ivanti

Endpoint Security

powered by HEAT Software

Patch and Remediation Best Practice Guide

Dec 2020

Contents

Introduction

Why is Patching Important?

Keeping your endpoints updated with the latest patches is crucial to keeping your network secure. This practice is the first and last line of defense against exploits, whether they are existing or new. Therefore, patch and vulnerability management should be a cornerstone of your risk mitigation strategy. Not only does patching reduce risk itself, it also provides a foundation that AntiVirus and other security technologies leverage. You need to keep your systems patched!

As exploits that target your operating systems and business applications increase in volume and sophistication, your window for assessing and deploying security patches is key for mitigating risks, remediating vulnerabilities, and reducing overall costs.

This guide details best practices for using Ivanti Patch and Remediation. We've developed these practices for patch and vulnerability management over thousands of customer engagements. These simple, flexible practices revolve around Patch Tuesday.

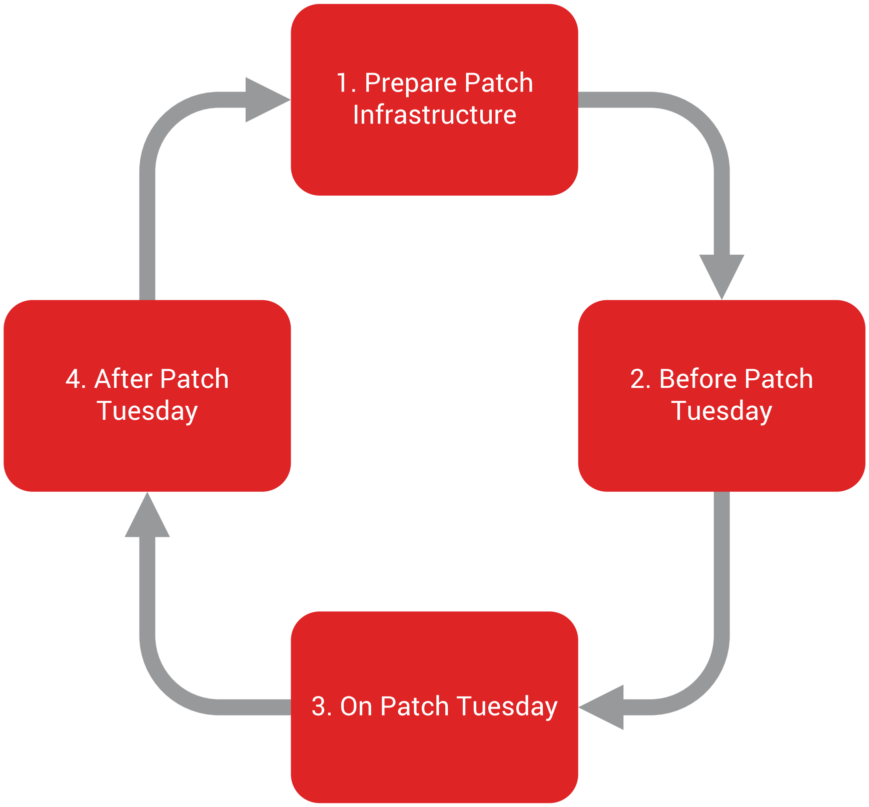
Patch Tuesday

Patch Tuesday is a software industry event that occurs once a month. On this day, Microsoft (who invented the practice) and other software companies release a collection of security updates. Ivanti adds these updates to the Global Subscription Server, a cloud service that contains thousands of security patches.

You should plan your patch workflow around this day. Patching your endpoints shortly after the latest security updates are released ensures your endpoints' exposure to vulnerabilities is minimized.

The Monthly Patch Cycle

The following chart displays how you should prepare for, execute, and follow up on vulnerability patching.

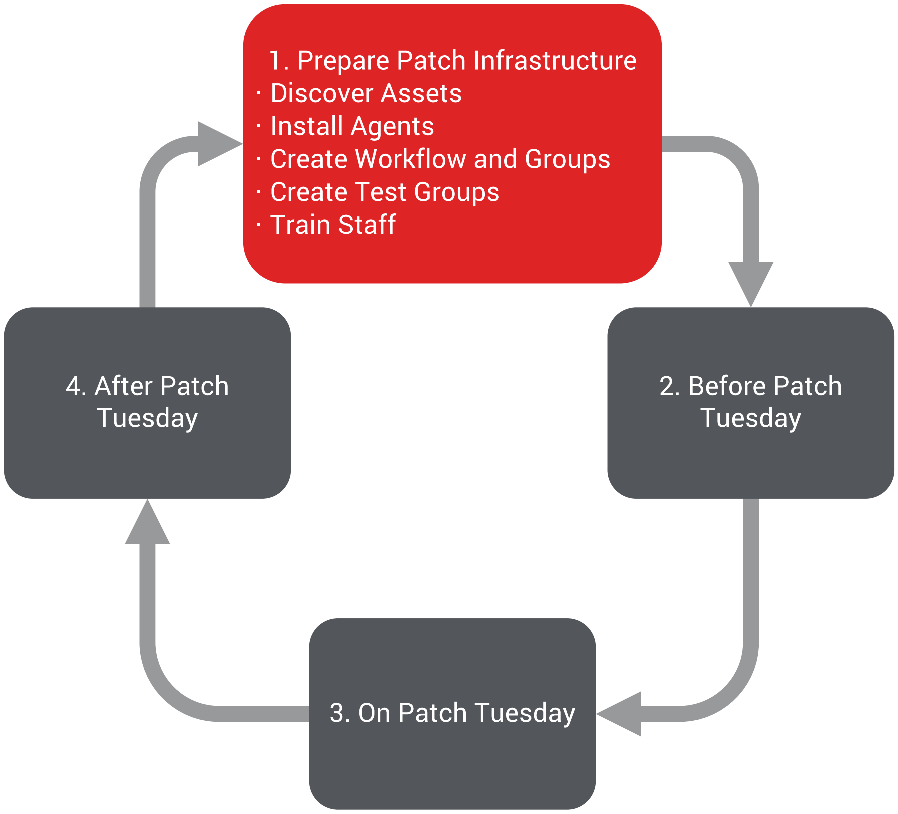


The patch management process for every company will be different; each network is unique and has unique requirements. What's most important to remember is that these best practices run in a monthly cycle based on Patch Tuesday. Additionally, these best practices are iterative–you can modify them based on what you learn each patch cycle.

We recommend documenting your own version of the Patch Tuesday process and sharing it with your organization. These documents help communicate the importance of patching and how it helps workers do their jobs. In this best practice guide, we base the process around Patch Tuesday, but you can customize your patch process for your organization and its IT practices—with equally effective results.

Prepare Patch Infrastructure

Before you can patch your network endpoints, you have to install endpoint software, group your endpoints, and train your staff about the patch process. This chapter covers how to complete each of these processes.



There are two contexts where you'll need to configure your patch infrastructure:

- Patch Infrastructure Setup:

  Before your first patch cycle, you'll need to complete a large-scale patch infrastructure configuration. This process involves quite a bit of work: installing software, creating endpoint groups, training staff, etc. Plan on devoting a few days to this process.

- Patch Infrastructure Maintenance:

  After your first patch cycle, you'll need to maintain your patch infrastructure. This means installing Endpoint Security software on new endpoints as staff arrive and depart from your organization and refining groups and policies for more efficient patching.

In This Chapter:

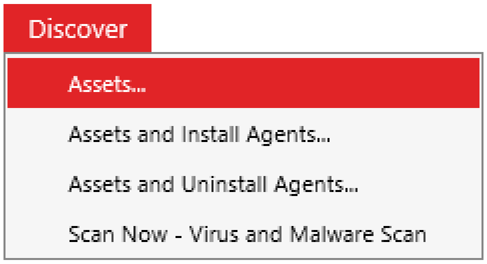
Discover Assets

Before you can patch your network, you need to install the Endpoint Security Agent on your endpoints. And before you install the agent, you need to know what's in your network.

The Ivanti Endpoint Security Server includes a feature that scans your network for devices, which we call **assets**. Assets include devices like desktop computers, laptops, printers, scanners, and so on. Use the Discover Assets feature to find computers in your network capable of hosting the Endpoint Security Agent, which include Windows desktops and laptops. This scan finds your assets and lists the operating systems that they're running.

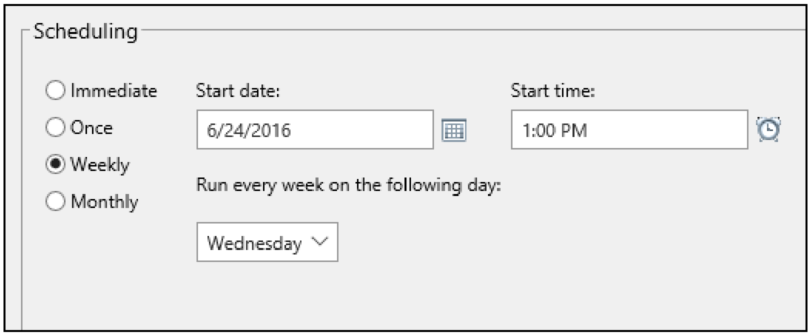
To Discover Assets:

1. From the Endpoint Security Console, select **Discover > Assets**.


Discover
Assets...
Assets and Install Agents...
Assets and Uninstall Agents...
Scan Now - Virus and Malware Scan

2. Follow the **Discover Assets** wizard to set up an Asset Discovery job.

   - After you've setup Endpoint Security, schedule a frequent, recurring scan to identify assets in your network.



Scheduling

○ Immediate
○ Once
● Weekly
○ Monthly

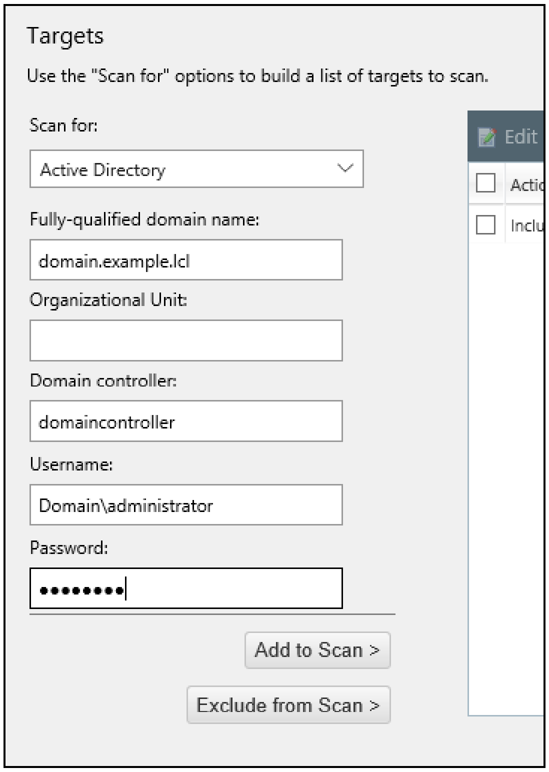
Start date: 6/24/2016

Start time: 1:00 PM

Run every week on the following day: Wednesday

   - After the number of endpoints managed by Endpoint Security stabilizes, replace the frequent scan with a less frequent scan to reduce scan bandwidth (for example, a monthly scan).

   - We recommend scanning your active directory so that endpoints don't have to be online for discovery. Use the picture below for examples of how to enter your information.



Targets

Use the "Scan for" options to build a list of targets to scan.

Scan for: Active Directory

Fully-qualified domain name: domain.example.lcl

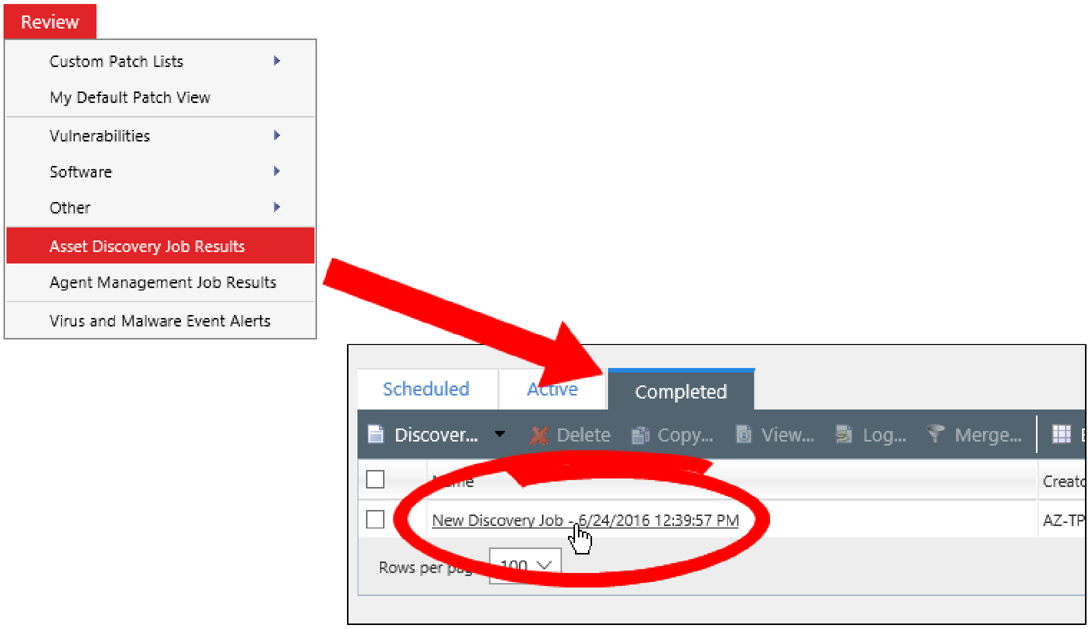
Organizational Unit:

Domain controller: domaincontroller

Username: Domain\administrator

Password: ••••••••

3. After your scan completes, you can view its result from **Review > Asset Discovery Job Results**.



The assets that the scan discovered are listed after you click-through the job link. You can use these results as a starting point to install the Endpoint Security Agent. Continue to the next section for more information.

Install Agents

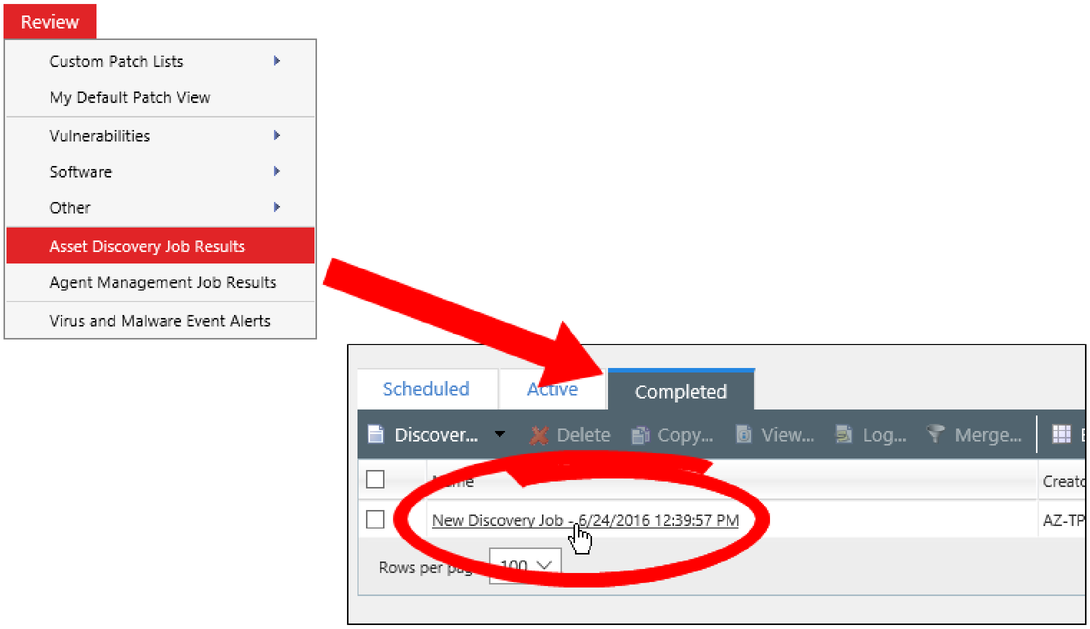
To patch the endpoints that you've discovered, they must have an Endpoint Security Agent and the Patch Module installed. Ensure that all endpoint assets in the network have this software installed.

If you haven't already installed this software using an automated method such as a group policy or login script, you can install it using Agent Management Jobs and the Add/Remove Modules feature.

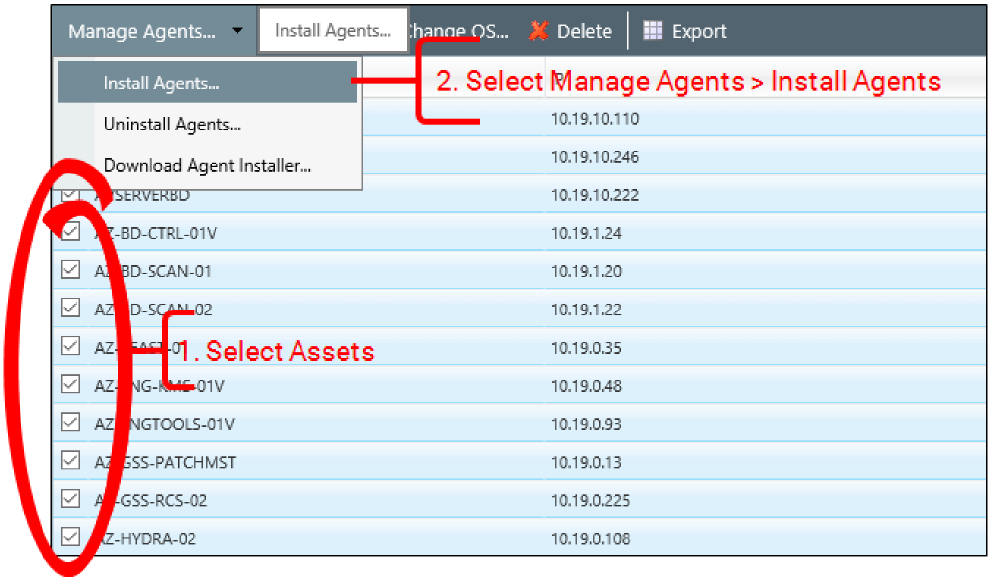
There are other methods available for install the Endpoint Security Agent. For additional information, refer to the Agent Install Guide available on the Ivanti Self-Service Portal .

To Install Agents:

1. Browse to the Discover Assets results from the previous section (select **Review > Asset Discovery Job Results** and select your discovery results).

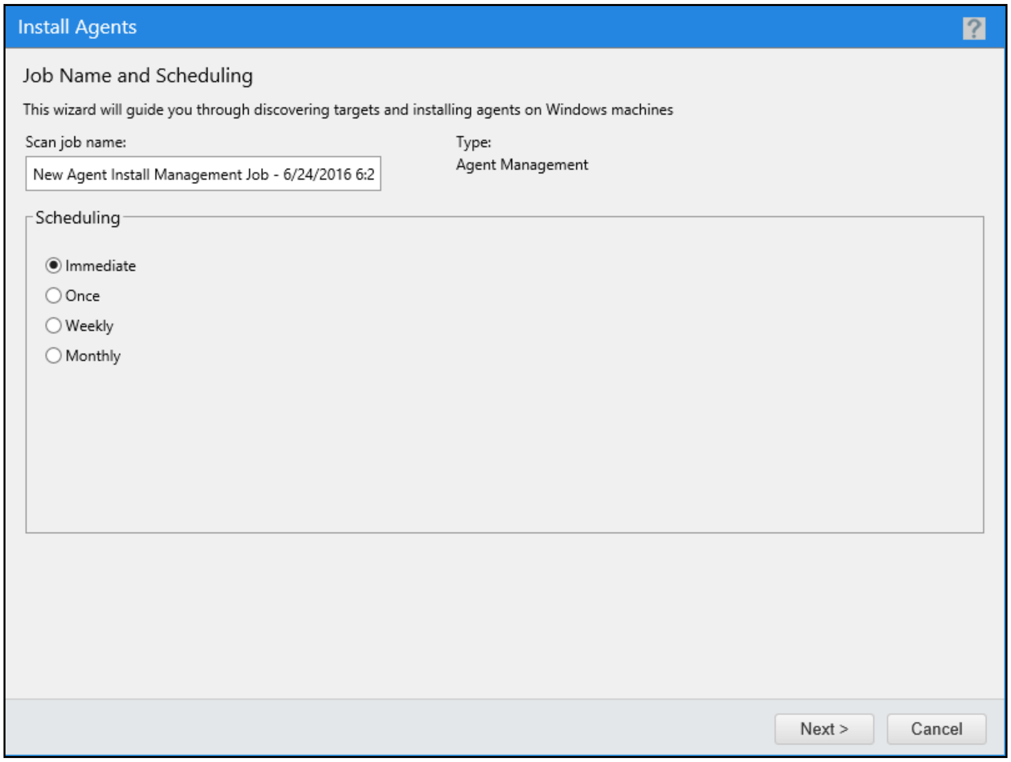


2. Select the assets that you want to install agents on, and then select **Manage Agents > Install Agents** from the toolbar.



		10.19.10.110
		10.19.10.246
☑	A SERVERBD	10.19.10.222
☑	Z-BD-CTRL-01V	10.19.1.24
☑	A BD-SCAN-01	10.19.1.20
☑	AZ D-SCAN-02	10.19.1.22
☑	AZ- -01	10.19.0.35
☑	AZ- NG-K -01V	10.19.0.48
☑	AZ NGTOOLS-01V	10.19.0.93
☑	AZ GSS-PATCHMST	10.19.0.13
☑	A -GSS-RCS-02	10.19.0.225
☑	Z-HYDRA-02	10.19.0.108

3. Configure the **Install Agents** job to run either once or immediately.



Install Agents

Job Name and Scheduling

This wizard will guide you through discovering targets and installing agents on Windows machines

Scan job name: New Agent Install Management Job - 6/24/2016 6:2

Type: Agent Management

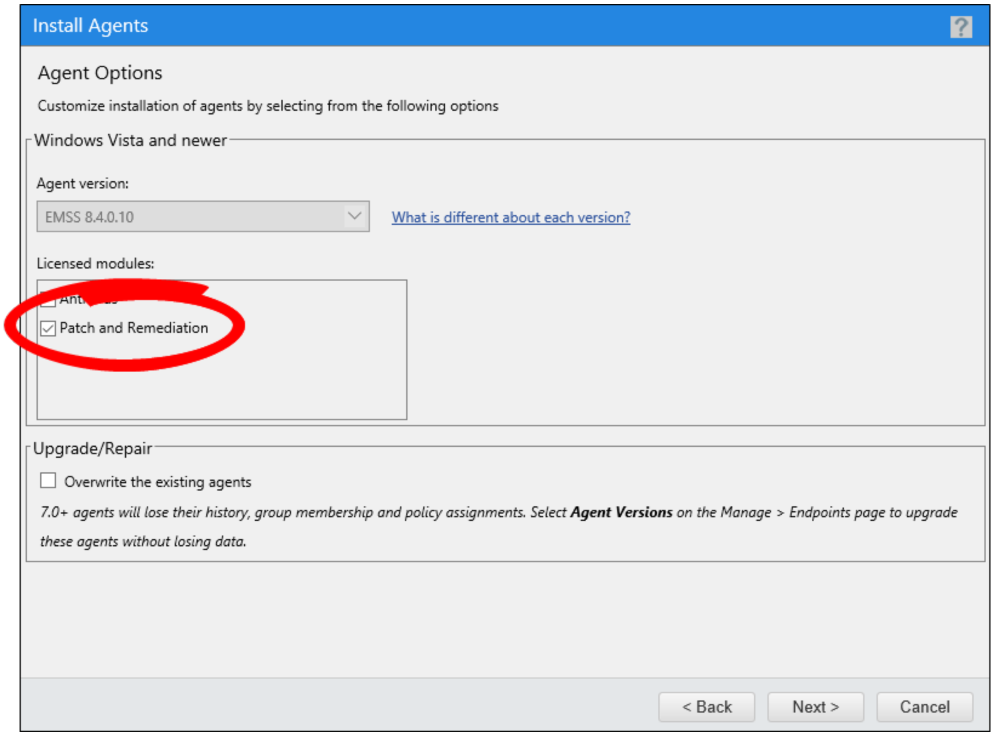
Scheduling

● Immediate
○ Once
○ Weekly
○ Monthly

Progress through the **Install Agents** wizard until you get to the **Agent Options** page.

The assets that you selected are automatically targeted for Endpoint Security Agent installation.

4. From the **Agent Options** page, make sure that the **Ivanti Patch and Remediation** module is selected. Then finish the wizard.



Install Agents

Agent Options

Customize installation of agents by selecting from the following options

Windows Vista and newer

Agent version: EMSS 8.4.0.10

What is different about each version?

Licensed modules:

☐ Antivirus

☑ Patch and Remediation

Upgrade/Repair

☐ Overwrite the existing agents

7.0+ agents will lose their history, group membership and policy assignments. Select ***Agent Versions*** *on the Manage > Endpoints page to upgrade these agents without losing data.*

5. Finish the **Install Agents** wizard. The Install Agents Job displays on the **Active** tab.
6. Wait for the Install Agents job to complete. When the job completes, it moves to the **Completed** tab.
7. Review the Job Results. Troubleshoot any endpoints that didn't complete the job successfully.

- We also recommend verifying agent installation using Ivanti Reporting Services if you have it installed:
  - Run **Endpoint Check-in** report. Select the current date as the **Last Contact Date on or before**.
  - Review the report to make sure communication is established between your endpoints and the Endpoint Security Server.
  - For endpoints that have not checked in, follow up with those endpoints for troubleshooting purposes.
- It may also be useful to verify the agent versions and operating systems of your endpoints using Ivanti Reporting Services, especially if you are planning on upgrading to a newer version of Endpoint Security:
  - Run the **Agent Version** and **Operating System Distribution** report, which displays a mix of agent versions, operating systems, and a detailed endpoint count.
  - Ensure that all desired endpoints are listed, have the expected agent version(s), and communicate properly.

The Endpoint Security Agent and the Patch Module are installed on the endpoints that you selected. Continue to the next section.

Create Workflows and Groups

You and your organization need to determine the best practices for patching your organization. You'll need to do some research about your organization to determine how you want to group them in Endpoint Security, as well as who will be doing that work, what policies are applied to those groups, etc.

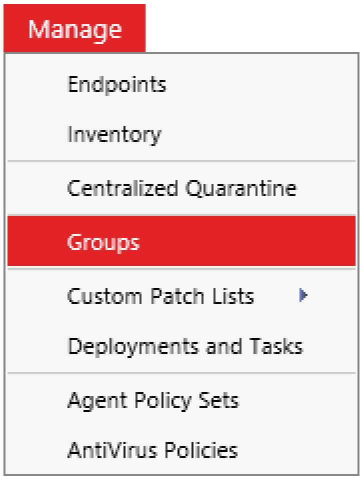
To Create Workflows and Groups:

1. Plan your Ivanti Patch and Remediation workflow by collecting the following information:
    - Survey your network topography. Categorize your endpoints based on criteria such as:
        - Endpoint Function: Is the endpoint a public facing server? A domain controller? Group endpoints that have a similar function together.
        - Endpoint Data: Endpoints containing sensitive data (like customer information) should be grouped together.
        - Attack Likelihood: Security threats target specific endpoints. Group these endpoints so that you can run more restrictive policies on them.
    - Plan patching policies:
        - Monitor endpoint operating hours. You need to determine when your endpoints are used for mission-critical tasks, and when they are safe to patch without negatively impacting your business.
    - Determine endpoint ownership. Each endpoint has various stakeholders attached to it, and you'll need to work with them throughout the patching process. Some examples include:
        - IT ownership: Who is the IT admin responsible for administration of the endpoint?
        - User: You need to keep workstation end users aware of administration tasks that impact them.
        - Management: You'll need to keep management informed of patching progress.
        - Business Owner: Which parts of the business are impacted if a server needs to be rebooted to apply patches? You need to communicate the patching schedule to the business owners to confirm that business operations are not adversely affected.

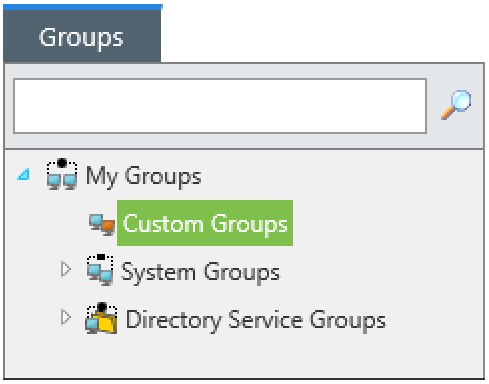
2. Create Custom Endpoint Security Groups. After surveying your network topography, use the results to recreate that topography in Endpoint Security.

   These groups should mimic how you plan to deploy patches to your organization. For example, you could create a test group (the first group that you'll deploy to test new patches) and a group for each department in your organization.

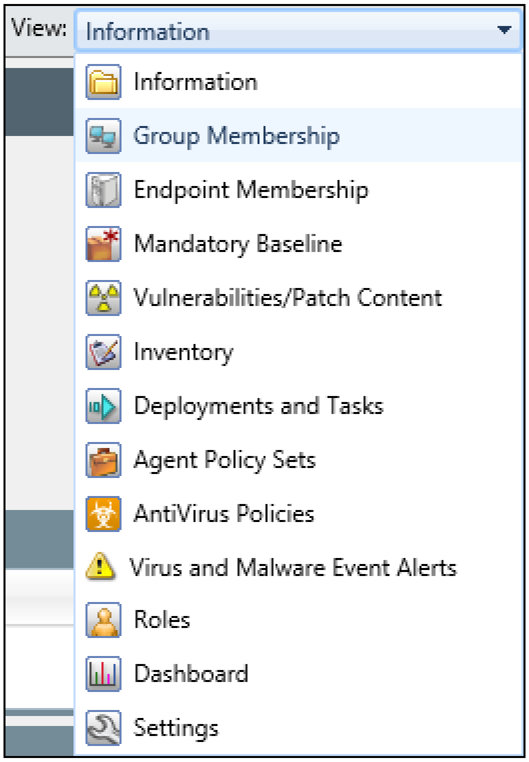
   a. From the Endpoint Security Console, select **Manage** > **Groups**.



   b. From the **Groups** browser, select **Custom Groups**.

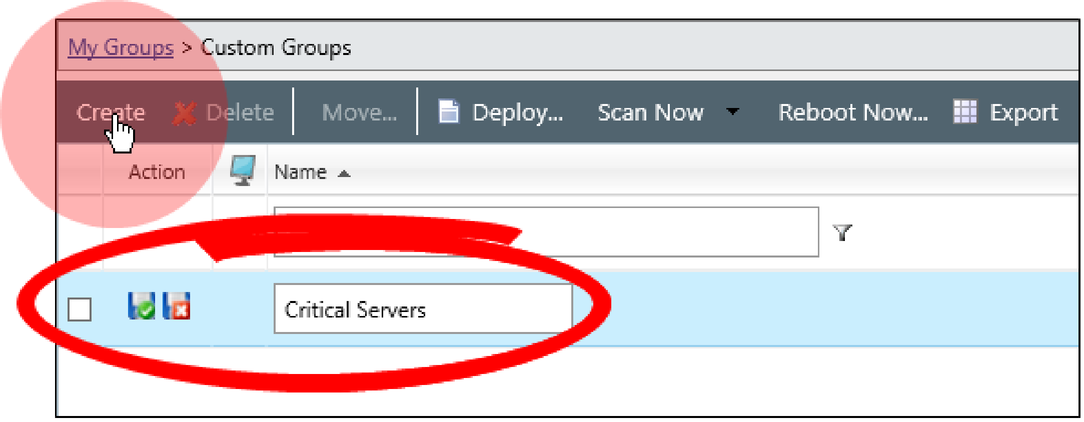


c. From the **View** list, select **Group Membership**.



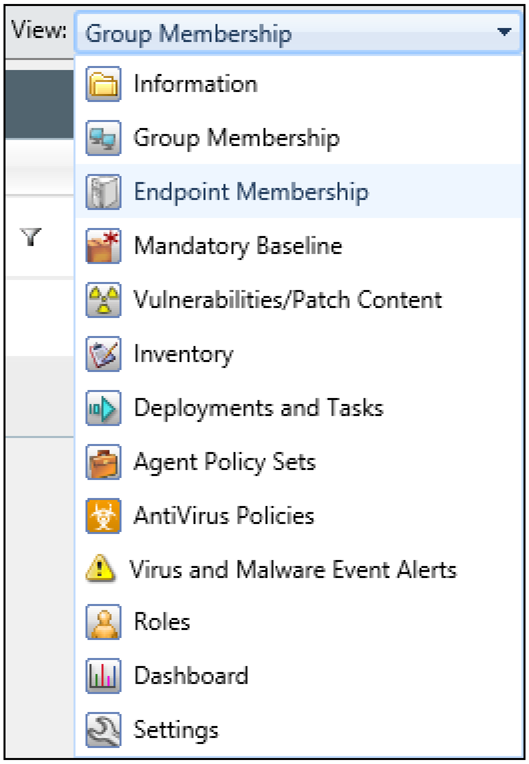
d. From the toolbar, click **Create**. Then name your new group something that describes it, and then click the **Save** icon.

Repeat steps a. through d. to create the number of groups needed to mimic your topography.

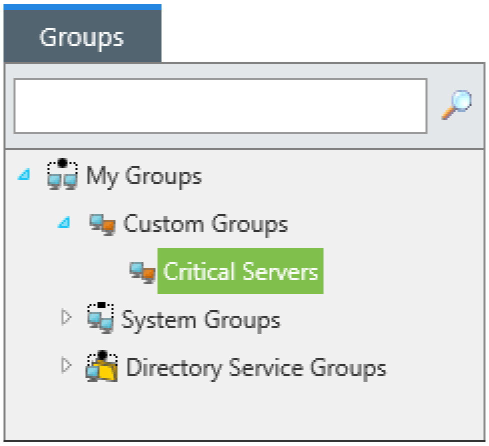


Critical Servers

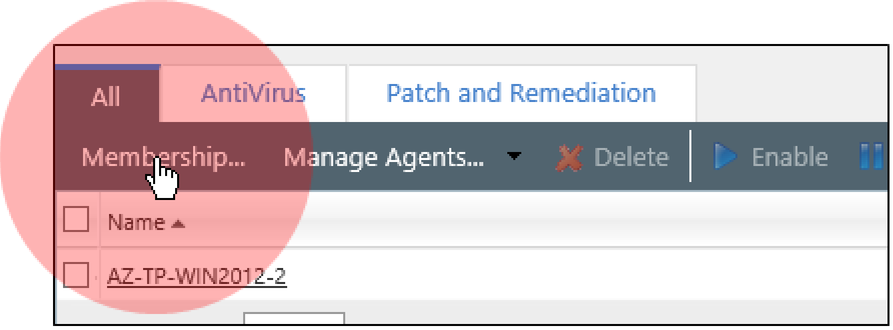
e. From the **View** list, select **Endpoint Membership**.



f. From the **Group** browser, select your new group.

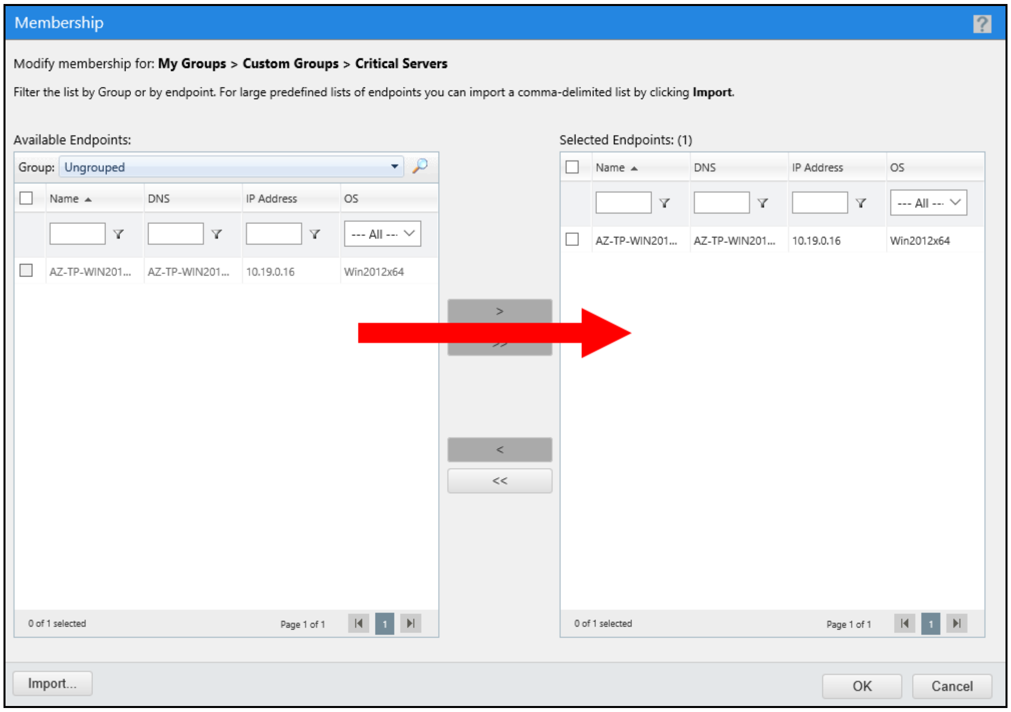


g. From the toolbar, click **Membership**.



h. Add the appropriate endpoints to the group.

Repeat steps e. through h. for each group you created.



Modify membership for: **My Groups** > **Custom Groups** > **Critical Servers**

Filter the list by Group or by endpoint. For large predefined lists of endpoints you can import a comma-delimited list by clicking **Import**.

Available Endpoints:

Group: Ungrouped

□	Name ▲	DNS	IP Address	OS
				--- All ---
□	AZ-TP-WIN201...	AZ-TP-WIN201...	10.19.0.16	Win2012x64

0 of 1 selected   Page 1 of 1

Selected Endpoints: (1)

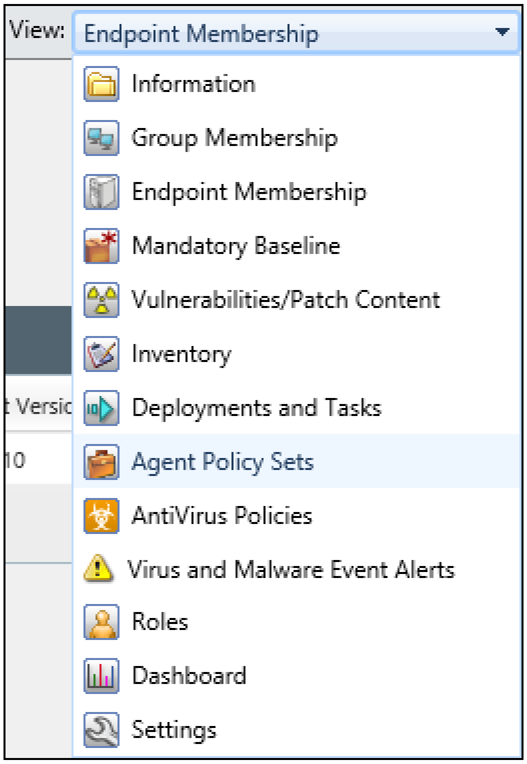
□	Name ▲	DNS	IP Address	OS
				--- All ---
□	AZ-TP-WIN201...	AZ-TP-WIN201...	10.19.0.16	Win2012x64

0 of 1 selected   Page 1 of 1

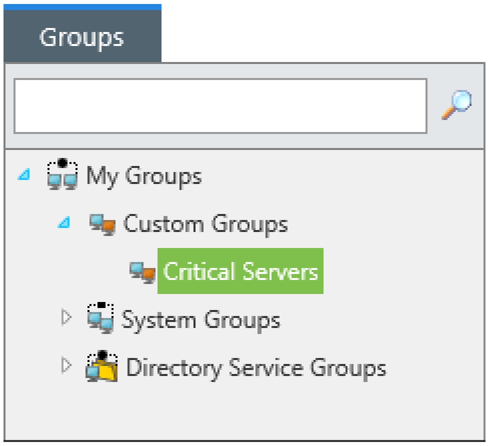
3. Create Agent Policy Sets.

   Agent Policy Sets are a collection of individual rules, called policies, that govern endpoint behavior. We're interested in one particular policy at the moment called Hours of Operation (or HOP). This policy determines when endpoints can communicate with the Endpoint Security Server and apply patches. You can also use Agent Policy Sets to determine other endpoint behaviors that we're going to skip over for now.

   a. From the **View** list, select **Agent Policy Sets**.

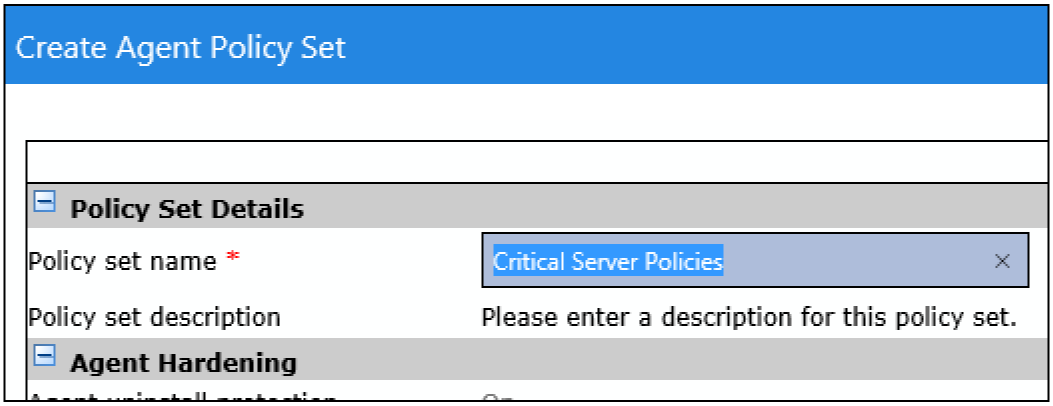


b. From the **Group** browser, make sure that one of your custom groups is selected.



c. From the toolbar, click **Create**.

d. Name the Policy Set.


Create Agent Policy Set

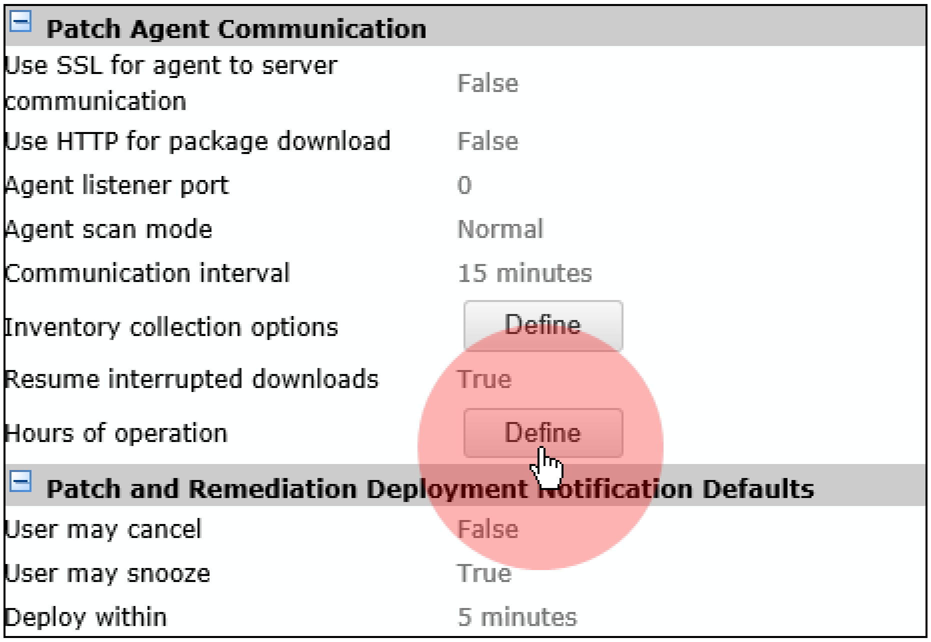
Policy Set Details

Policy set name * Critical Server Policies

Policy set description Please enter a description for this policy set.

Agent Hardening

e. Scroll down to **Patch Agent Communication**. Click the **Define** button next to **Hours of Operation**.



Patch Agent Communication

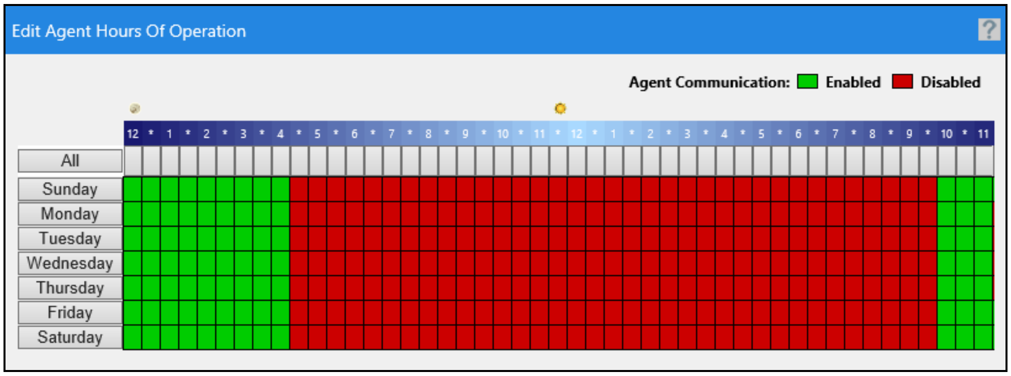
Use SSL for agent to server communication	False
Use HTTP for package download	False
Agent listener port	0
Agent scan mode	Normal
Communication interval	15 minutes
Inventory collection options	Define
Resume interrupted downloads	True
Hours of operation	Define

Patch and Remediation Deployment Notification Defaults

User may cancel	False
User may snooze	True
Deploy within	5 minutes

f. Use the dialog that opens to set Agent Hours of Operation. These options set the hours that endpoint patching is permitted. We recommend only patching workstations during hours that staff aren't working. For servers running business applications, check with your business owners to negotiate server hours of operation and whether there are any restrictions that must be followed.

You can use Endpoint Security: Wake on LAN to boot offline endpoints.



Edit Agent Hours Of Operation

Agent Communication: 🟩 Enabled 🟥 Disabled

g. Set any other policies that you want to set, and then click **Save**.

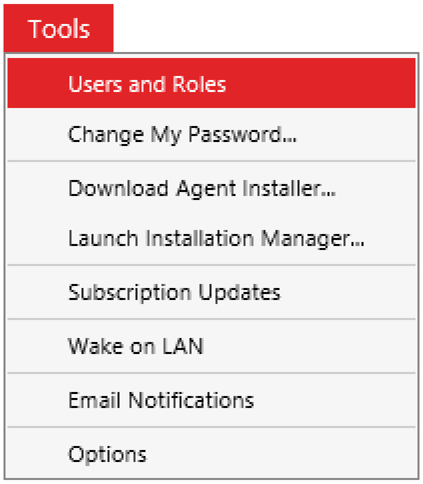
   For more information on what each policy does, refer to the following guides available on Product Documentation.

   - Endpoint Security User Guide
   - Ivanti Patch and Remediation and Remediation User Guide

h. Repeat steps a. through g. for each group that you created.

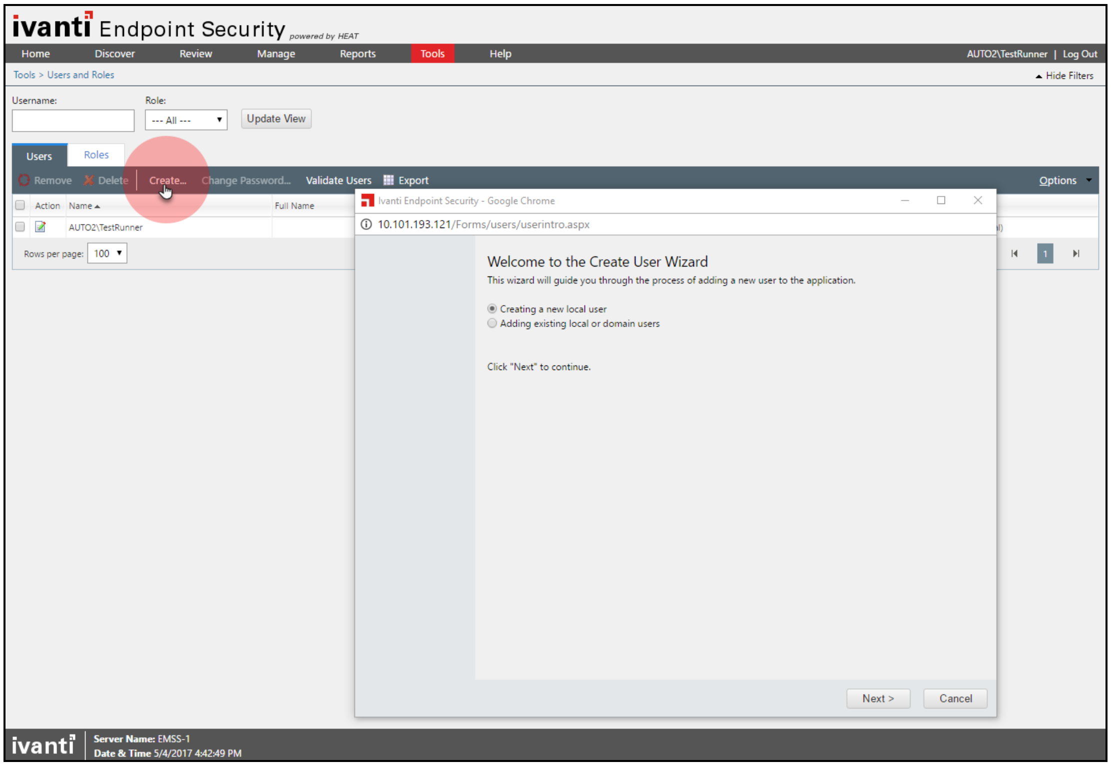
4. Create Endpoint Security Users. You likely won't be the only person in your organization using Endpoint Security. Therefore you'll need to create additional logins and assign them access rights for the different system features that the user is entitled to.

    1. From the Navigation Menu, select **Tools > Users and Roles**.



2. From the **Users** tab, click the **Create** button. Begin completing the dialog that opens to create a new user.

   We recommend adding domain users as new Endpoint Security users.



Welcome to the Create User Wizard

This wizard will guide you through the process of adding a new user to the application.

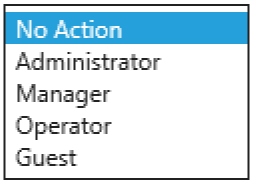
● Creating a new local user

○ Adding existing local or domain users

Click "Next" to continue.

.

3. When you get to the **User Roles** page (or **Create User** page, depending on whether you're adding a local or domain account), select a **User Role**, which grants the user access to different Endpoint Security pages and features.

   These roles include:

   - **Administrator**: Entitles the user to full access in the Endpoint Security Console.
   - **Manager**: Entitles the user to all Endpoint Security pages and features with the exception of Endpoint Security Server upgrades. Suitable for most IT administrators.
   - **Operator**: Entitles the user to basic Endpoint Security features and reports. Suitable for managers who want information about their network.
   - **User**: Entitles the user to view Endpoint Security pages, but not use them meaningfully. Suitable for end users.
   - Need another role not described here? Create a custom role from the **Roles** tab.
4. Finish and close the wizard.

Groups and Agent Policy Sets are created for your organization. Continue to the next section.

Create Test Group

You should never deploy patches to productiion endpoints without testing the patches first. You should first test them on some quarantined virtual machines or a few volunteer endpoints from each department. You should add these endpoints to a test group. This group should contain:

- A sample of endpoints that represent the different operating systems that you use.
- The major applications that your staff uses in your organization.

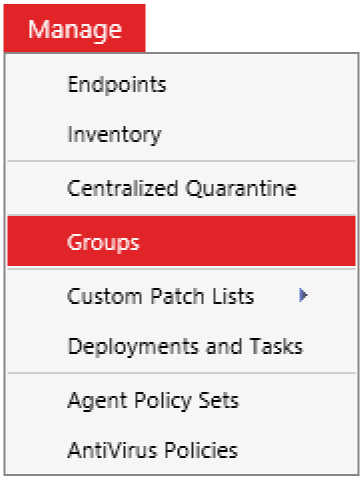
As a best practice, at least one endpoint from each major Endpoint Security group should be added to the test group.

For larger enterprise customers, we recommend setting up multiple test groups.

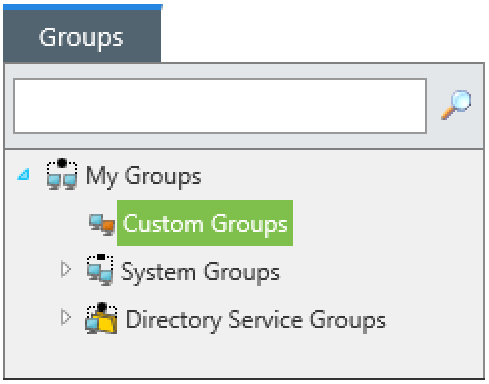
To Create a Test Group:

This process is very similar to step 2 in the previous topic. You're using the same process to create a group, but the intent is different—you're making a group for *testing* patch deployment, not the deployment itself.

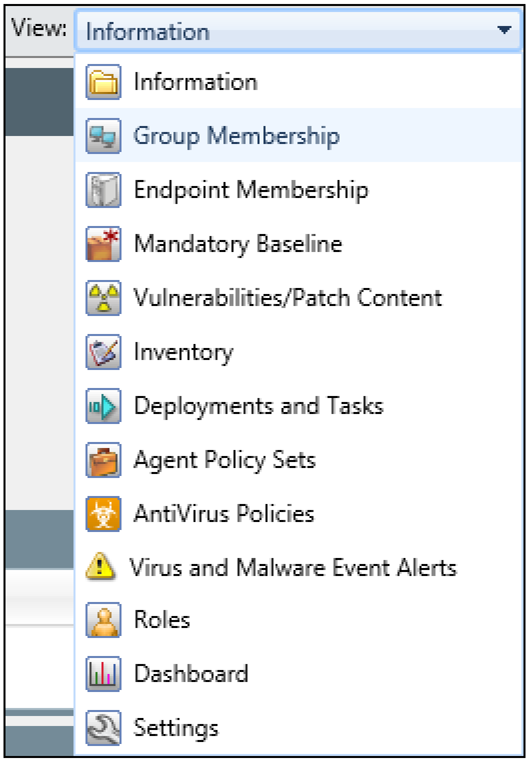
1. From the Endpoint Security Console, select **Manage** > **Groups**.



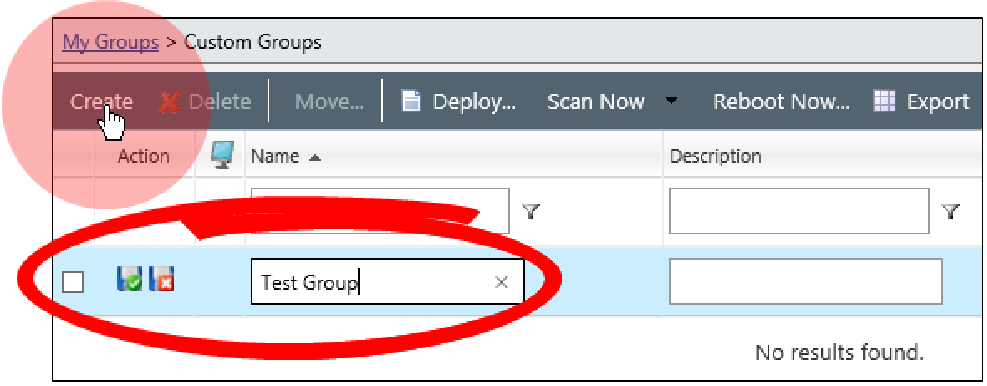
2. From the **Groups** browser, select **Custom Groups**.



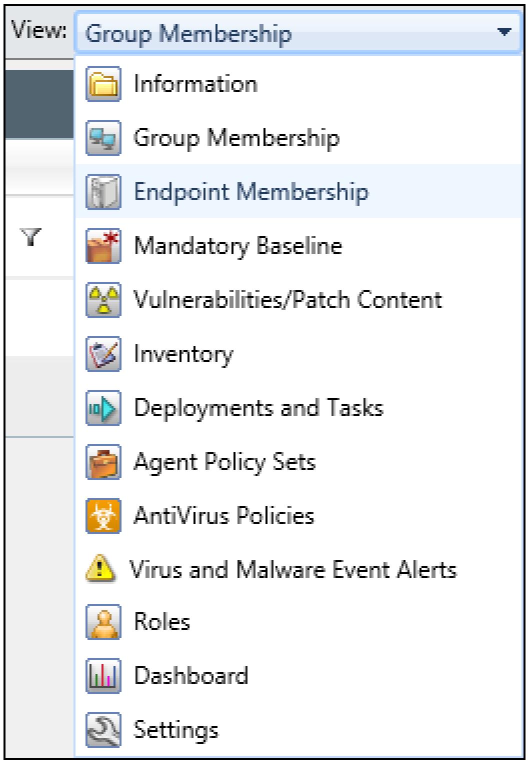
3. From the **View** list, select **Group Membership**.



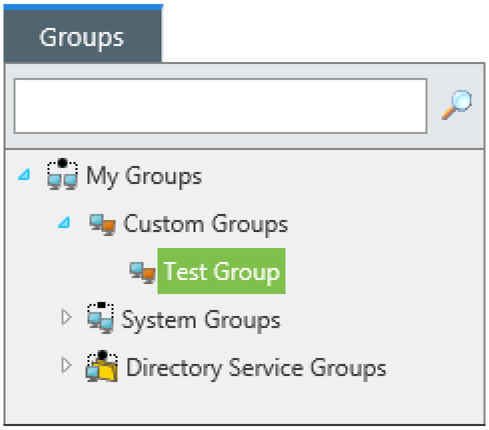
4. From the toolbar, click **Create**. Name your new group something like **Test Group**, and then click the **Save** icon.



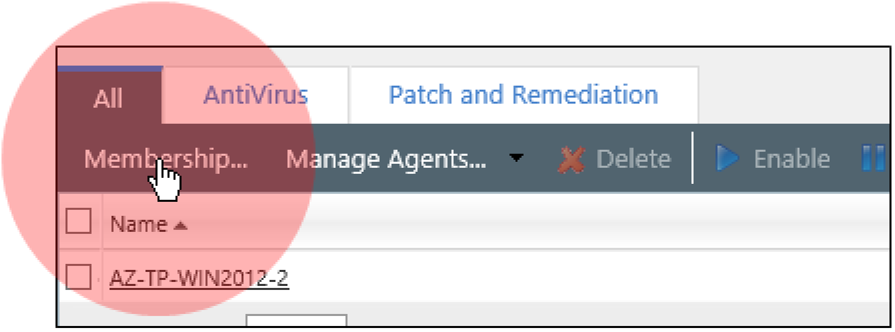
5. From the **View** list, select **Endpoint Membership**.



6. From the **Group** browser, select your test group.

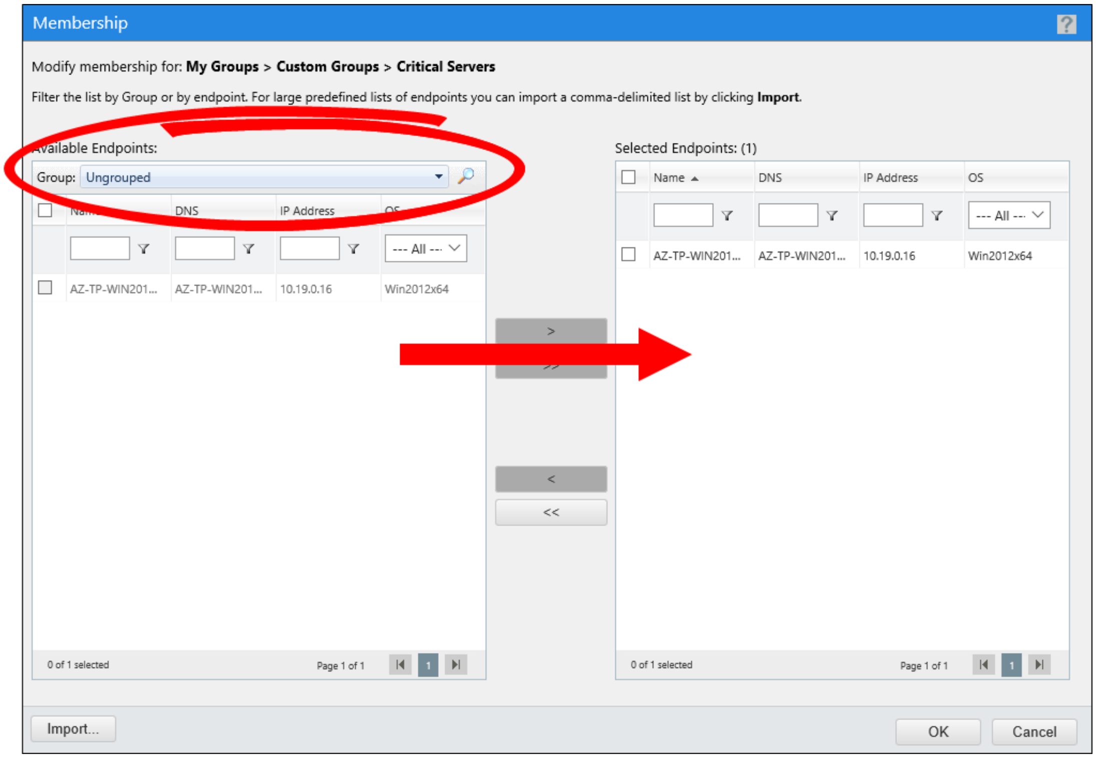


7. From the toolbar, click **Membership**.



8. Add one endpoint from each of your existing custom groups (or, select whatever test endpoints you need). Then click **OK**.

   Use the **Group** filter (circled below) to quickly and easily add an endpoint from each group.



Membership

Modify membership for: **My Groups > Custom Groups > Critical Servers**

Filter the list by Group or by endpoint. For large predefined lists of endpoints you can import a comma-delimited list by clicking **Import**.

Available Endpoints:

Group: Ungrouped

□	Name	DNS	IP Address	OS
□	AZ-TP-WIN201...	AZ-TP-WIN201...	10.19.0.16	Win2012x64

0 of 1 selected

Selected Endpoints: (1)

□	Name ▲	DNS	IP Address	OS
□	AZ-TP-WIN201...	AZ-TP-WIN201...	10.19.0.16	Win2012x64

0 of 1 selected

You've created a new test group and added endpoints to it. We'll revisit the concept of patch testing later in this guide, but for now, we're moving to a different topic.

You can always apply Agent Policy Sets to your test group.

Train Staff

Train applicable staff on vulnerability monitoring and remediation techniques.

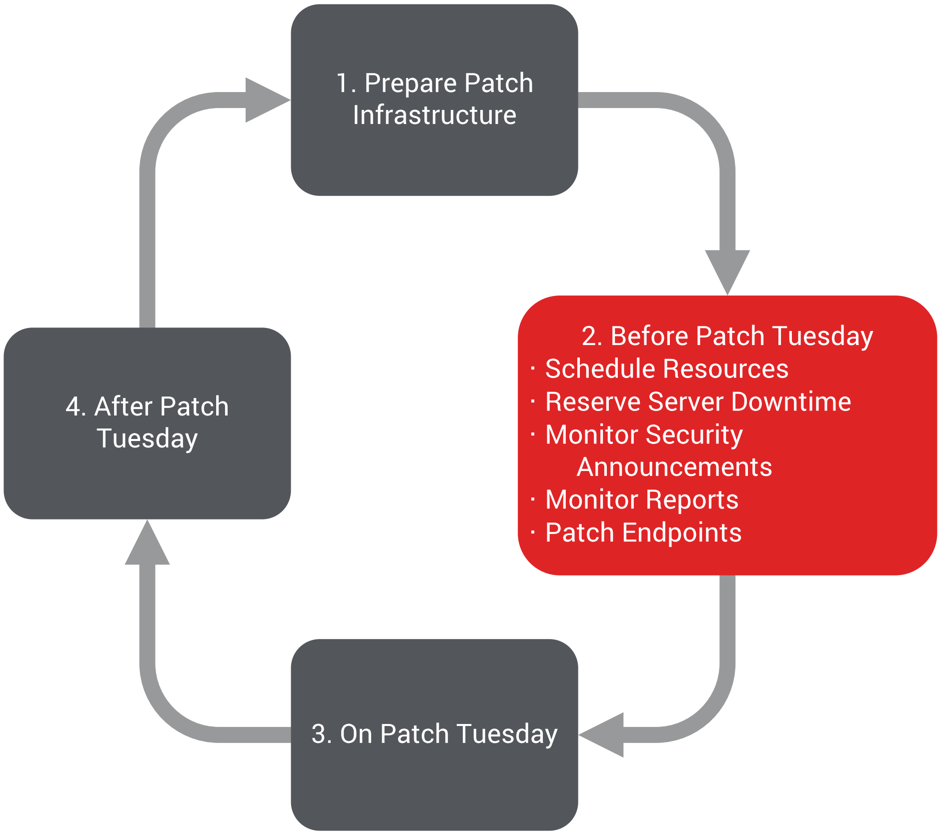
- At minimum, you should train your Endpoint Security administrators responsible for patching how to use Ivanti Patch and Remediation.
- As a best practice, you should create an internal resource where employees can learn more about the importance of keeping your organization fully patched.

  Use HEAT Software Academy resources to help train your staff.

Before Patch Tuesday

This section is about preparing the environment for the monthly patch deployment, including:

- Researching what content is planned for release by Microsoft and other application vendors
- Assessing the impact of those planned releases on your endpoints



In This Chapter:

Schedule Resources

Before Patch Tuesday, we recommend the following actions:

- Research the patch release schedules for third-party software vendors, such as Adobe, Apple, and Java.
- Review the patching needs of any internally developed applications and/or custom patches. Consider deploying these patches as part of the monthly patch cycle.

Reserve Server Downtime

Reserve a date and time to patch mission critical servers within 72 hours of Patch Tuesday releases. Inform stakeholders of the scheduled patching.

Monitor Security Announcements

Monitor security sites for discussions about vulnerabilities and potential zero-day exploits discovered by endpoint security experts.

Such sites include:

- Microsoft Security Response Center (MSRC)
- SANS Internet Storm Center
- National VulnerabilityDatabase (NVD)

You can configure Endpoint Security to send you emails when new patches are available from the Global Subscription Server.

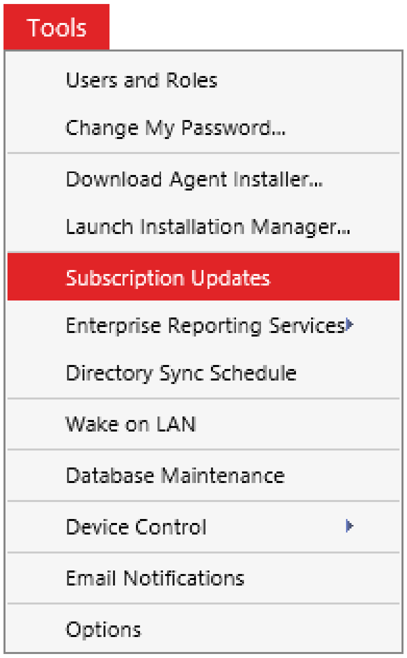
Monitor Reports

Leading up to Patch Tuesday, review the data available in Endpoint Security to make sure that:

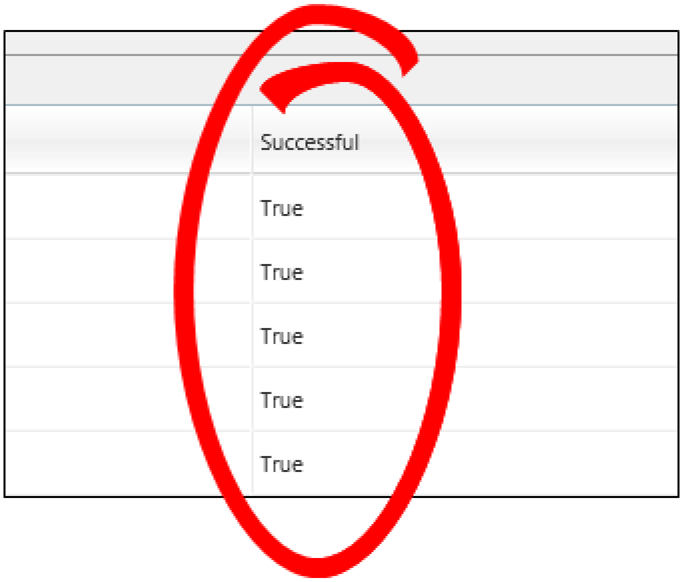
- Your Endpoint Security Server is communicating with the Global Subscription Server
- Your endpoints are communicating with the Endpoint Security Server

To Monitor Reports:

1. Confirm that Endpoint Security is communicating with the Global Subscription Server.
   a. From the Endpoint Security Console, select **Tools > Subscription Updates**.



b. Make sure that the recent entries in the **Subscription Service History** have completed successfully. Successful replications display a state of **True** in the **Successful** column.



	Successful
	True
	True
	True
	True
	True

If **False** is shown in any of the rows, troubleshoot to repair replication.

2. To confirm recent deployments and ongoing scanning within Endpoint Security, perform the following actions in Ivanti Reporting Services:
   - Run the operational report **Deployment Detail**
   - Select the group(s) that you are monitoring
   - Review success/failure results (Patched and Complete %)

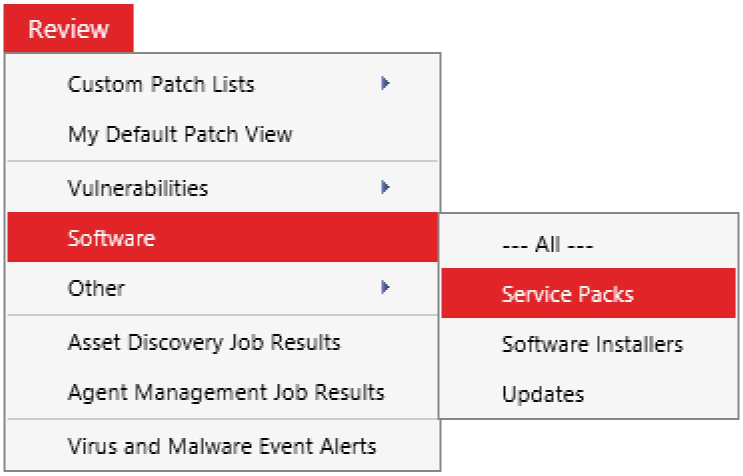
Patch Endpoints to Minimum Standard

Before your first Patch Tuesday, you should patch your endpoints to a minimum standard. Make sure that service packs, hotfixes, or rollups from prior months are installed on your endpoints.

If your endpoints don't already have this software installed, they likely don't meet the prerequisites to install the patches releases on Patch Tuesday. Therefore, if you have any endpoints that don't already have this software, deploy it to your endpoints.

To Patch Endpoints:

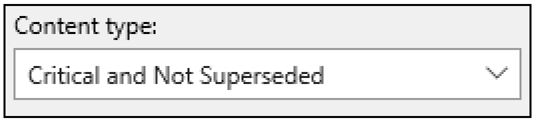
1. From the Endpoint Security Console, navigate to **Review** > **Software** > **Service Packs**.



2. Set the following filters (and any others that you want to set), and then click **Update View**:

- **Content type: Critical and Not Superseded**

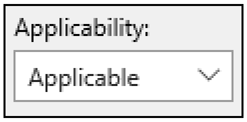
  This filter updates the page list with only patches that haven't been outdated by another patch.



Content type:
Critical and Not Superseded

- **Applicability: Applicable**

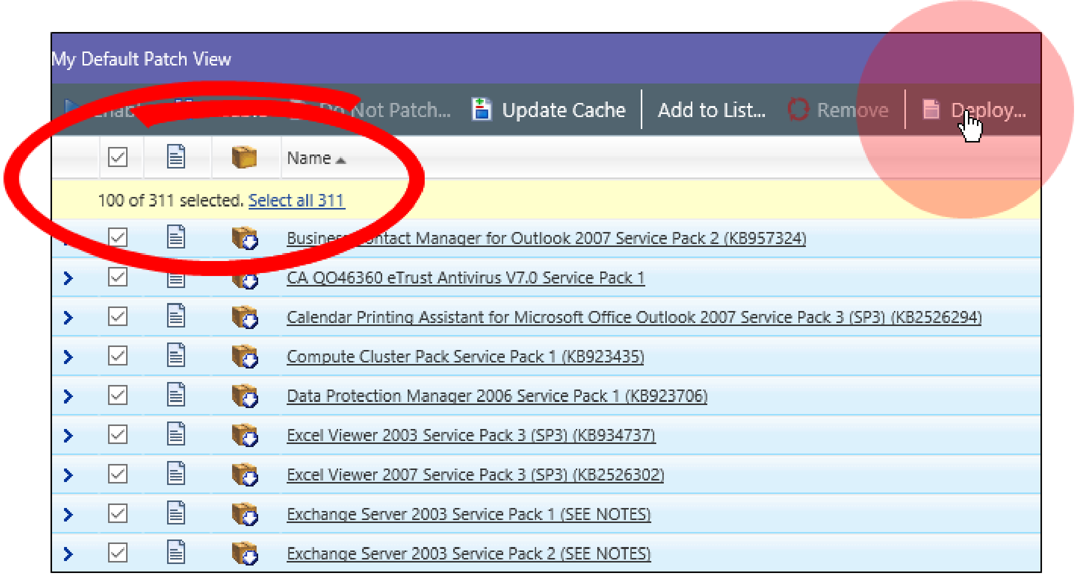
  This filter further reduces results so that only patches that apply to endpoints that you support are listed.



Applicability:
Applicable

3. Deploy the services packs that are listed to any endpoints that don't have them installed.

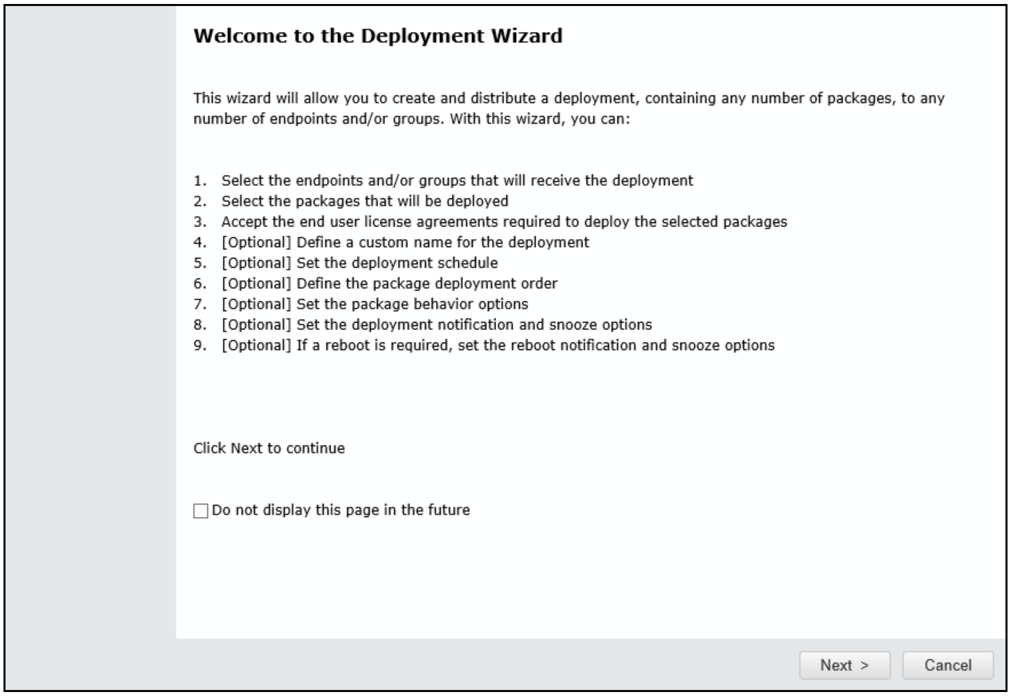
   Select all the service packs that are listed, and then click **Deploy**.



100 of 311 selected. Select all 311

☑	Name ▲
☑	Business Contact Manager for Outlook 2007 Service Pack 2 (KB957324)
☑	CA QO46360 eTrust Antivirus V7.0 Service Pack 1
☑	Calendar Printing Assistant for Microsoft Office Outlook 2007 Service Pack 3 (SP3) (KB2526294)
☑	Compute Cluster Pack Service Pack 1 (KB923435)
☑	Data Protection Manager 2006 Service Pack 1 (KB923706)
☑	Excel Viewer 2003 Service Pack 3 (SP3) (KB934737)
☑	Excel Viewer 2007 Service Pack 3 (SP3) (KB2526302)
☑	Exchange Server 2003 Service Pack 1 (SEE NOTES)
☑	Exchange Server 2003 Service Pack 2 (SEE NOTES)

4. Complete the **Deployment Wizard**.



Welcome to the Deployment Wizard

This wizard will allow you to create and distribute a deployment, containing any number of packages, to any number of endpoints and/or groups. With this wizard, you can:

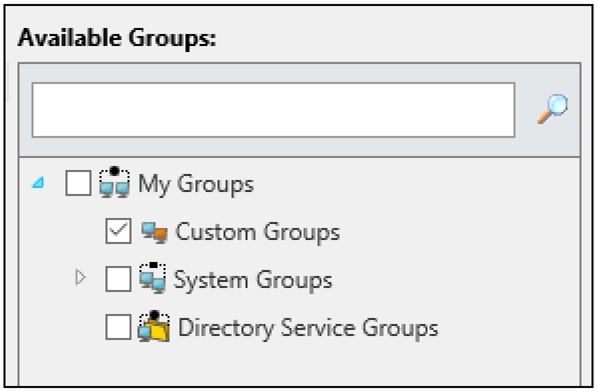
1. Select the endpoints and/or groups that will receive the deployment
2. Select the packages that will be deployed
3. Accept the end user license agreements required to deploy the selected packages
4. [Optional] Define a custom name for the deployment
5. [Optional] Set the deployment schedule
6. [Optional] Define the package deployment order
7. [Optional] Set the package behavior options
8. [Optional] Set the deployment notification and snooze options
9. [Optional] If a reboot is required, set the reboot notification and snooze options

Click Next to continue

□ Do not display this page in the future

A few tips for while you're completing the **Deployment Wizard**:

- Make sure you select all groups and endpoints that don't have the recently released service packs (and other software) installed. The easiest way to patch all these endpoints is to select the root **Custom Groups** object.



Available Groups:

- □ My Groups
  - ☑ Custom Groups
  - □ System Groups
  - □ Directory Service Groups

- Don't select any patches from the **Available Packages** page. You've already selected the patches you're deploying.
- Make sure you schedule the deployment after business hours.

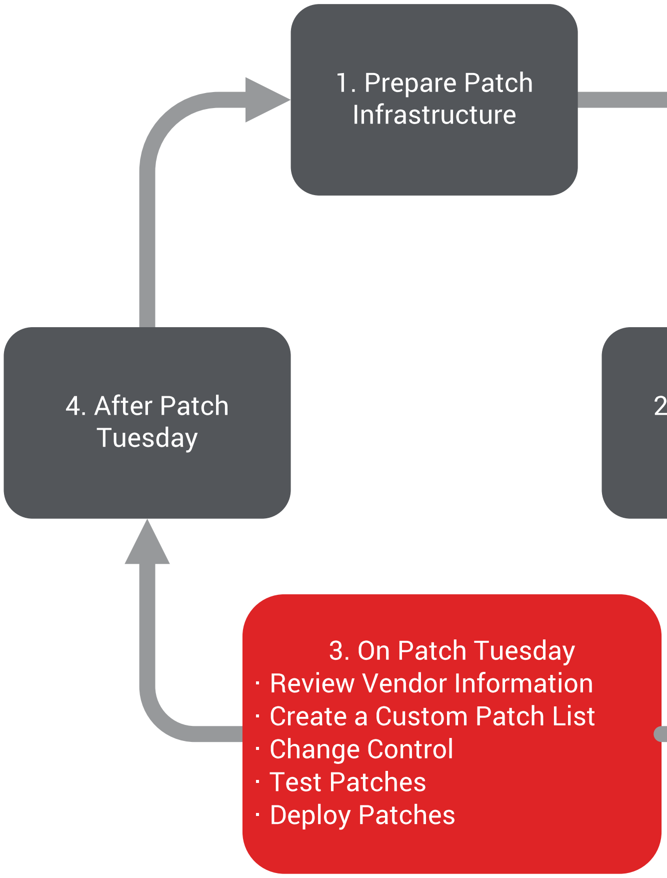
  - Don't finish the deployment without caching the patches first. Before you finish the Wizard, it will ask you if you want to deploy without caching the content. Always cache the content first, because this practice assures that the patches are installed in the proper order.

- The deployment is scheduled.
- The **Deployments and Tasks** page opens to your deployment.

  From this page you can monitor the deployment progress once it begins.

On Patch Tuesday

This section outlines the steps to prioritize the Security Patches released by Microsoft and other application vendors and to deploy those patches out to the machines managed in your environment.



In This Chapter:

Review Vendor Information

Microsoft and other vendors provide webinars, email alerts, and comprehensive online information on all new Patch Tuesday updates.

Important information for understanding the impact of Patch Tuesday on your environment includes:

- What is the bulletin severity rating?
- Is the vulnerability known/publicly disclosed at the time of release?
- Does the vendor know of any active exploits at the time of release?
- How easily can the vulnerability be exploited once the bulletin is been released?

Create a Custom Patch List

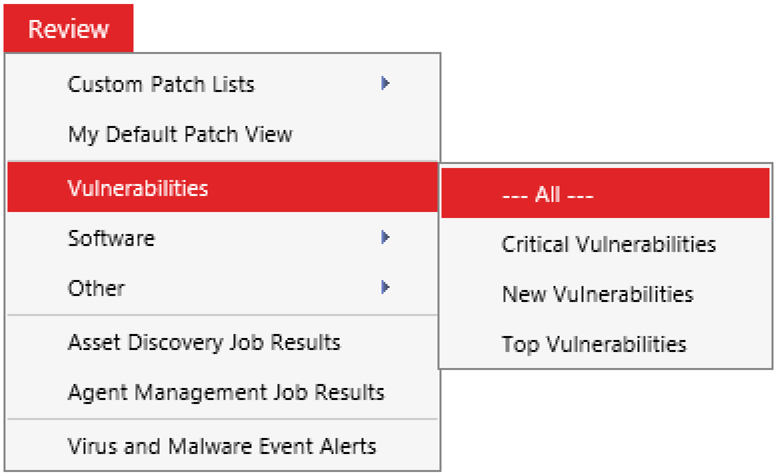
With the vendor information gathered in "Review Vendor Information" on the previous page, use patch impact (Critical, Important, etc.), asset risk, and asset value to create a Custom Patch List. A Custom Patch List is an object that you can add patches to and then deploy to your endpoints. These lists are a great way to keep a history of patches you've deployed each Patch Tuesday.

While creating a Custom Patch List, understand the applicability and impact of deploying these patches to your environment, especially critical machines. When making this assessment, consider:

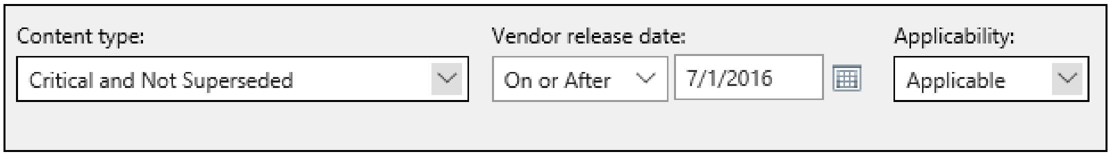
- Threat Level
- Known Active Exploits in the Wild
- Risk of Compromise
- Consequences of Compromise

To Create a Custom Patch List:

1. From the Endpoint Security Console, select **Review** > **Vulnerabilities** > **All**.



2. Set the patch filters to the following settings, and the click **Update View**:



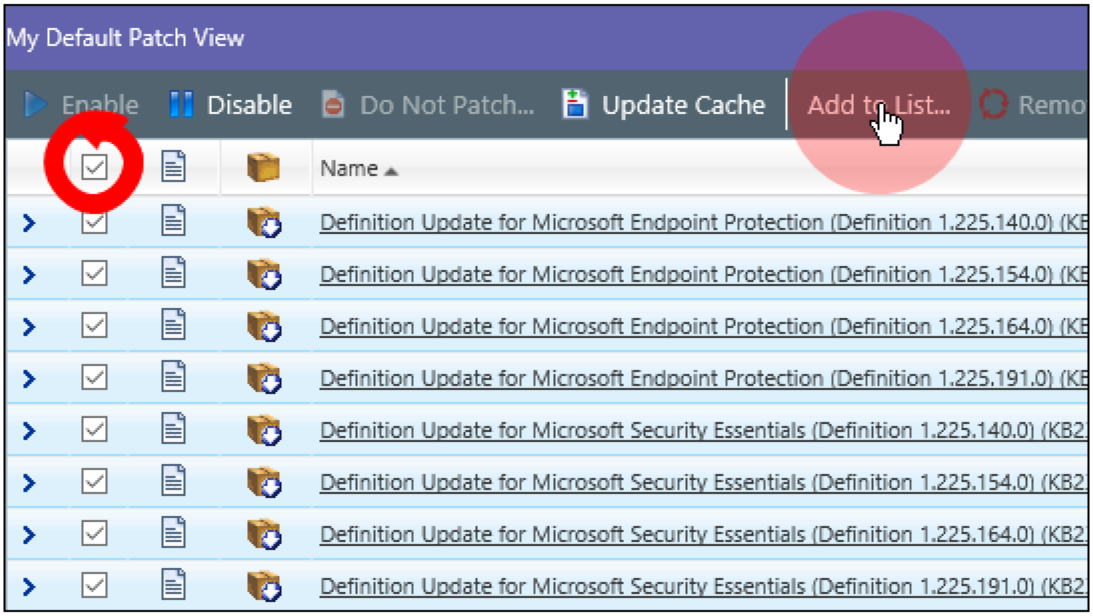
Content type: Critical and Not Superseded

Vendor release date: On or After 7/1/2016

Applicability: Applicable

- **Content type: Critical and Not Superseded**
- **Vendor release date: On or After the first day of the month**
- **Applicability: Applicable**

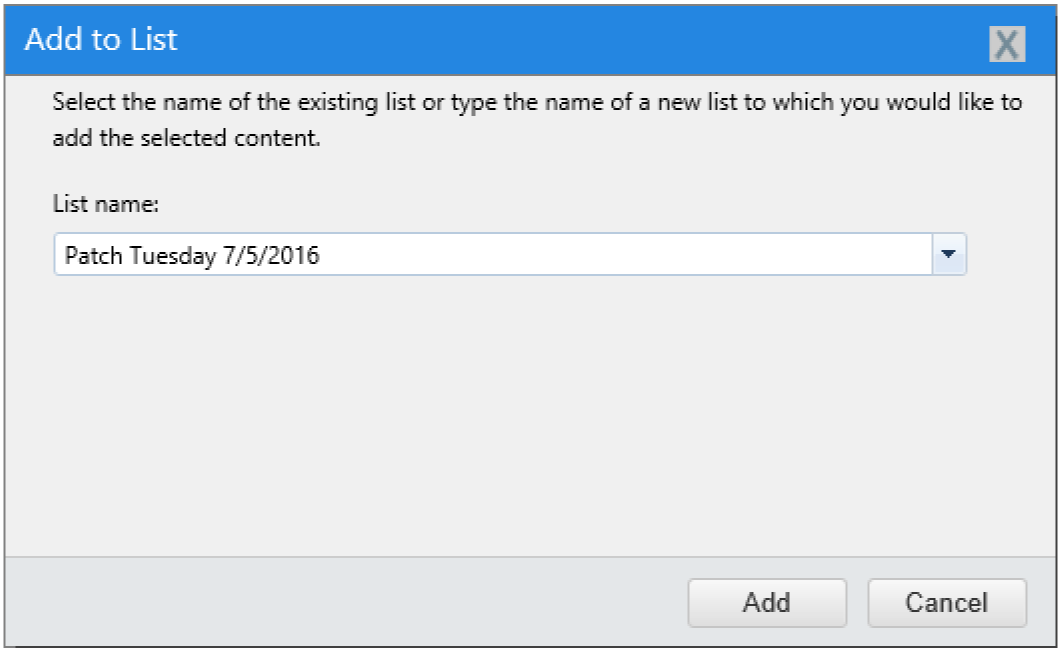
3. Select all patches on the page, and then click **Add to List**.



My Default Patch View

☑	Name ▲
☑	Definition Update for Microsoft Endpoint Protection (Definition 1.225.140.0) (KB
☑	Definition Update for Microsoft Endpoint Protection (Definition 1.225.154.0) (KB
☑	Definition Update for Microsoft Endpoint Protection (Definition 1.225.164.0) (KB
☑	Definition Update for Microsoft Endpoint Protection (Definition 1.225.191.0) (KB
☑	Definition Update for Microsoft Security Essentials (Definition 1.225.140.0) (KB2
☑	Definition Update for Microsoft Security Essentials (Definition 1.225.154.0) (KB2
☑	Definition Update for Microsoft Security Essentials (Definition 1.225.164.0) (KB2
☑	Definition Update for Microsoft Security Essentials (Definition 1.225.191.0) (KB2

4. From the **Add to List** dialog, enter a name for a new Custom Patch List. We recommend naming it **Patch Tuesday**, followed by the date. Then click **Add**.

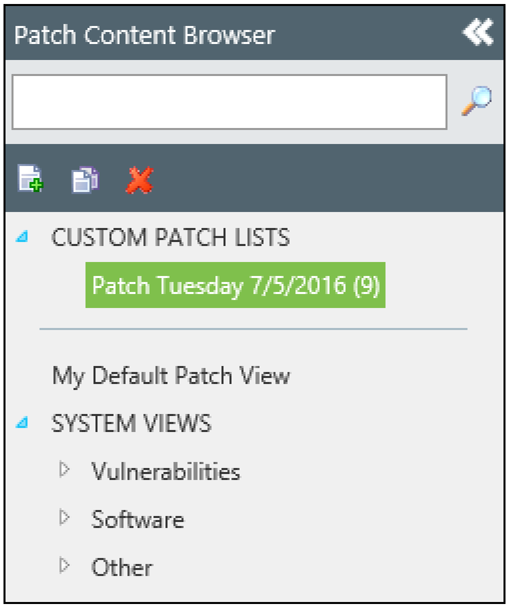


Add to List

Select the name of the existing list or type the name of a new list to which you would like to add the selected content.

List name: Patch Tuesday 7/5/2016

5. From the **Patch Content Browser**, select your new *Custom Patch List*.



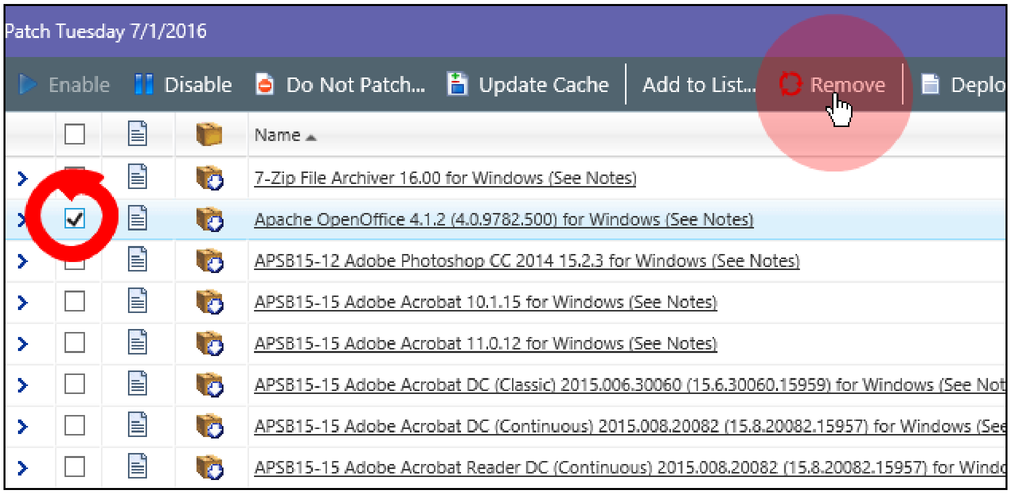
6. Research each patch in the list by performing a web search.

   Read the information about each patch at the vendor website. If you find any information that gives you a reason not to deploy the patch in your environment, remove the patch from your Custom Patch List.

- Click a patch link and then select the Information tab to view metadata for a patch.
- You can also view newly released Patch Tuesday patches by running the **Patch Release by Vendor** report available within Ivanti Reporting Services.

  This report lists all Patch Tuesday patches, and whether they apply to your endpoints. It provides:

  - An overview of patch severities
  - The expected workload for the monthly Patch Tuesday release
  - The patch status for your organization



	Name
□	7-Zip File Archiver 16.00 for Windows (See Notes)
☑	Apache OpenOffice 4.1.2 (4.0.9782.500) for Windows (See Notes)
□	APSB15-12 Adobe Photoshop CC 2014 15.2.3 for Windows (See Notes)
□	APSB15-15 Adobe Acrobat 10.1.15 for Windows (See Notes)
□	APSB15-15 Adobe Acrobat 11.0.12 for Windows (See Notes)
□	APSB15-15 Adobe Acrobat DC (Classic) 2015.006.30060 (15.6.30060.15959) for Windows (See Not
□	APSB15-15 Adobe Acrobat DC (Continuous) 2015.008.20082 (15.8.20082.15957) for Windows (See
□	APSB15-15 Adobe Acrobat Reader DC (Continuous) 2015.008.20082 (15.8.20082.15957) for Windo

Your Custom Patch List is created, and the patches from Patch Tuesday are added to it. Continue to the next section.

Change Control

Follow any internal plans and approval processes for patch deployment. For example, you may have stricter standards for patching server endpoints than desktop endpoints to minimize service interruptions.

Test Patches

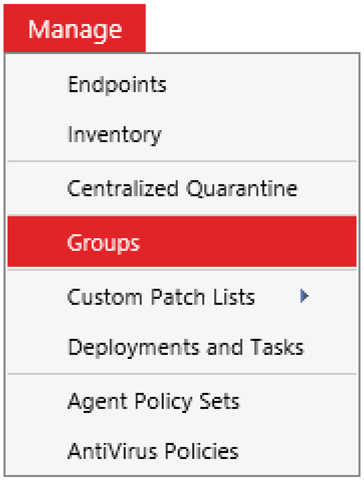
Before deploying your Custom Patch List to the various groups that you've created, you need to test them. Testing each patch is vital for finding different software conflicts. By testing your patches, you can discover issues that they cause and confine those problems to a small sample size of endpoints and not your entire organization!

- Automated deployment without testing is risky and not advised. Be certain to test the patch in each environment of your previously defined groups and deploy the patches in phases.
- Pay special attention to any potential impact to custom-developed, internal applications, especially when deploying Java updates.

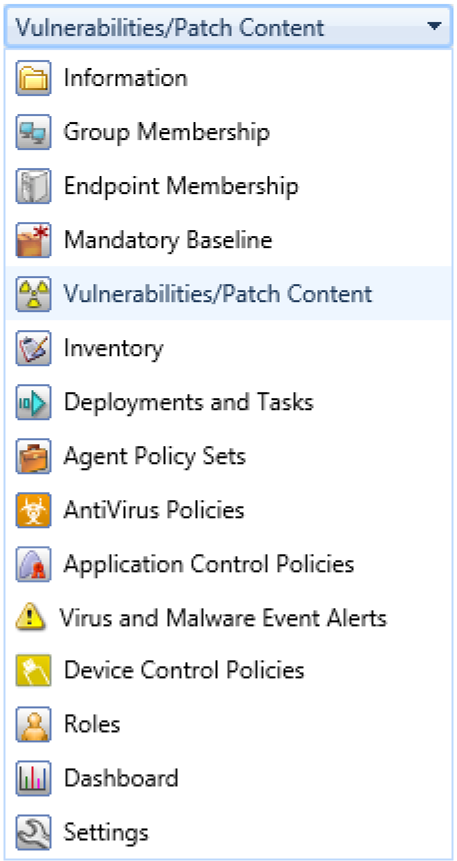
If you have a shortage of time or resources on Patch Tuesday, browse the Ivanti Patch Tuesday page for information on Patch Tuesday patches. This practice is a great way to discover patch issues without testing.

To Test Patches:

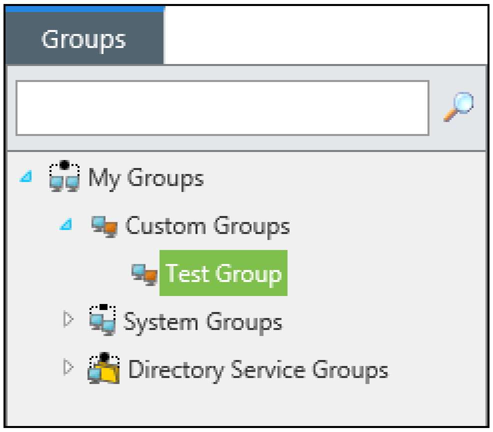
1. From the Navigation Menu, select **Manage > Groups**.



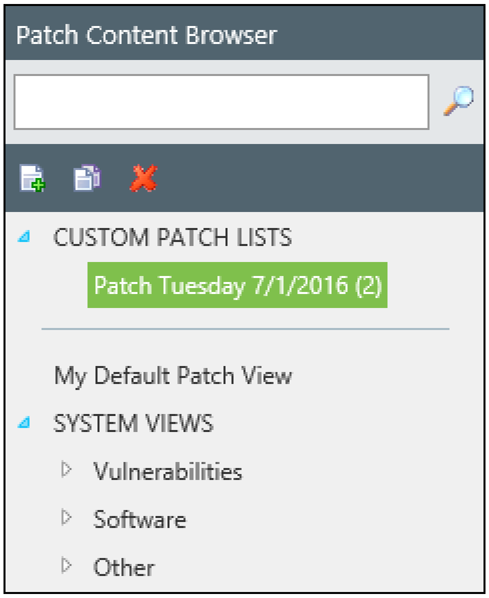
2. Make sure that the **Vulnerabilities/Patch Content** view is selected.



3. From the **Group** browser, select your test group.



4. From the **Patch Content Browser**, select your custom patch list.

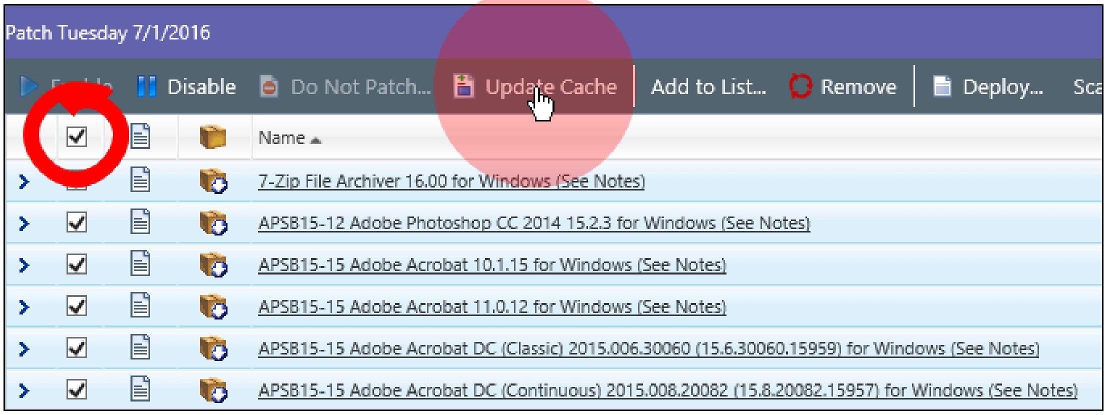


Patch Content Browser

- CUSTOM PATCH LISTS
  - Patch Tuesday 7/1/2016 (2)
- My Default Patch View
- SYSTEM VIEWS
  - Vulnerabilities
  - Software
  - Other

5. Select all patches in the list, and then click **Update Cache**.

   Updating the cache downloads the patches from the cloud to your local Endpoint Security Server. Caching patches to your Endpoint Security Server increases deployment speed and optimizes deployment order.



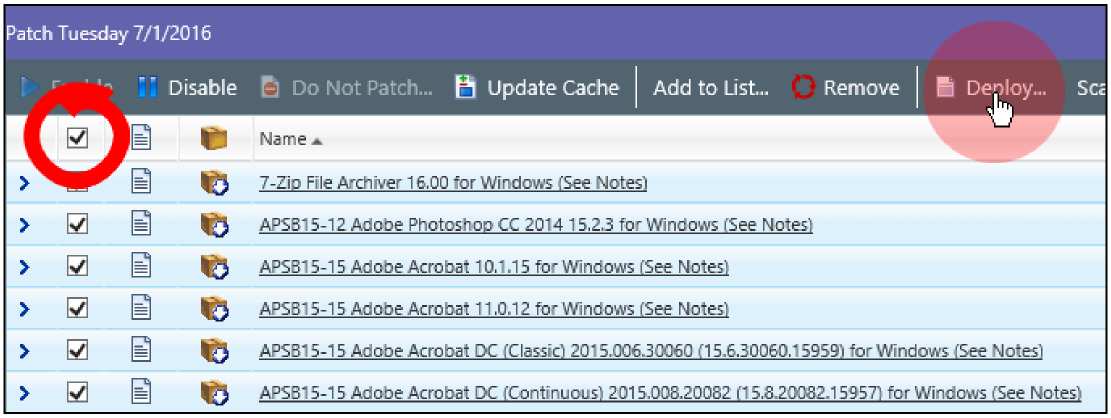
Patch Tuesday 7/1/2016

☑	Name ▲
☑	7-Zip File Archiver 16.00 for Windows (See Notes)
☑	APSB15-12 Adobe Photoshop CC 2014 15.2.3 for Windows (See Notes)
☑	APSB15-15 Adobe Acrobat 10.1.15 for Windows (See Notes)
☑	APSB15-15 Adobe Acrobat 11.0.12 for Windows (See Notes)
☑	APSB15-15 Adobe Acrobat DC (Classic) 2015.006.30060 (15.6.30060.15959) for Windows (See Notes)
☑	APSB15-15 Adobe Acrobat DC (Continuous) 2015.008.20082 (15.8.20082.15957) for Windows (See Notes)

6. Wait for the patches to cache. The icons in the 📦 column indicate caching progress.

   - ⏬: This icon indicates that the patch is still caching. Keep waiting.
   - 📦: This icon indicates that the patch has finished caching. Wait for all patches in the Custom Patch List to display this icon before continuing to the next step.

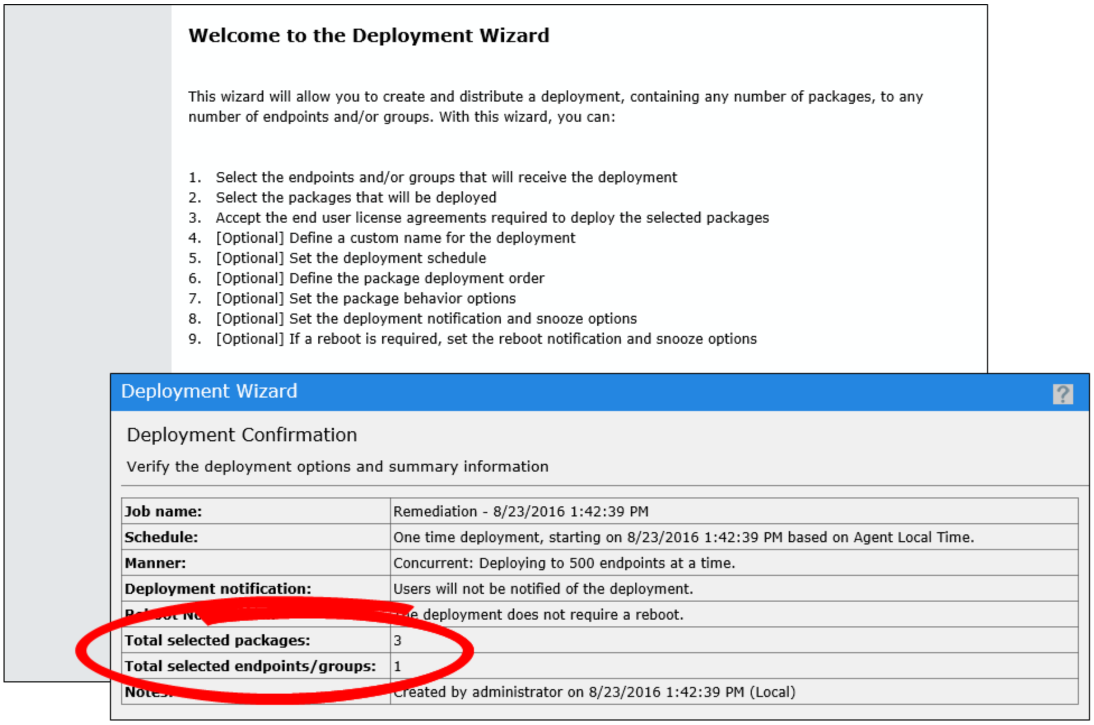
7. Select all patches listed, and then click **Deploy**.



	☑			Name ▲
>				7-Zip File Archiver 16.00 for Windows (See Notes)
>	☑			APSB15-12 Adobe Photoshop CC 2014 15.2.3 for Windows (See Notes)
>	☑			APSB15-15 Adobe Acrobat 10.1.15 for Windows (See Notes)
>	☑			APSB15-15 Adobe Acrobat 11.0.12 for Windows (See Notes)
>	☑			APSB15-15 Adobe Acrobat DC (Classic) 2015.006.30060 (15.6.30060.15959) for Windows (See Notes)
>	☑			APSB15-15 Adobe Acrobat DC (Continuous) 2015.008.20082 (15.8.20082.15957) for Windows (See Notes)

8. Complete the **Deployment Wizard**.

When you get to the **Deployment Confirmation** page, make sure that number of selected packages and endpoints/groups is what you expect.



Welcome to the Deployment Wizard

This wizard will allow you to create and distribute a deployment, containing any number of packages, to any number of endpoints and/or groups. With this wizard, you can:

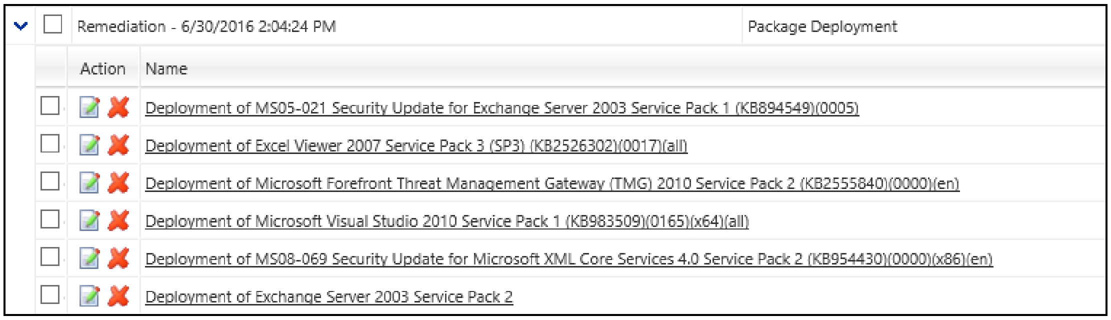
1. Select the endpoints and/or groups that will receive the deployment
2. Select the packages that will be deployed
3. Accept the end user license agreements required to deploy the selected packages
4. [Optional] Define a custom name for the deployment
5. [Optional] Set the deployment schedule
6. [Optional] Define the package deployment order
7. [Optional] Set the package behavior options
8. [Optional] Set the deployment notification and snooze options
9. [Optional] If a reboot is required, set the reboot notification and snooze options

Deployment Confirmation

Verify the deployment options and summary information

Job name:	Remediation - 8/23/2016 1:42:39 PM
Schedule:	One time deployment, starting on 8/23/2016 1:42:39 PM based on Agent Local Time.
Manner:	Concurrent: Deploying to 500 endpoints at a time.
Deployment notification:	Users will not be notified of the deployment.
[illegible]	[illegible] deployment does not require a reboot.
Total selected packages:	3
Total selected endpoints/groups:	1
Notes:	Created by administrator on 8/23/2016 1:42:39 PM (Local)

9. Navigate to **Manage** > **Deployments and Tasks**. Expand your Test Deployment.



□		Remediation - 6/30/2016 2:04:24 PM	Package Deployment
	Action	Name	
□	✎ ✗	Deployment of MS05-021 Security Update for Exchange Server 2003 Service Pack 1 (KB894549)(0005)	
□	✎ ✗	Deployment of Excel Viewer 2007 Service Pack 3 (SP3) (KB2526302)(0017)(all)	
□	✎ ✗	Deployment of Microsoft Forefront Threat Management Gateway (TMG) 2010 Service Pack 2 (KB2555840)(0000)(en)	
□	✎ ✗	Deployment of Microsoft Visual Studio 2010 Service Pack 1 (KB983509)(0165)(x64)(all)	
□	✎ ✗	Deployment of MS08-069 Security Update for Microsoft XML Core Services 4.0 Service Pack 2 (KB954430)(0000)(x86)(en)	
□	✎ ✗	Deployment of Exchange Server 2003 Service Pack 2	

10. Review the deployment outcome after it finishes.

    - If a patch deploys successfully to all endpoints (as indicated by the ✓ icon), then the patch is safe to deploy to your organization.
    - If a patch does not deploy successfully to all endpoints (as indicated by the ✗ icon), you should not deploy the patch to your organization. Investigate why the patch is not deploying successfully, and then take one of the following actions:
        - Fix the problem.
        - If you can't fix the problem and the patch isn't successfully deploying to a large number of endpoints, consider removing it from the Custom Patch List.
        - If you can't fix the problem and the patch isn't successfully deploying to a few endpoints, you can mark it Do Not Patch for those endpoints. Do Not Patch is a state that exempts selected endpoints from receiving deployment of that patch.

The Patch Tuesday patches are tested. After confirming all patches are functioning as intended (or dealt with if functioning incorrectly), begin rolling the patches out. See the next section for more details.

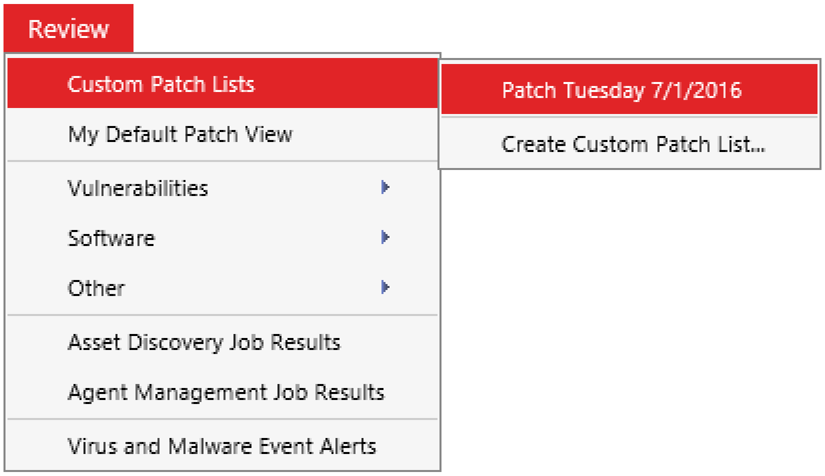
Deploy Patches

Now that you've tested your Patch Tuesday Custom Patch List and dealt with problematic patches, you can begin rolling the Custom Patch List out to your environment.

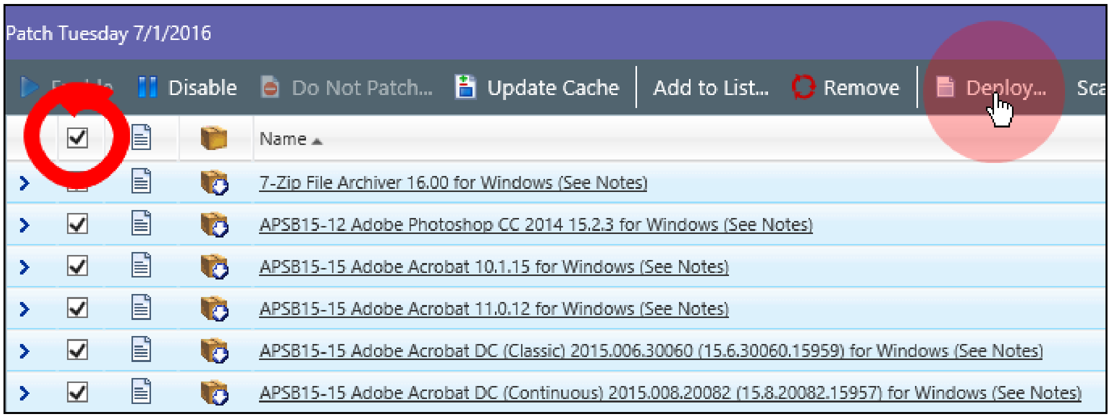
- Stage deployments by system groups and prioritization. Start with smaller, low-risk groups, and validate that no problems occur, and then work your way to larger and higher-risk areas of the network.
- As a best practice, and especially if your servers have a limited maintenance window, it is recommended to cache all the patch content before deployment.
- If deployments are scheduled off-hours, take advantage of Wake-on-LAN settings to wake up any powered-down endpoints and ensure that they receive the content.

To Deploy Patches:

1. From the Navigation Menu, select **Review** > **Custom Patch List** > ***Your Patch Tuesday List***.


Review
Custom Patch Lists
My Default Patch View
Vulnerabilities
Software
Other
Asset Discovery Job Results
Agent Management Job Results
Virus and Malware Event Alerts
Patch Tuesday 7/1/2016
Create Custom Patch List...

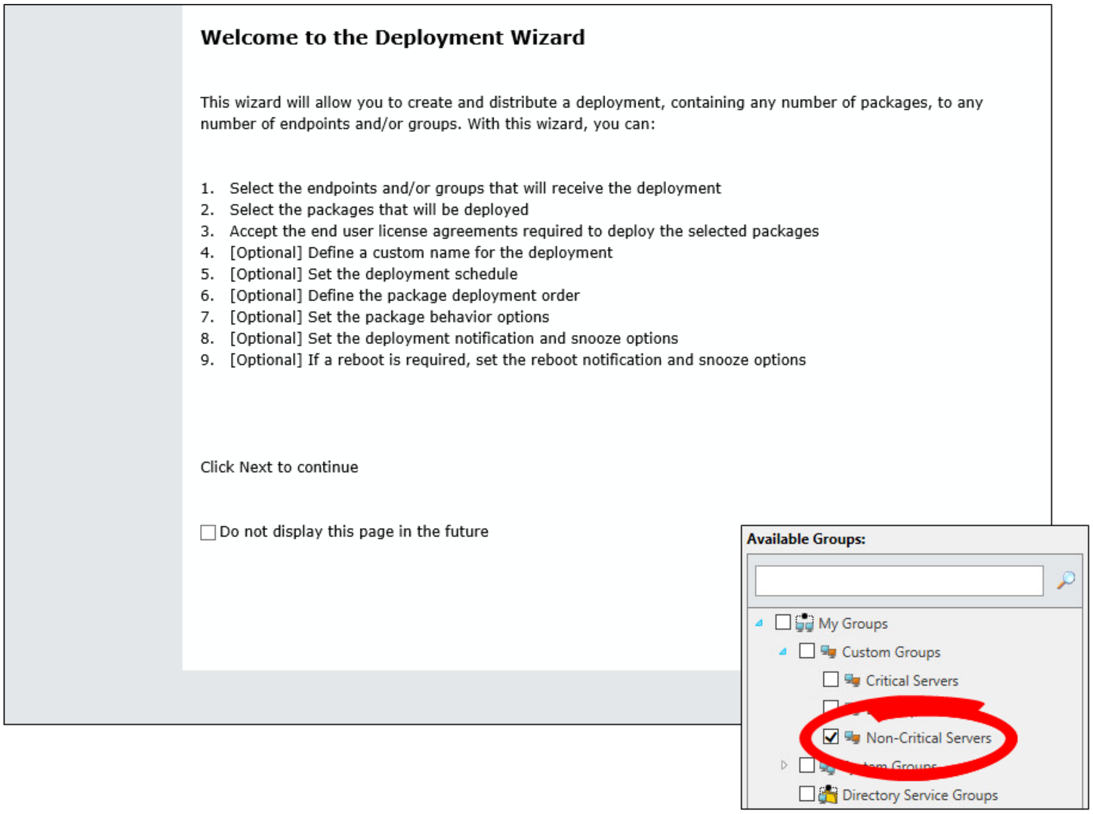
2. Select all patches listed, and then click **Deploy**.



☑	Name
☑	7-Zip File Archiver 16.00 for Windows (See Notes)
☑	APSB15-12 Adobe Photoshop CC 2014 15.2.3 for Windows (See Notes)
☑	APSB15-15 Adobe Acrobat 10.1.15 for Windows (See Notes)
☑	APSB15-15 Adobe Acrobat 11.0.12 for Windows (See Notes)
☑	APSB15-15 Adobe Acrobat DC (Classic) 2015.006.30060 (15.6.30060.15959) for Windows (See Notes)
☑	APSB15-15 Adobe Acrobat DC (Continuous) 2015.008.20082 (15.8.20082.15957) for Windows (See Notes)

3. Complete the **Deployment Wizard**.

When you get to the **Available Endpoints/Groups** page, select a small, low-risk group for your first deployment. After the deployment completes, deploy to progressively larger, higher-risk groups.



Welcome to the Deployment Wizard

This wizard will allow you to create and distribute a deployment, containing any number of packages, to any number of endpoints and/or groups. With this wizard, you can:

1. Select the endpoints and/or groups that will receive the deployment
2. Select the packages that will be deployed
3. Accept the end user license agreements required to deploy the selected packages
4. [Optional] Define a custom name for the deployment
5. [Optional] Set the deployment schedule
6. [Optional] Define the package deployment order
7. [Optional] Set the package behavior options
8. [Optional] Set the deployment notification and snooze options
9. [Optional] If a reboot is required, set the reboot notification and snooze options

Click Next to continue

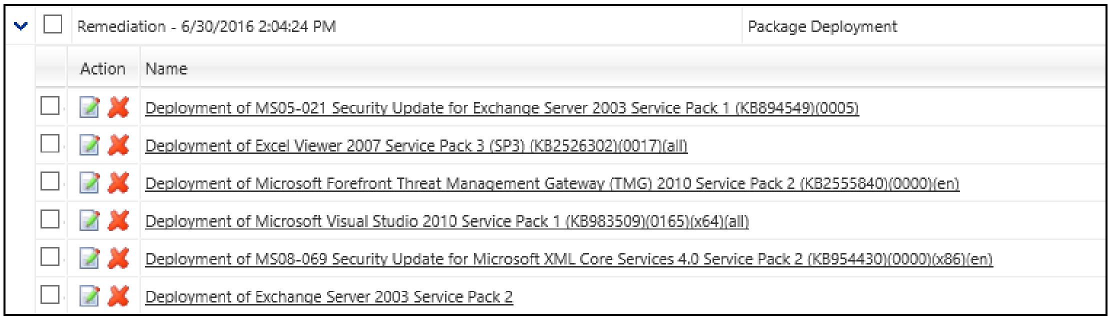
□ Do not display this page in the future

Available Groups:

□ My Groups
- □ Custom Groups
  - □ Critical Servers
  - □
  - ☑ Non-Critical Servers
- □ tem Groups
- □ Directory Service Groups

4. After completing the wizard, monitor the deployment until it completes successfully.

   Browse to **Manage > Deployments and Tasks** and expand your deployment. Wait for each deployment icon to complete successfully (as indicated by the ✓ icon).

   □ Remediation - 6/30/2016 2:04:24 PM — Package Deployment

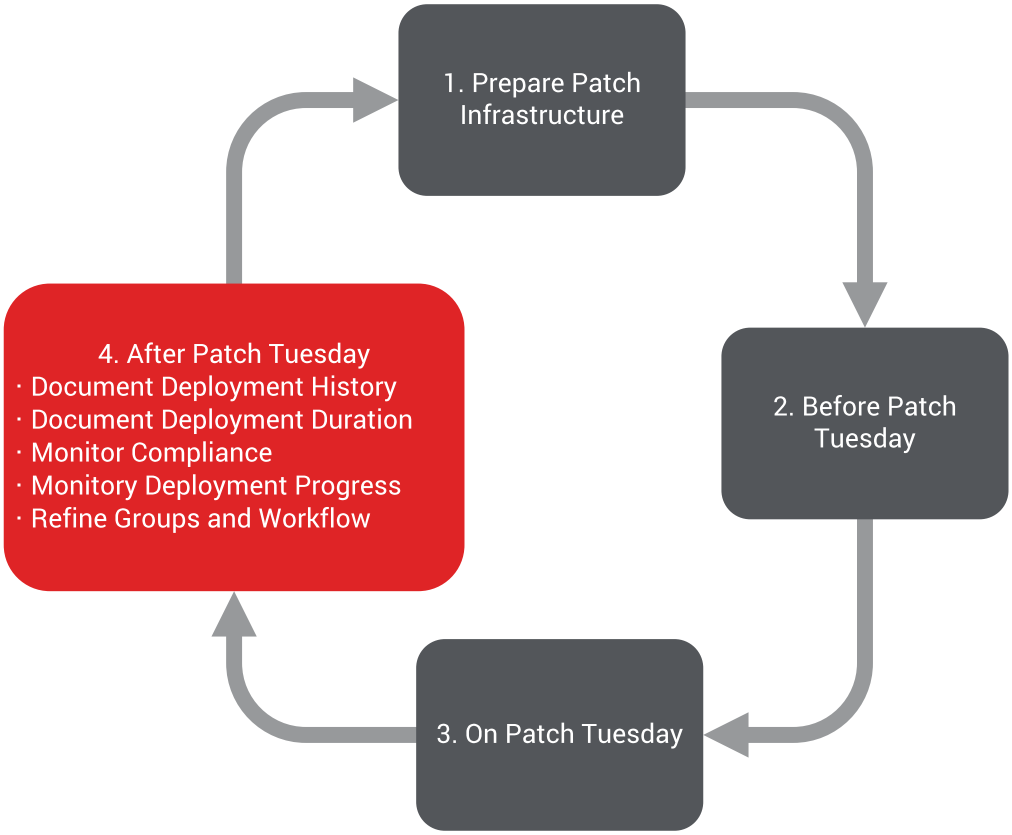
	Action	Name
□	✎ ✗	Deployment of MS05-021 Security Update for Exchange Server 2003 Service Pack 1 (KB894549)(0005)
□	✎ ✗	Deployment of Excel Viewer 2007 Service Pack 3 (SP3) (KB2526302)(0017)(all)
□	✎ ✗	Deployment of Microsoft Forefront Threat Management Gateway (TMG) 2010 Service Pack 2 (KB2555840)(0000)(en)
□	✎ ✗	Deployment of Microsoft Visual Studio 2010 Service Pack 1 (KB983509)(0165)(x64)(all)
□	✎ ✗	Deployment of MS08-069 Security Update for Microsoft XML Core Services 4.0 Service Pack 2 (KB954430)(0000)(x86)(en)
□	✎ ✗	Deployment of Exchange Server 2003 Service Pack 2

5. Repeat steps 1 through 4 for each group that you created.

All Patch Tuesday content is deployed to each group in your organization.

After Patch Tuesday

This section is about assessing the success of the Patch and Remediation deployments in your environment.


1. Prepare Patch Infrastructure
2. Before Patch Tuesday
3. On Patch Tuesday
4. After Patch Tuesday
· Document Deployment History
· Document Deployment Duration
· Monitor Compliance
· Monitory Deployment Progress
· Refine Groups and Workflow

In This Chapter:

Document Deployment History

Maintain accurate records of all patches deployed. Validate that any necessary reboot(s) occurred and/or that your endpoints don’t require a reboot.

- To confirm recent deployments in Ivanti Reporting Services:
    - Run the **Deployment Detail** operational report
    - Select the group(s) that you are monitoring
    - Review success/failure results (**Patched and Complete %**)

Document Deployment Duration

Following your first Patch Tuesday, monitor how long it takes for each deployment to complete. Monitoring each deployment gives you important data, such as:

- The average amount of time it takes the deployment to complete.
- The average amount of time it takes absentee endpoints (such as laptops and VPN-connected endpoints) to complete.

Fully patched and deploy duration success metrics may be defined differently for different organizations depending on the mobility of the endpoints under your management, how often the endpoints are online, or the type of endpoints under management (such as desktop or server).

To Find Information About Deployment Duration:

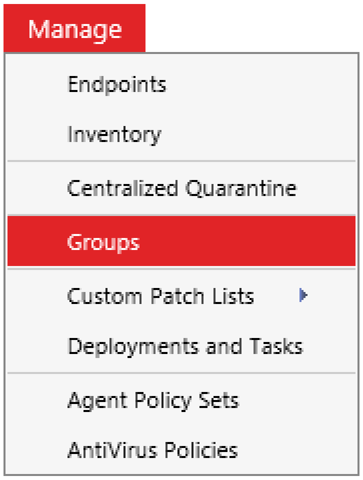
- Strategize and organize patch deployments to the appropriate endpoints and endpoint groups, with the help of Ivanti Reporting Services:
  - Run the **Patch Tuesday Monitoring Report**
  - Select the group(s) that you are monitoring
  - The report provides a summary of the patch status for a selected group of machines for the critical patches released in the selected Patch Tuesday cycle.
  - Set the Auto Refresh parameter to monitor the progress of deployments on endpoints in near-real-time.

Monitor Compliance

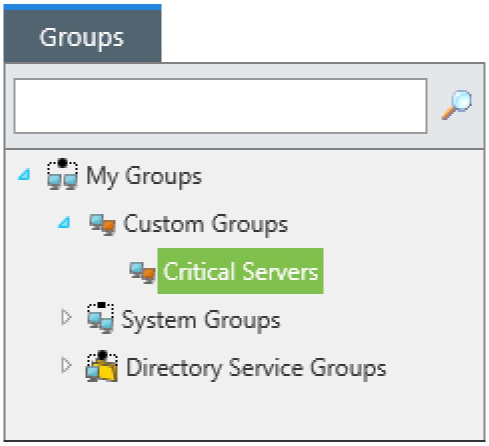
New or rebuilt systems often require a standard set of patches installed. You can use the Ivanti Patch and Remediation Mandatory Baseline feature to automatically install this important software. Mandatory Baselines check for these patches every time the Endpoint Security Agent uploads its scan results to the Endpoint Security Server. The Mandatory Baseline deploys any software you've added to it whenever an endpoint is found that doesn't have that software installed. Create or update an existing mandatory baseline for future deployments.

To Create a Mandatory Baseline:

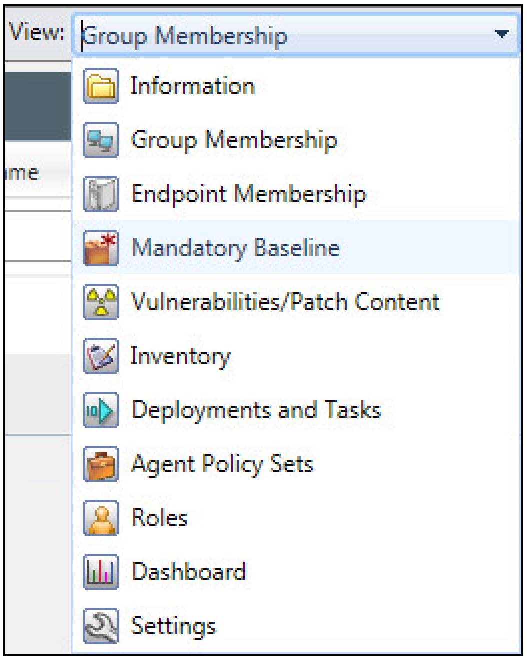
1. From the Navigation Menu, select **Manage > Groups**.



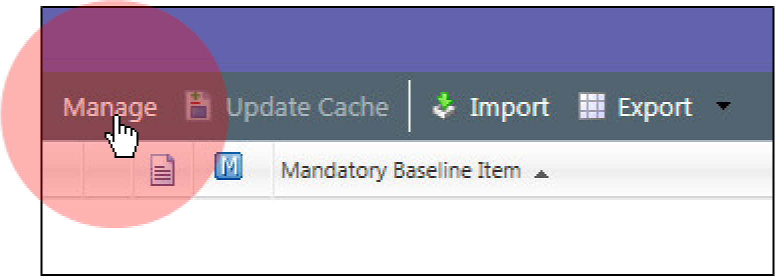
2. From the **Group Browser**, select the group that you want to apply a Mandatory Baseline to.



3. From the **View** menu, select **Mandatory Baseline**.

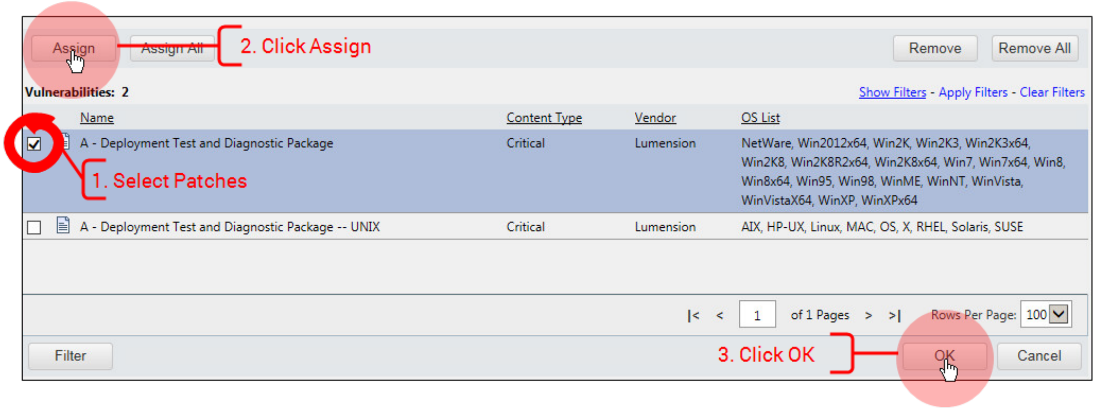


4. Click the **Manage** button.



5. Add patches that you consider to be default content to the Mandatory Baseline.

   To add patches to the Mandatory Baseline, select patches from the **Vulnerabilities** table, and then click **Assign** to move them to the **Selected Vulnerabilities** table. Click **OK** when you're done.

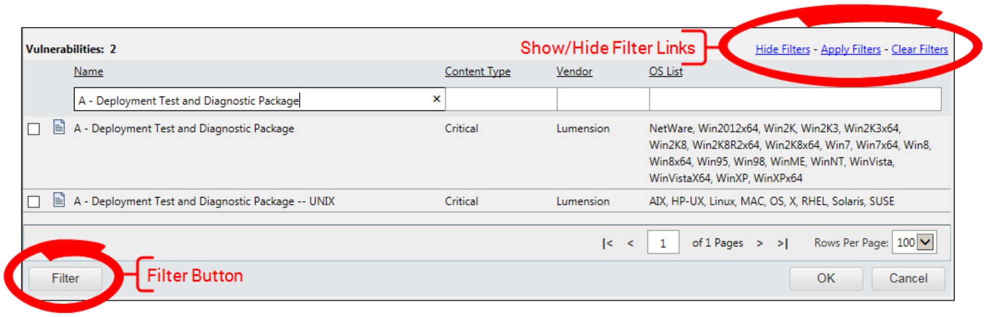


Vulnerabilities: 2

	Name	Content Type	Vendor	OS List
☑	A - Deployment Test and Diagnostic Package	Critical	Lumension	NetWare, Win2012x64, Win2K, Win2K3, Win2K3x64, Win2K8, Win2K8R2x64, Win2K8x64, Win7, Win7x64, Win8, Win8x64, Win95, Win98, WinME, WinNT, WinVista, WinVistaX64, WinXP, WinXPx64
☐	A - Deployment Test and Diagnostic Package -- UNIX	Critical	Lumension	AIX, HP-UX, Linux, MAC, OS, X, RHEL, Solaris, SUSE

Filter the **Vulnerabilities** table using one of the following methods:

- Toggle the **Show/Hide Filters** link
- Click the **Filter** button



Vulnerabilities: 2

	Name	Content Type	Vendor	OS List
	A - Deployment Test and Diagnostic Package			
☐	A - Deployment Test and Diagnostic Package	Critical	Lumension	NetWare, Win2012x64, Win2K, Win2K3, Win2K3x64, Win2K8, Win2K8R2x64, Win2K8x64, Win7, Win7x64, Win8, Win8x64, Win95, Win98, WinME, WinNT, WinVista, WinVistaX64, WinXP, WinXPx64
☐	A - Deployment Test and Diagnostic Package -- UNIX	Critical	Lumension	AIX, HP-UX, Linux, MAC, OS, X, RHEL, Solaris, SUSE

6. **Optional:** Add Mandatory Baselines to additional groups by repeating steps 2 through 5.

You have added patches to your group Mandatory Baselines. If the groups do not already have the patches installed, Endpoint Security automatically installs them the next time each endpoint communicates with Endpoint Security.

Monitor Deployment Progress

Review the Effectiveness of Patch Tuesday Remediations report in Ivanti Reporting Services to validate the deployment.

- To review the patch progress, your organization security posture, your organization vulnerability compliance, and the effectiveness of your Patch Tuesday deployments, use Ivanti Reporting Services as follows:
  - Run the **Effectiveness of Patch Tuesday Remediations** report
  - Select the groups that you are monitoring
- The report provides an executive overview of the Patch Tuesday deployment status. It also allows you to see additional endpoint details.

Refine Groups and Workflow

Modify system settings, distribution parameters, and further optimize the system for next month’s updates in other ways. WAN optimization, polling frequency and minimizing the patches being detected can all help further optimize performance. Look for endpoints that did not receive updates at all or those that took unusually long to receive updates.

To Refine Groups and Workflow:

1. Go the **Manage > Groups** page.
2. Identify any endpoints that are offline and/or have not been remediated.
3. Troubleshoot the endpoints to determine why endpoints were not updated and modify deployments accordingly.