

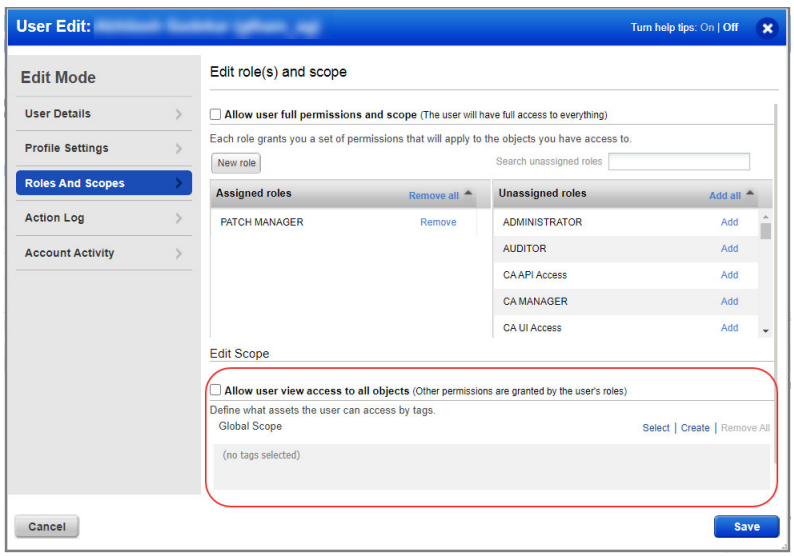
1) Go to the **Administration** module and then from the **User Management** tab search or select the user.

2) From the **Quick Actions** menu, click **Edit**.



3) On the User Edit screen, go to the **Roles and Scopes** tab.

4) In the Edit Scope section, select one or more asset tags that you want to assign to the user. Then click **Save**.



Creating Assessment Profiles for Windows Assets

You can create custom assessment profiles to add assets with specific tags and configure scan interval at which you want the cloud agent to collect patch information from the assets. This is an optional step.

By default, your cloud agents scan for patches (missing and installed) at a specific interval, as defined in the default Assessment Profile.

For Linux jobs, the patch scan is currently not supported and the installed and missing patches information is also not collected. Because of this reason, the assessment profiles are not applicable for Linux assets.

What is the default assessment profile?

At first, a default assessment profile is applied to all agents, which scans the assets at an interval of 24 hours for free subscription and 4 hours for trial/paid subscription.

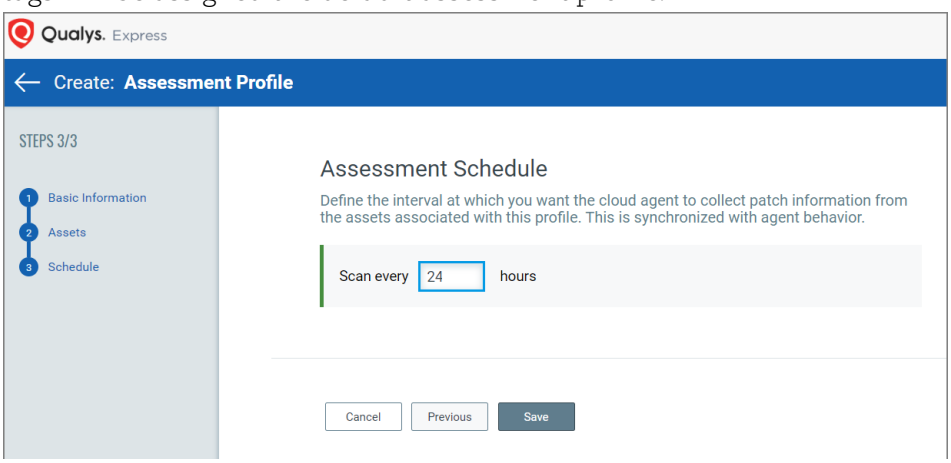
Adding a custom assessment profile

Simply go to **Configuration** > **Create Profile**, provide a profile name, select asset tags to apply this custom profile to, and then select the scan interval (minimum 24 hours for free subscription and 4 hours for trial/paid subscription). Multiple assessment profiles can be created with different intervals.

Note: Only admin users can create/modify/delete the assessment profiles. Non-admin users can only view assessment profiles.

Scan interval of less than 24 hours will be automatically changed to an interval of 24 hours, when a Paid or Trial subscription expires and the app gets converted into a free version.

Good to Know - Asset tags once applied to one custom profile, cannot be applied to another custom profile. When you select an asset tag, corresponding child tags are automatically selected. Assets falling under more than one profile because of different tags will be assigned the default assessment profile.



Reviewing Missing and Installed Windows Patches

The patch list under Patch Management patch catalog for Windows assets are the ones missing on the host which were detected using the Patch Management scan. You can view missing and installed patches on the **Patches** and **Assets** tab. The **Patches** tab show a key icon for patches that cannot be downloaded via the Qualys Cloud Agent. A key shaped icon indicates that the patch must be acquired from the vendor.

On the **Patches** tab, we list two types of patches:

1) Qualys Patchable

2) AcquireFromVendor

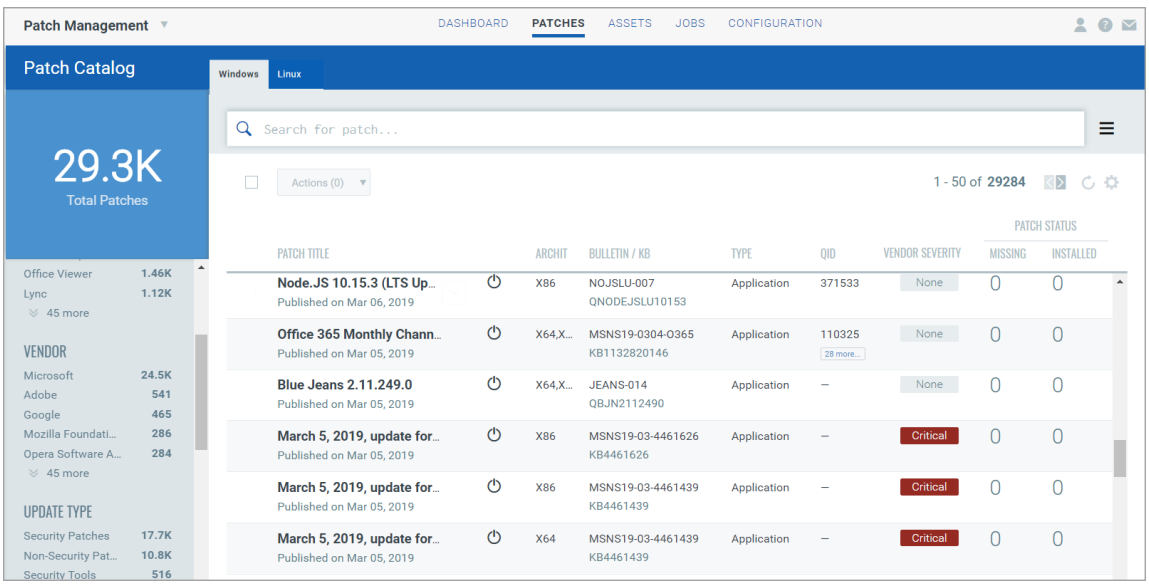
Qualys Patchable

Qualys Patchable are the patches that can be installed using Patch Management. Most of the patches listed on the Patches tab are Qualys Patchable.

AcquireFromVendor

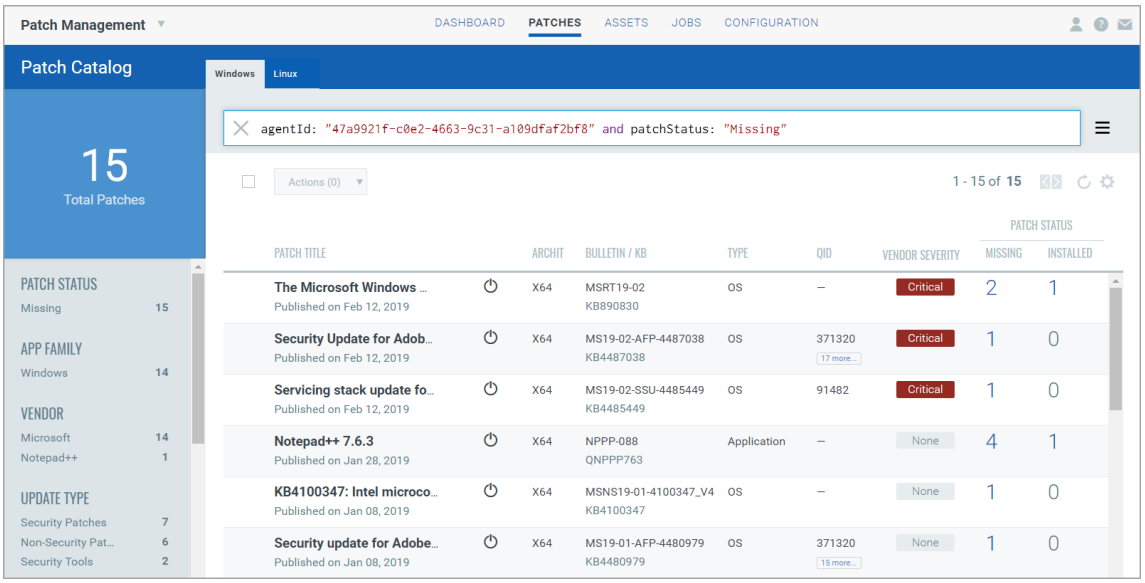
We have certain patches which are listed under **Patches** tab but cannot be installed using Patch Management. These patch are marked as "AcquireFromVendor" which means you need to manually download the patch from vendor website and install them on the host. See Downloading Patches from the Vendor Site.

Patches which are not marked as "AcquireFromVendor" are defined as "Qualys Patchable" which mean they can be added to a patch job.

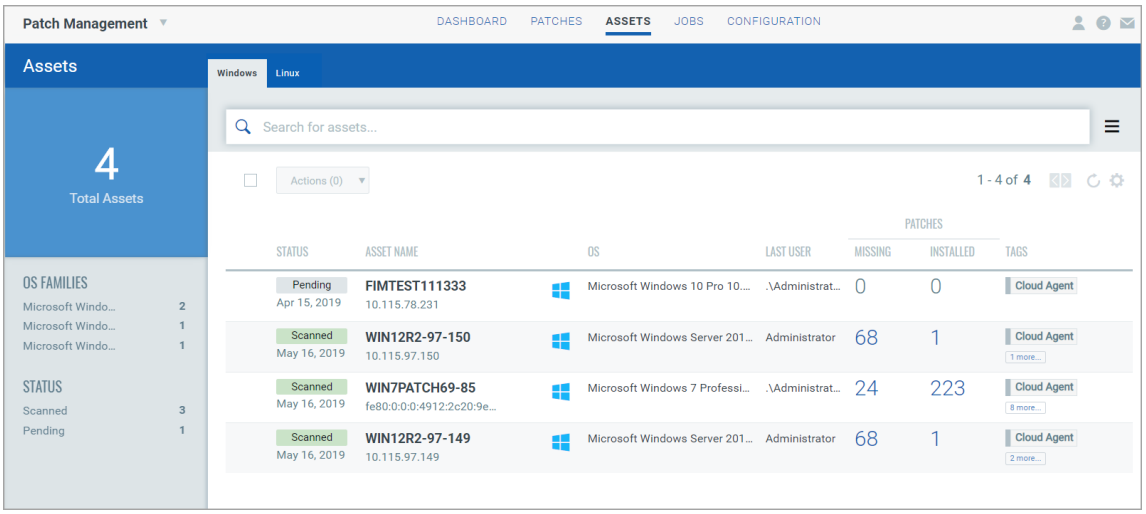


Default or custom assessment profile scans the assets for missing and installed patches at regular intervals. This information is then displayed on the **Patches** tab in the form of missing or installed patches.

Note that patches are linked to QIDs using CVE IDs. The QID for a patch is not shown if the QID is not linked to a CVE ID. CVE ID is the common point of linking and required to link the patch with the QID.

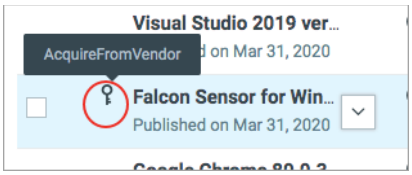


Alternatively, you can go to the **Assets** tab to view missing and installed patches on particular assets.



Downloading Patches from the Vendor Site

The Patches tab show a key icon for patches that can not be downloaded via the Qualys Cloud Security Agent. This “key” shaped icon indicates that the patch must be acquired from the vendor.



If you try to add such a patch to a patch job, then the system will show a message informing you that these patches will be not be added to said job as they are no longer supported for download via the Cloud Agent.

For such patches, the patch details page displays the Download Method as “AcquireFromVendor” and known patch URL in the Patch Information section. Use the URL to download the patch.

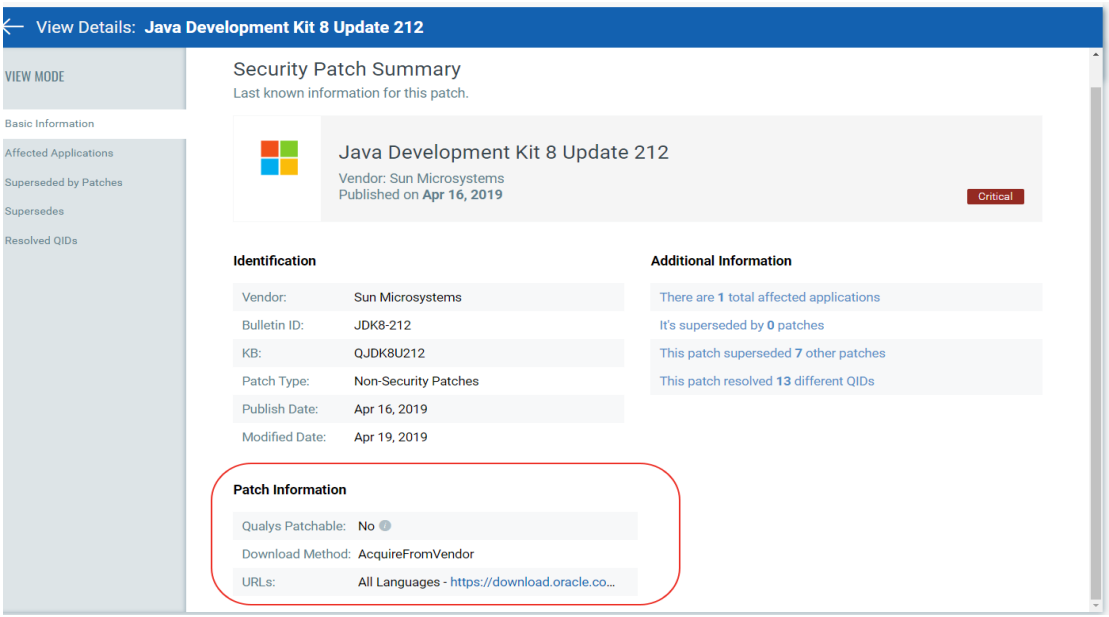
Download methods for patch are:

- Automatic - Patch downloadable using the Cloud Agent (Qualys Patchable: Yes)

- AcquireFromVendor - Patch must be acquired from the vendor and installed manually

(Qualys Patchable: No)

- Unavailable - Patch download information is not available (Qualys Patchable: No)



Deploying Patches Jobs on Windows Assets

You can create a deployment job to install missing patches on assets. You have three options to create the deployment job from the following tabs:

1) **Jobs**

2) **Assets**

3) **Patches**

Refer to the Managing Patch Jobs for Windows Assets topic in the online help.

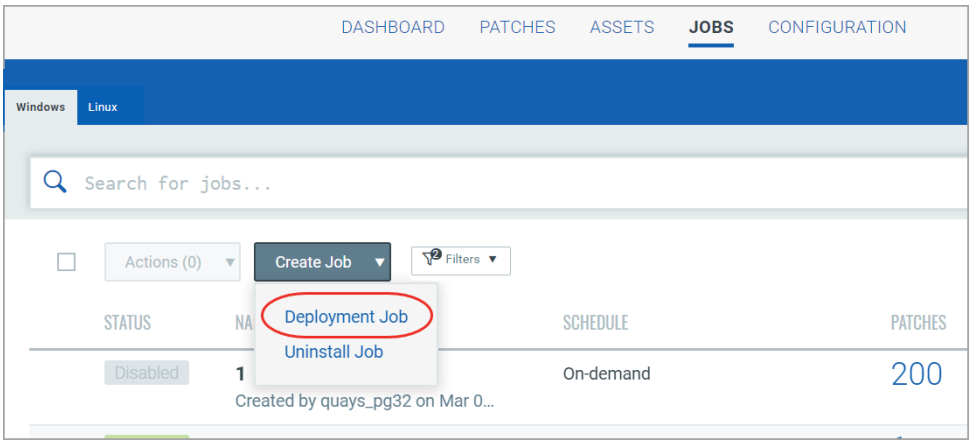
You can check the workflow to deploy jobs on Windows assets.

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**.



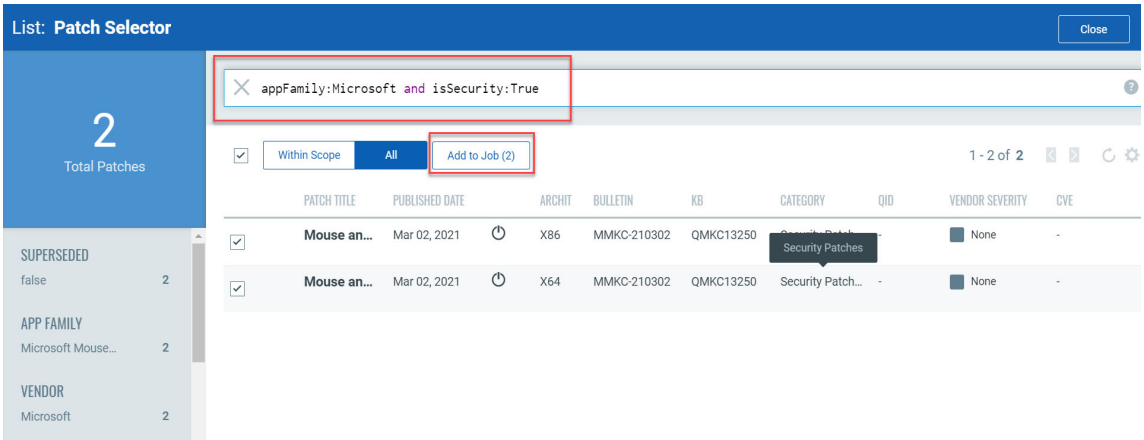
2. Enter the job title as ***Microsoft Security Patches*** and click **Next**.

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.



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

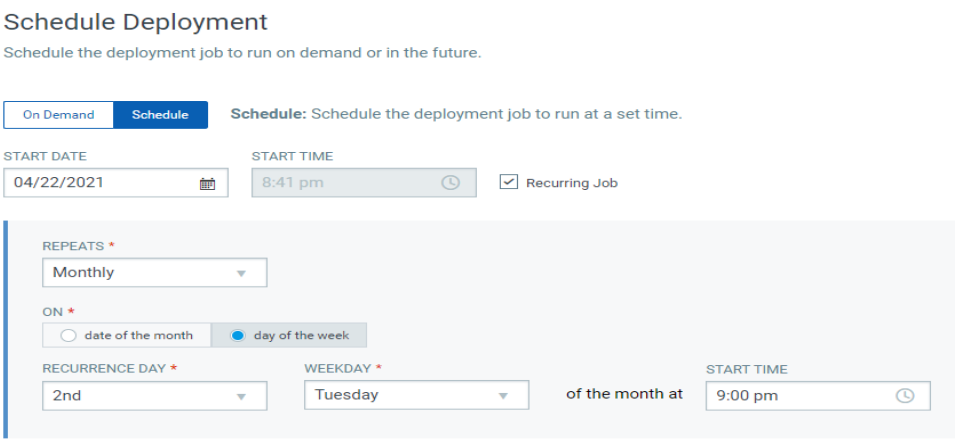
7. Click **Add to Job** and then click **Close**.

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

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

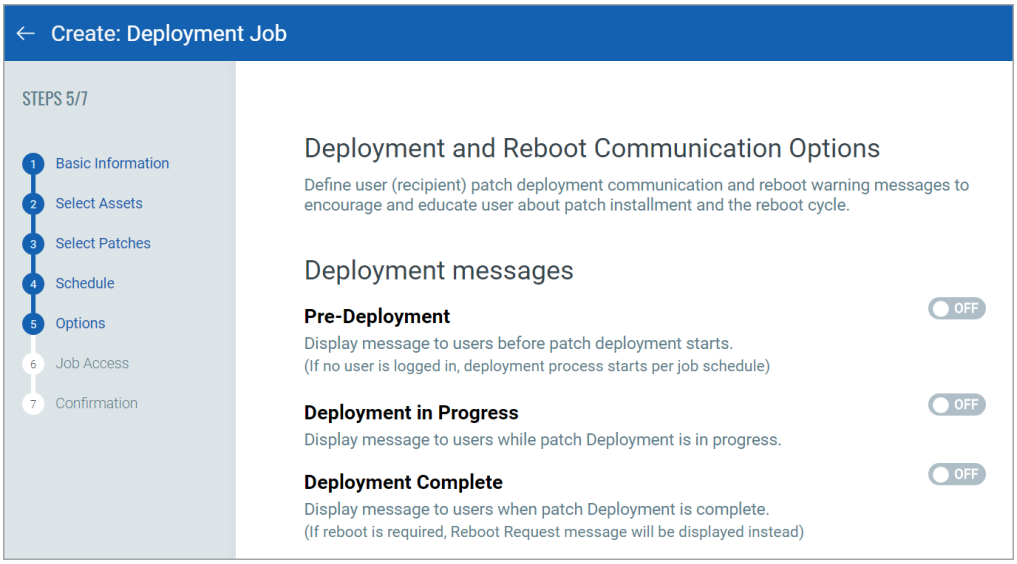
10. Select the start date and time, and select the **Recurring Job**.

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

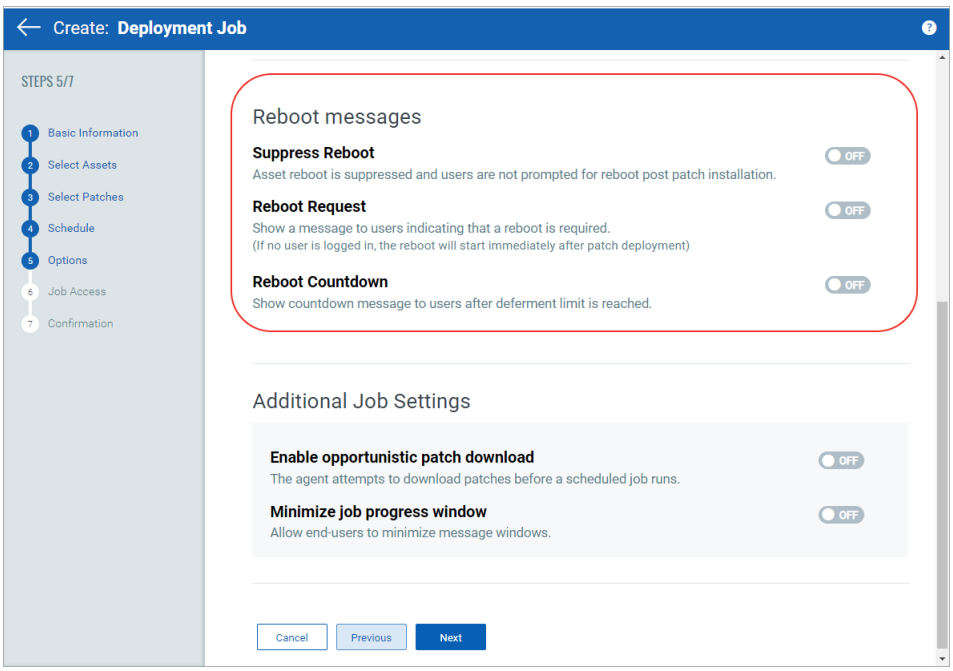


12. *(Optional)* Set the Patching window if you want to restrict the agent to start the job within the specified patch window (e.g., start time + 6 hours). The job gets timed out if it does not start within this window.

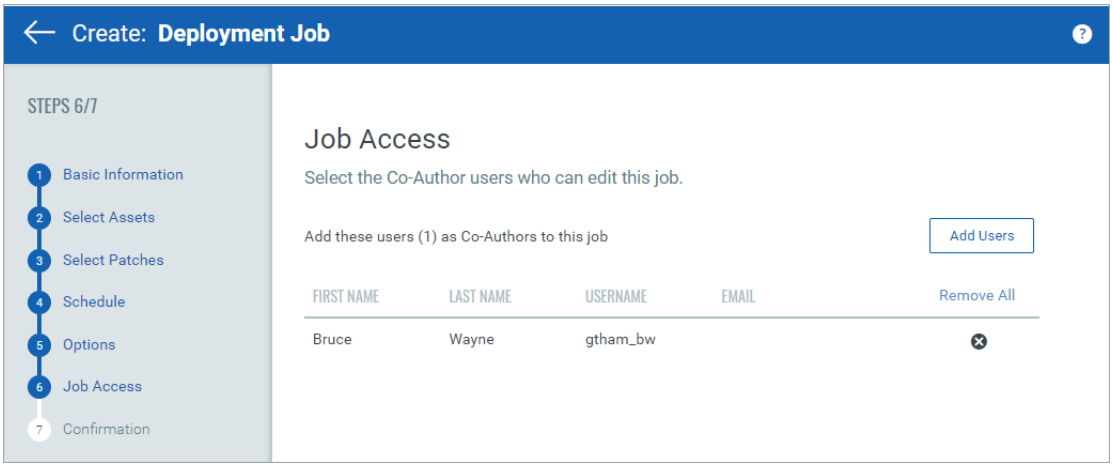
13. Based on your preference, configure how to notify the users about the patch deployment. Configure the pre-deployment messages, deferring the patch deployment certain number of times.



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

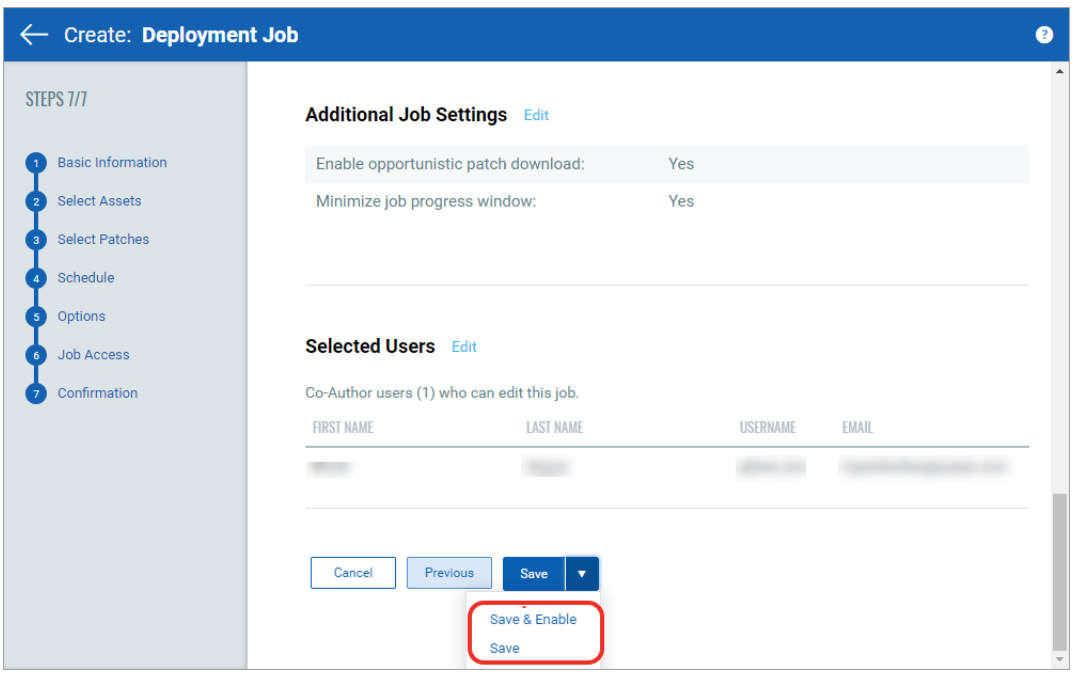


14. Finally based on the permissions assigned to other users, choose Co-Authors who can edit this job.



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

Using QQL to Automate Patch Selection for Windows Jobs

You can use Qualys Query Language (QQL) to provide the criteria that associates selective patches to a deployment job. QQL ensures that all the latest patches that qualify based on the criteria are automatically associated to a job without a manual intervention. This saves time and ensures that the critical patch updates are installed regularly.

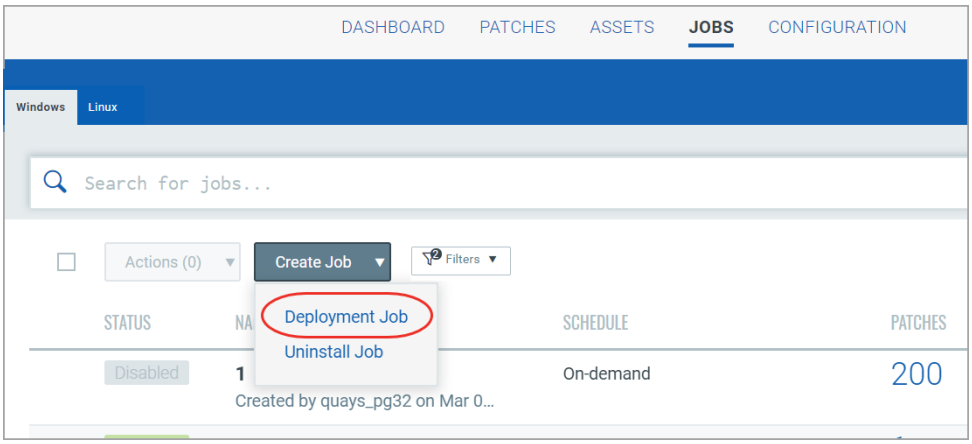
Although, you can use QQL for a run-once job, QQL is optimally utilized for recurring jobs.

QQL is available only for the deployment jobs and not for the uninstall jobs. Since uninstall patch jobs are executed for selective patches and rarely used, the QQL option is not provided for the uninstall 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**.

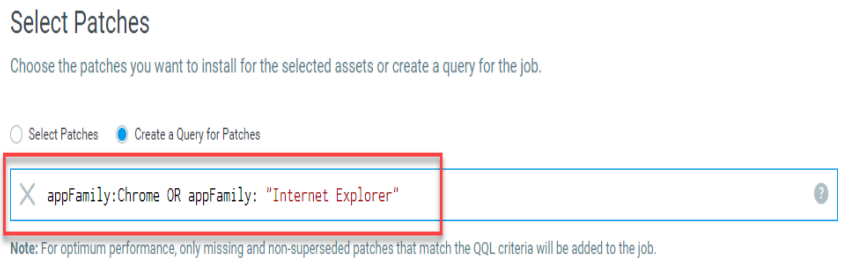


2. Enter the job title as ***Browser Security Patches*** and click **Next**.

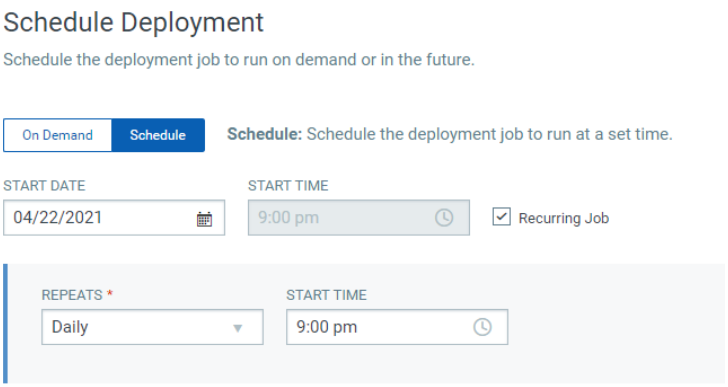
3. Select assets or asset tags on which you want to apply the patches.

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"`**.

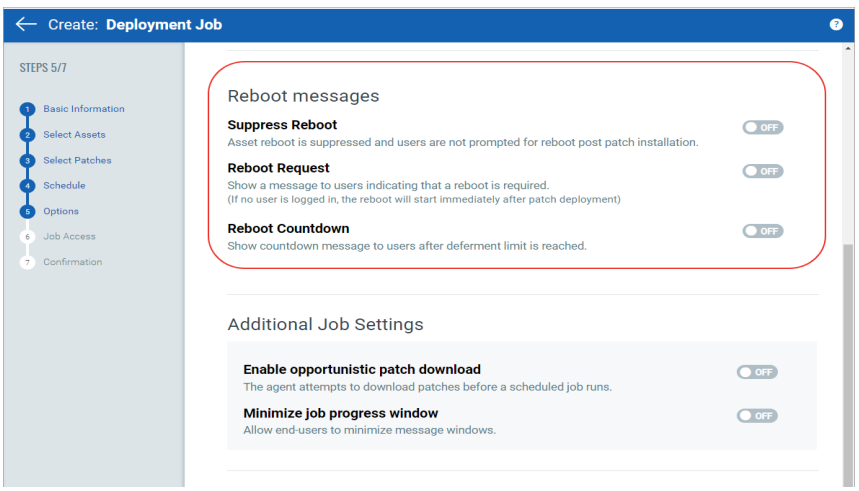


6. Create the following job schedule:

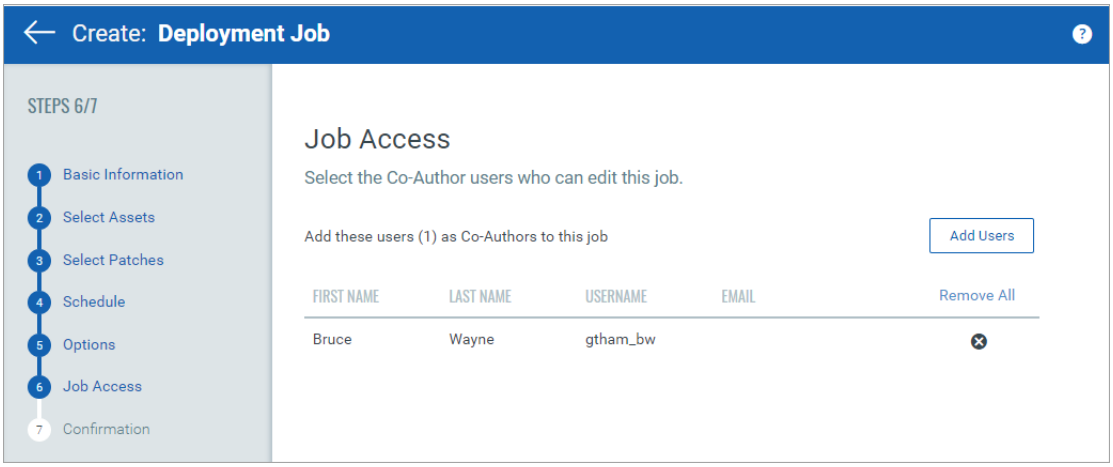


7. *(Optional)* Set the Patching window if you want to restrict the agent to start the job within the specified patch window (e.g., start time + 6 hours). The job will time out if it does not start within this window.

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.

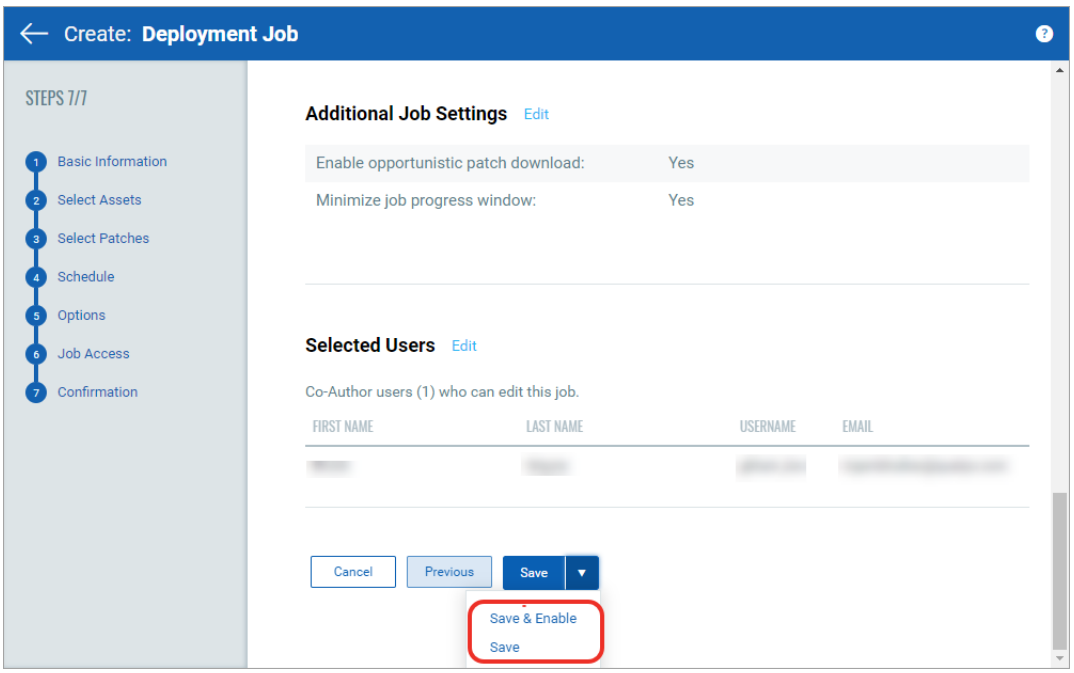


9. Finally based on the permissions assigned to other users, choose Co-Authors who can edit this job.



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.



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

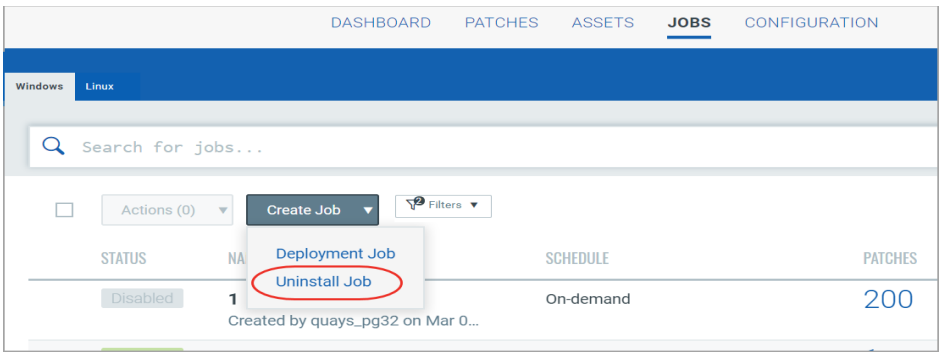
Uninstalling Patches from Windows Assets

You can create a patch uninstall job to uninstall patches from Windows assets. Uninstall job is rare and should be used with caution because it can uninstall patches that you might not have wanted to uninstall. We recommend that you use the run-once option for the uninstall Windows job. We don't uninstall software applications by default, however if a patch is rolled back, sometimes the software application might get uninstalled. Be extremely precise while selecting the patches that you want to uninstall.

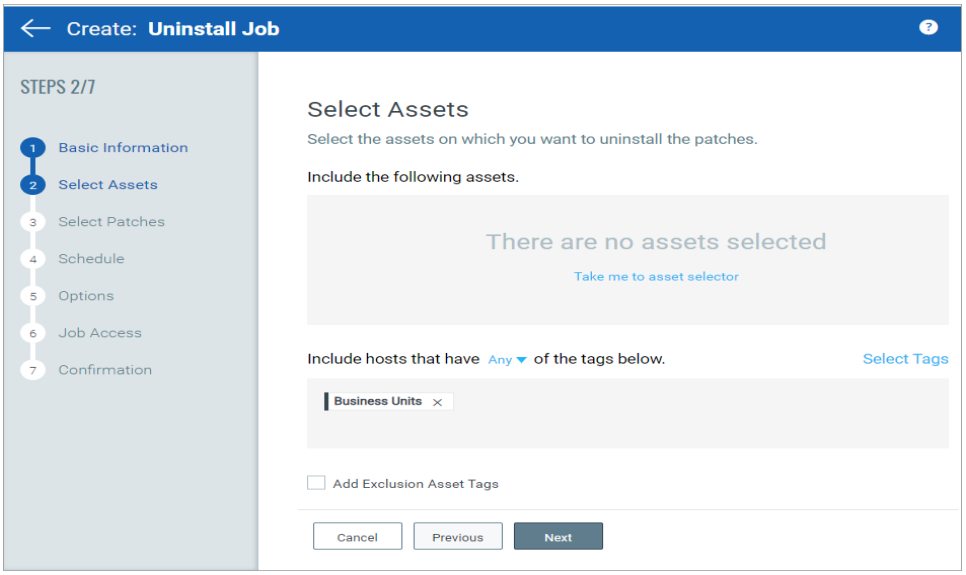
User Scenario: Uninstalling older version of Internet Explorer browser

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

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

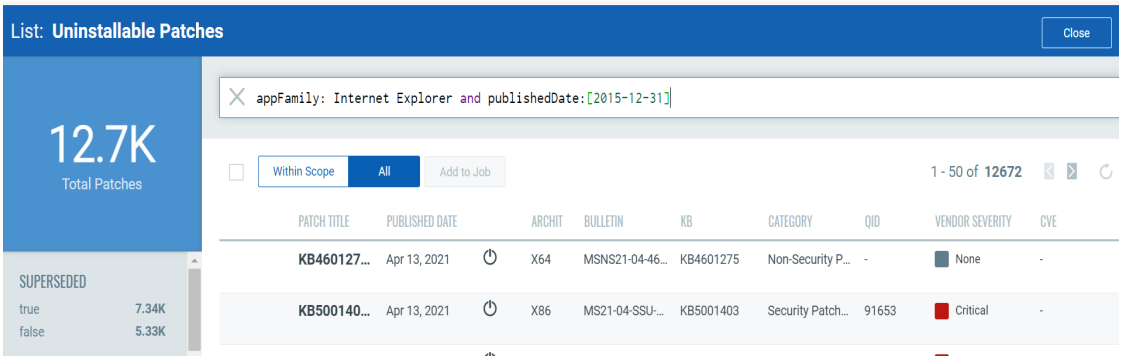


2. Provide a job title, and then select assets or asset tags uninstall the patches from.

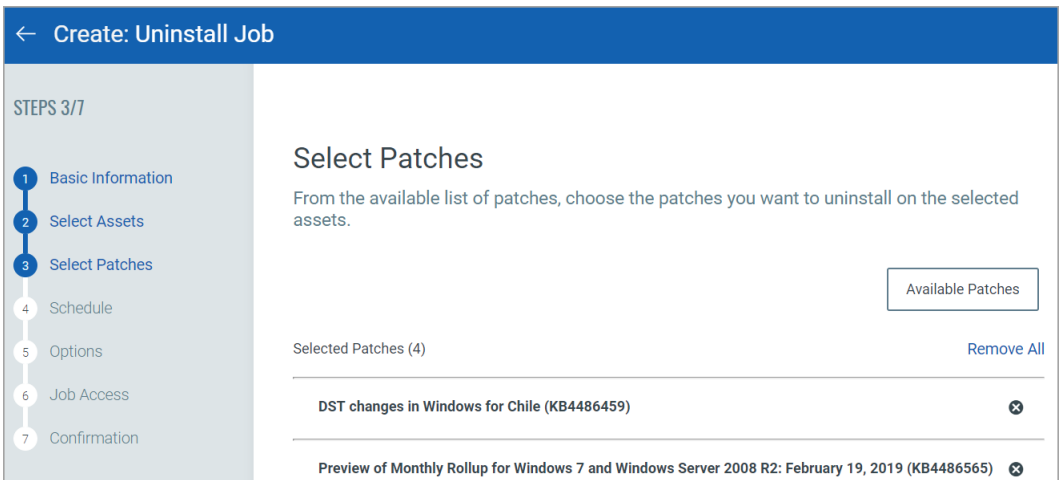


3. Select patches to uninstall from the assets. Use the patch selector link to select patches.

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



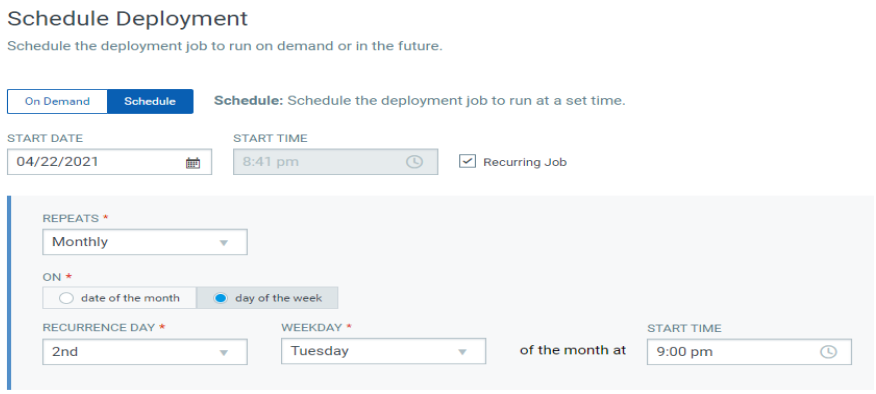
Note: You can add maximum 2000 patches to a single job.



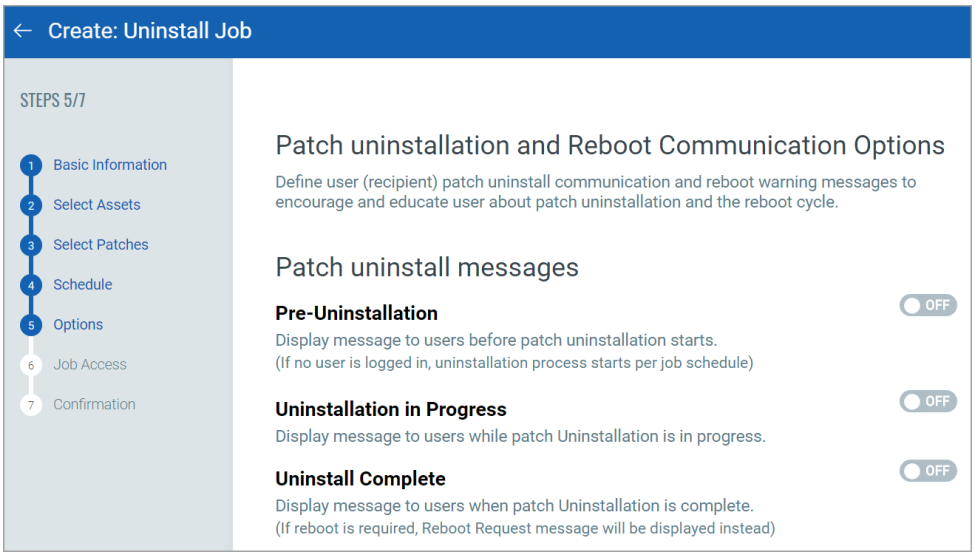
7. Click **Add to Job** and then click **Close**.

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

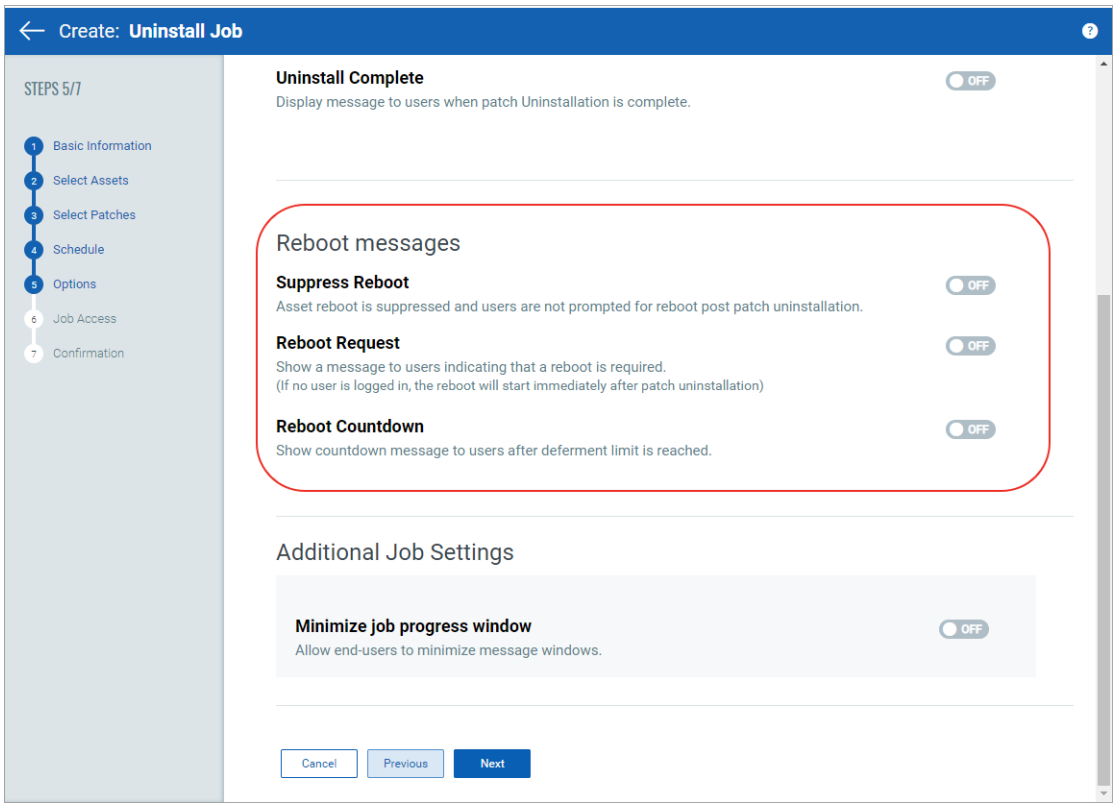
9. On the Schedule Deployment page, click **On Demand**.



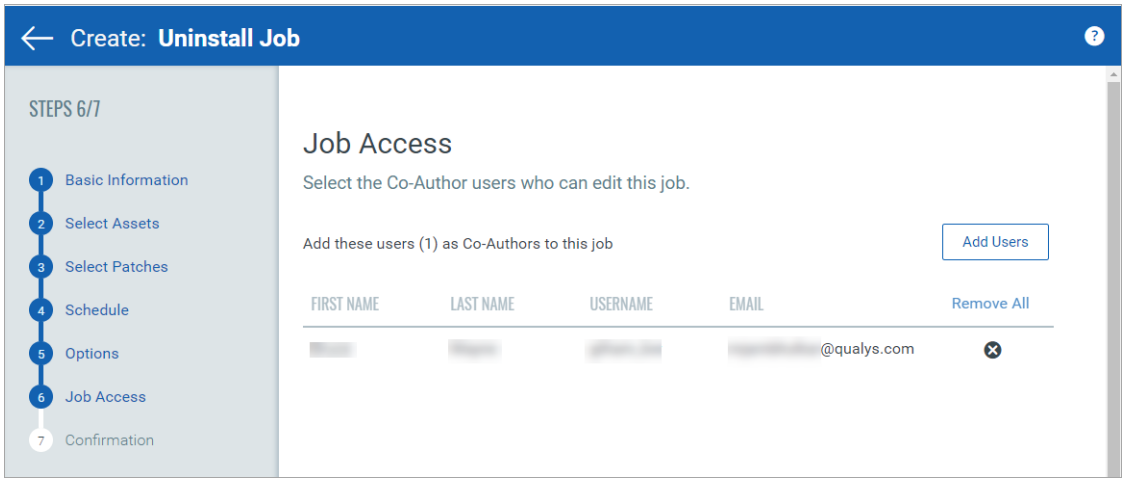
10. Based on your preference, configure how to notify the users about the patch deployment. Configure the pre-deployment messages, deferring the patch deployment certain number of times.



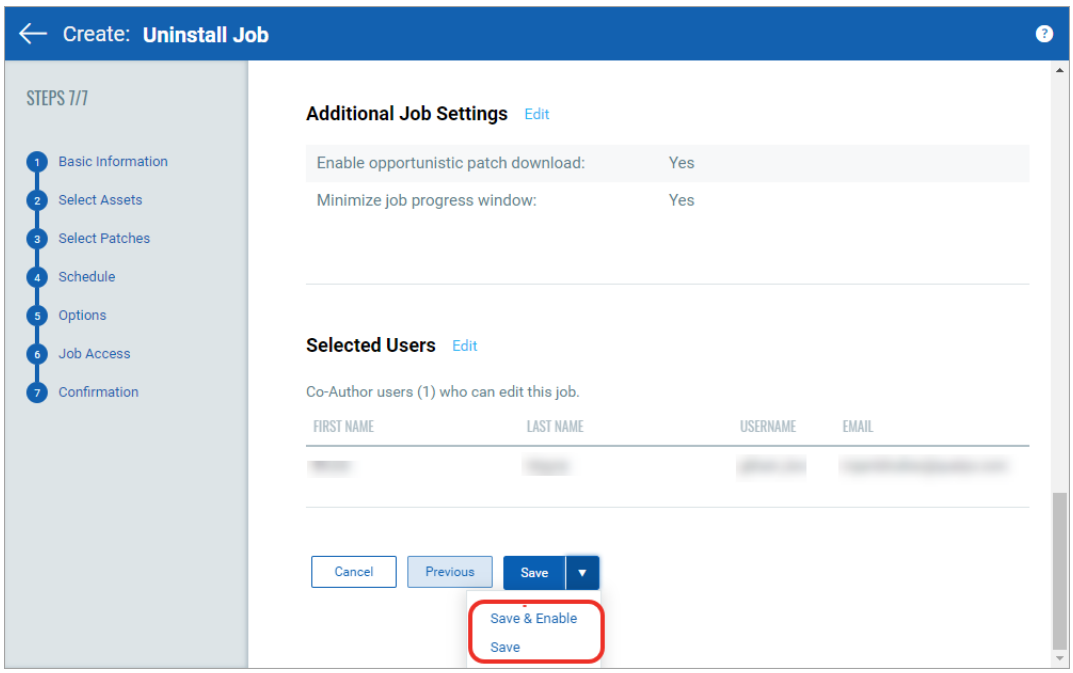
11. Finally, you can prompt the user or choose suppress reboot when asset reboot is required post patch installation.



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



13. 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.



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.

Deploying Patches Jobs on Linux Assets

You can create a deployment job to install patches on Linux assets. You have three options to create the deployment job from the following tabs:

1) **Jobs**

2) **Assets**

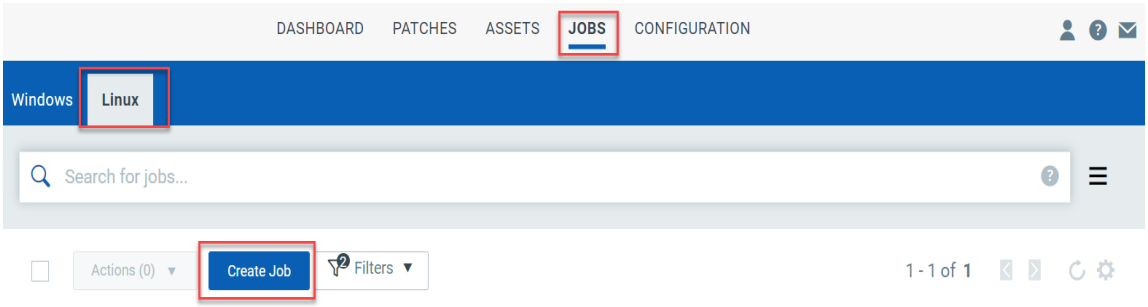
3) **Patches**

Refer to the Managing Patch Jobs for Linux Assets topic in the online help.

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**.



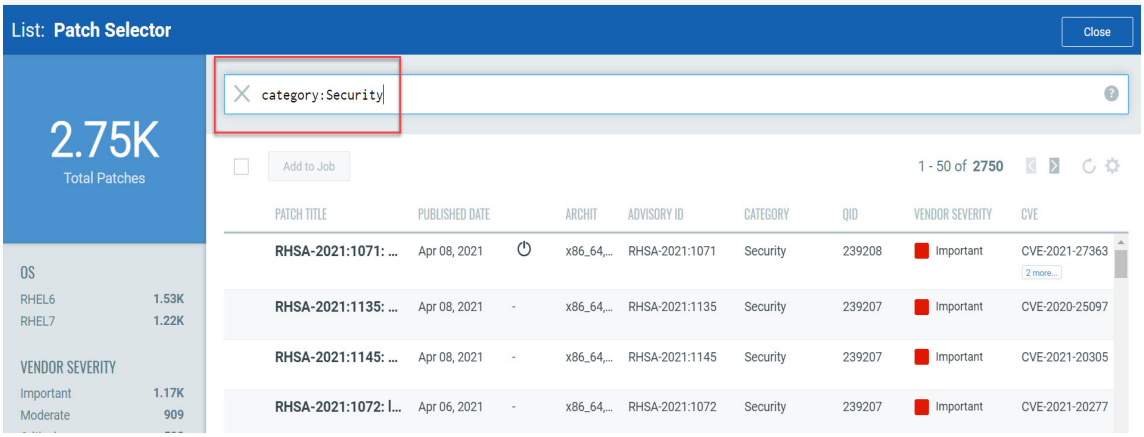
2. Enter the job title as ***RHEL Security Patches*** and click **Next**.

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.

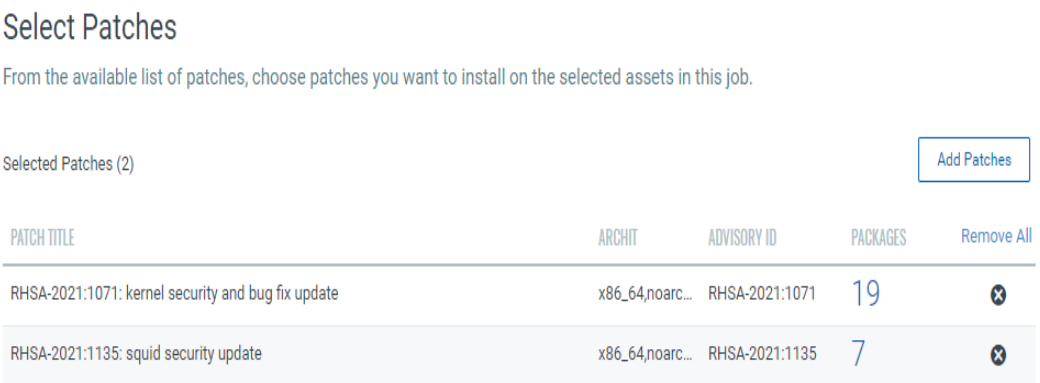
6. On the Patch Selector page, in the search query, enter **`category: security`** and select the patches.



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

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

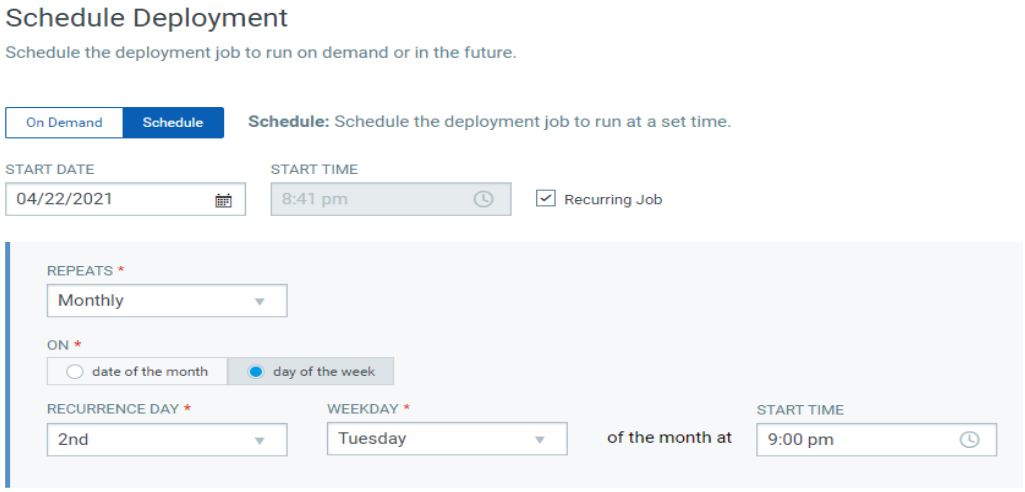
8. On the Select Patches page, click **Next**.



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

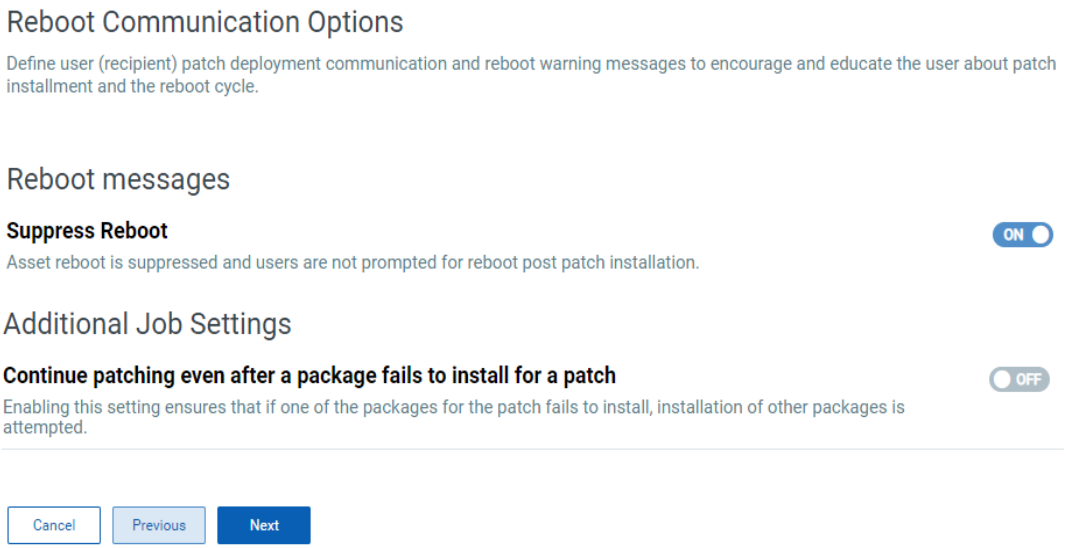
10. Select the start date and time, and select **Recurring Job**.

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

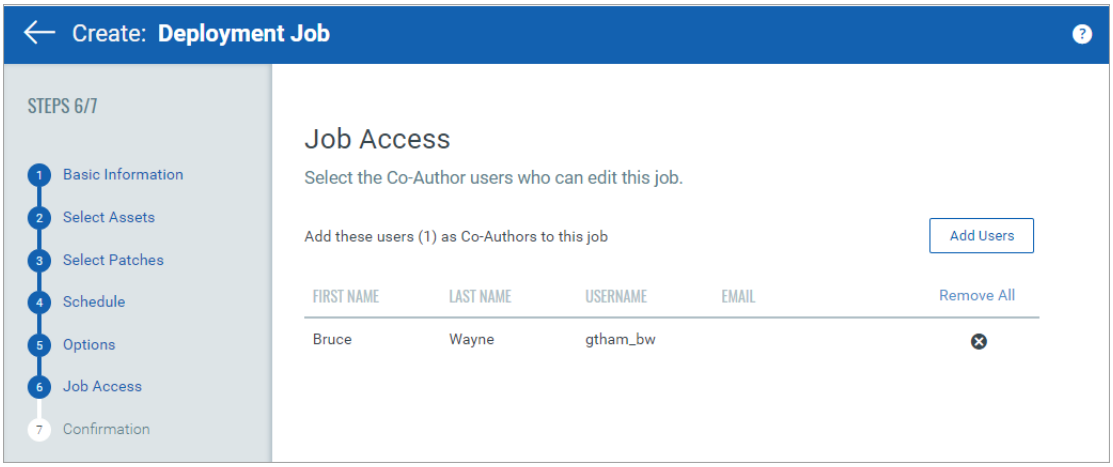


12. *(Optional)* Set the Patching window if you want to restrict the agent to complete the job within the specified patch window (e.g., start time + 6 hours). The job will timed out if it does not complete within this window.

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.



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



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.

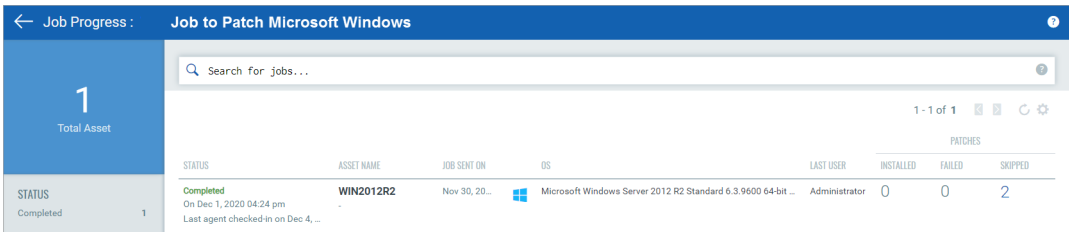
Note: The Patch Manager super user can change the job status (enable/disable), delete and edit the job.

Reviewing Job Results

Once the deployment or uninstall job is created, it runs immediately (OnDemand) or at the specified schedule. You can view the results of a job run, whether all patches were successfully installed or uninstalled or if there were failures.

To view the job results, go to Jobs, then from the **Quick Actions** menu of a job, click **View Progress**. You can see the assets on which the patch deployment / uninstall job was run, and the results in the Progress column.

On this screen, we also show you the assets that are not licensed in Patch Management. We skip job execution for these assets.



We also show the following patch count for Windows jobs:

- INSTALLED: Number of patches that were successfully deployed on the agent in the latest job run.

- FAILED: Number of patches that failed to install due to some errors on the agent in the latest job run.

- SKIPPED: Number of patches that were skipped in latest job run.

A few patches might be skipped because the patches are not applicable for the asset, superseded by another patch, or are already installed.

Note: The error logs for failed patches of Linux patch jobs are stored only for 14 days.

Job activities corresponding to the reboot messages and notifications displayed on the asset, are logged at the following location:

%USERPROFILE%\AppData\Local\Qualys\QualysAgent\QAgentUiLog.txt

Exporting Patch Data for Windows Assets

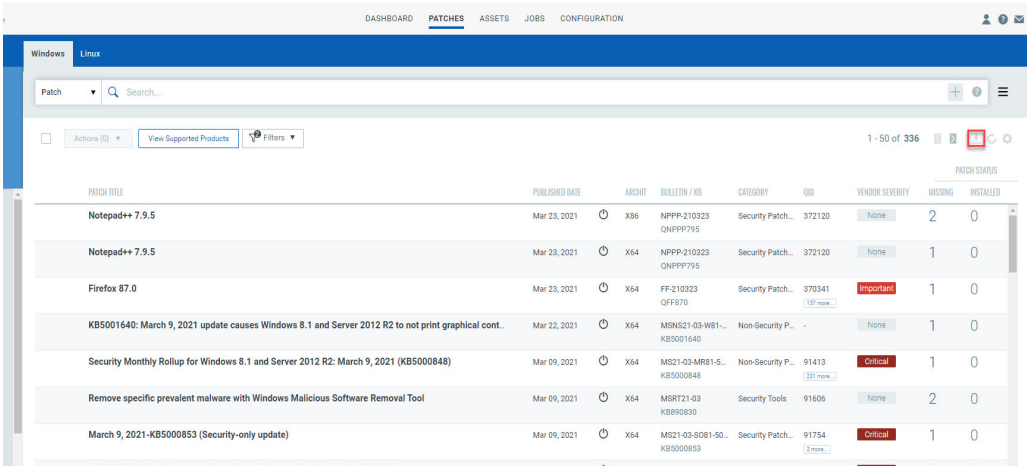
You can export detailed patch data for Windows assets from the **Patches** and **Assets** tabs. You can download job progress details from the **Job Progress** option on the **Jobs** tab.

You can also view the list of reports generated and their statuses. Exporting the patch data allows to import the data to a preferred analytic tool, such as Tableau. For example, you can analyze the data and calculate compliance ratio to make sound decisions or you can use the patch data to identify patches that were missed based on the severity of the critical assets.

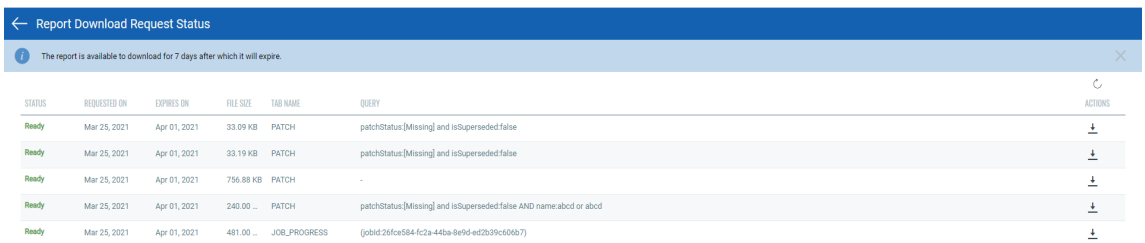
You can now overlay the patch data with other business data to set a new context for analysis. Exporting allows you to integrate data from different systems and view it on a single pane of glass. The reports are available to download for 7 days.

How to Export Patch Data?

To export patch data, go to the **Patches** or **Assets** tab and click **Download**:



The Report Download Request Status page lists all the reports that are ready to download or are being generated. Once the reports are generated, click to download the report and then simply unzip the file to view the data.



You can also export the data from the J**ob Progress** tab. To download the individual job details. Go to **Jobs** > **Quick Actions** > **View Progress** > **Download**.