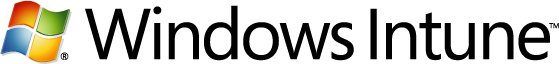
****

**Getting Started Guide: Part Two** *Enroll your managed PCs*

Contents

[**Welcome back to the Windows Intune Getting Started Series** 2](#_Toc300153767)

[Client Enrollment 2](#_Toc300153768)

[Offline Client Enrollment 4](#_Toc300153769)

[Organizing Your Computers 4](#_Toc300153770)

[Manage Update and Automatic Approvals 5](#_Toc300153771)

[Set up Alerts Notifications 7](#_Toc300153772)

[Summary 8](#_Toc300153773)

[Additional Resources: 9](#_Toc300153774)

**Welcome back to the Windows Intune Getting Started Series**

This set of tutorials is designed to help you set up your new Windows Intune environment and evaluate the main features of Windows Intune.

In the previous tutorial, we helped you set up your Windows Intune environment so that you can get ready to manage and secure PCs through the web-based administration console. Specifically, we provided steps to:

* Guide you around the administrator console
* Add administrators to the administration console
* Set your default policies

This tutorial will help you install the client software on PCs you will manage so that you can easily monitor the health and status of your PC environment. You will also learn how to configure groups to help organize the computers you have added to the service, setup automatic approval rules to speed up the deployment of critical updates, and configure alert notifications to help your administrators get the latest alerts.

To help in illustrating the guidelines and recommendations in this guide, we have created a number of demonstration environments throughout this paper you will see example screenshots taken from these environments to help illustrate how you can similarly configure your Windows Intune environment. Subsequently, you can take the steps we have documented to create and customize them to meet your own business needs.

# Client Enrollment

Before you can manage a computer with Windows Intune you will need to install the Windows Intune client software package on the PC – this can be your physical PC or even a virtual machine. Use the following steps to complete this step:

1. Starting from the Systems Overview workspace you can either click the *Download and Deploy the Client software* link or click the **Administration** workspace and then select “**Client Software Download**”.
2. The software can be installed on 32 and 64 bit version of the operating systems and will support Windows XP, Windows Vista and Windows 7.

**Important**: *Before you deploy the Windows Intune client you should consider how you want to handle your existing malware protection software. By default, Windows Intune Endpoint Protection will not be installed if existing protection software is detected. If you want to ensure you are using the Windows Intune Endpoint Protection, we recommend removing the 3rd party malware protection software just before the Windows Intune installation.*

To install the client software on a computer, follow these steps:

1. Click on **Download Client Software***.*
2. When the download dialog opens, select **Save** and select a secure location to save the download package.
3. Once the download has completed, open the folder where you saved the installation package.
4. Right-click the **Windows\_Intune\_Setup.zip** package and select **Extract All…**, this will display the dialog box shown in Figure 5:

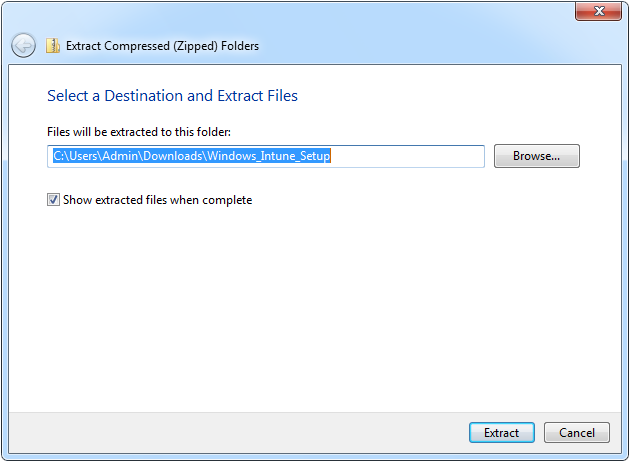


Figure5: Setup files extraction Process

1. Click **Browse…** to select an alternative path (if required) and then click **Extract** to extract the setup files.
2. When the extraction has completed, a new window will be displayed similar to that shown in Figure 6:

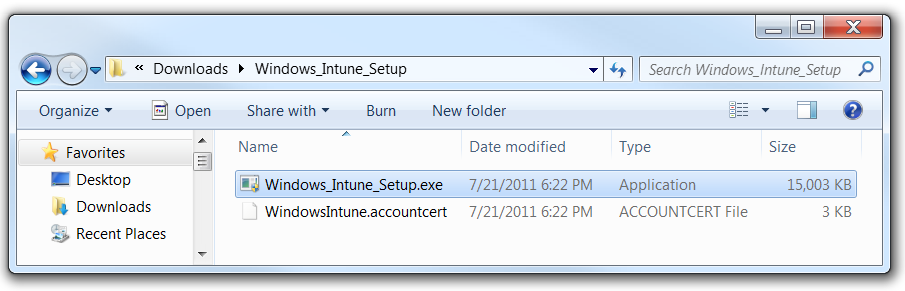
**

Figure 6: Extracted Setup Files

1. These files can be copied to a network share, a thumb drive, or deployed using an electronic software deployment (ESD) system. However it is important to keep these two files together as the ACCOUNTCERT file is used by the setup application when it is executed.

***Note****: If your ESD requires a Microsoft Installer (MSI) file for distribution, you can use the /Extract command line argument on the Windows\_Intune\_Setup.exe file to extract both a 32 bit and 64 bit MSI package. You can also use the /Quiet argument if you wish to suppress the Installation wizard and run it with no user interaction.*

If you wish to use the standard installation process, make sure you are logged on with an account that has local administration rights and double click Windows \_Intune\_Setup.exe from the client computer. Then follow the instructions in the Setup Wizard to complete the installation.

Once the installation has completed, you may be prompted to reboot the computer, this will allow the protection and update agents to complete their installation and will download any required malware protection definitions and other agent updates. The computer account will appear in the Administration console within a few minutes, but it can take up to 30 minutes for all the agents to complete their installations and report all inventory and status updates.

## Offline Client Enrollment

For the standard installation process to complete a live Internet connection is required. If this is not possible at installation time, for example if you are installing the agent into a deployment image that will be used to create a number of computer deployments, there is a command line switch that can be used to schedule a task that will attempt to enroll the computer at a later time. This will ensure that the computer image is not enrolled before it has been deployed to the target computer. To launch a delayed installation use the following command line argument to launch the installation:

*Windows\_Intune\_Setup.exe /PrepareEnroll*

For more information on using this installation option see the [Windows Intune Online Help.](http://onlinehelp.microsoft.com/en-us/windowsintune/hh127729.aspx)

# Organizing Your Computers

The following steps will take you through the process of configuring groups to help organize the computers you will add to the service. Below is an example of how you can go about setting up your first computer groups. Feel free to customize this to meet your organization’s needs.

1. From the Windows Intune Administration Console click the **Computers** Tab.
2. You will see two groups: “All Computers” and “Unassigned Computers”.

The **All Computers** group contains all computers managed by the system at any one time, whereas the **Unassigned Computers** group will contain computers that have not been assigned to a group yet by the systems administrator.

1. Click on the **Create Computer Group** link in the **Tasks** panel on the right.
2. In the **Name** box type “HQ”.
3. In the **description** type “Our HQ site computers”.
4. Under the **Parent Group** heading, make sure the **All Computers** group is selected so that this group appears at the top level of the groups.
5. Now scroll down the page until you can see the **Members** section of the page.
6. Click the **Add…** button and select computers to add to the group.
7. Click **OK** to add the computers and click **Create Computer Group.**
8. Now you can click on the new group in the list to the left and this will show the status of computers in that group.
9. Next, click on the **Computers** tab in the main information panel to show the computers you added to the group.



You can now repeat these steps for all groups you wish to create. Figure 7 shows three examples of grouping strategies you could use to help organize your computers. Managed computers can be a member of multiple Windows Intune groups. This allows you a great deal of flexibility in how you can use groups.

It is important to know that these groups are completely independent of any Active Directory Domain Service (ADDS) groups you have in your domains. The groups only apply to the Windows Intune agents so you are free to change these to meet those needs without having to worry about any possible conflict with ADDS groups.

**Note**: *The numbers in the Departmental example are used to help organize the order the groups are listed in. By default they are sorted* alpha-numerically.

Figure 7: Grouping examples

Once you have created the groups you need to organize your computers you can use them to control the deployment of your Windows Intune polices, software updates and application deployment.

# Manage Update and Automatic Approvals

The groups you created above can now be used to deploy Windows Intune Policies, software updates, and software packages. If you wish to closely manage all the updates that are managed by Windows Intune you can use the Updates workspace to **Approve** or **Decline** them. However, if you wish to ensure that critical or security updates are installed as quickly as possible on your managed PCs, you can use the Windows Intune auto-approval rules. The following steps will take you through the process of setting up an auto-approval rule that can be used to help automate the process of approving updates of the classifications you select.

1. From the Windows Intune Administration Console click **Administration** and **Updates.**
2. Select **Automatic Approval Rules**, scroll down to the bottom of the page, if required, and then click **New….**
3. Type in a Rule name such as: “Default Approval Rule” then click **Next.**
4. In Step 2 of 4, check the All Categories option and click **Next.**
5. Now you can select the update classifications that you wish to automatically approve. We recommend that you select the categories shown in Figure 8 to be automatically approved as these will help to keep your managed computer better protected from new threats or vulnerabilities.

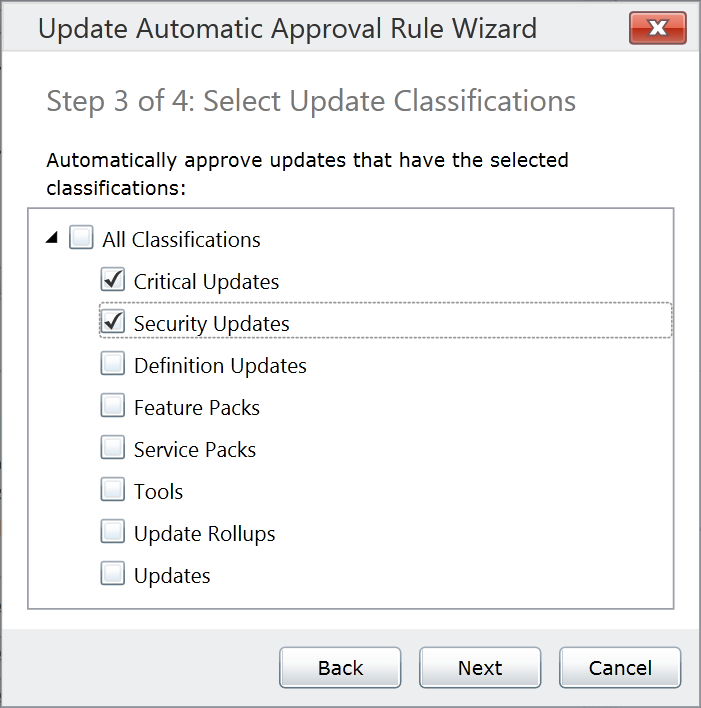
**

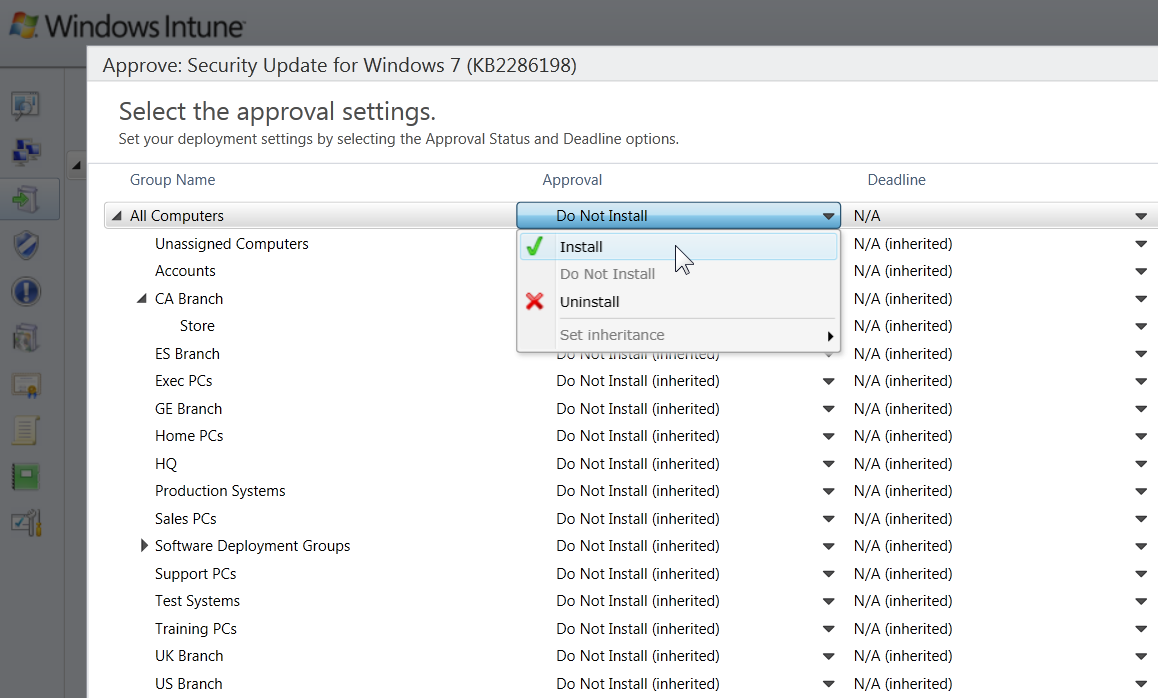
Figure 8: Approval Rule Classifications

1. Once you have selected the classifications you wish to automate click **Next.**
2. Now you can select the groups you wish to deploy this rule to. To deploy it to all your managed computers, select the **All Computers** group and click **Finish.**
3. Click **Run Selected** to force this rule to evaluate all updates on the systems currently and make them available for the managed computers the next time they check in. Or if you click save here, it will only apply to future updates as they are released.

As the managed computers check back in to the service (by default this is every 8 hours), they will be instructed to apply all critical and security updates as soon as they are available.

For those updates that you wish to approve manually, you can use the Updates workspace to review and approve them. There are two types of updates that can be managed in Windows Intune, the first is the Microsoft Updates that are automatically made available to you via the Windows Intune service. For these updates you simply need to select the update and approve it for deployment to the groups you select as shown in Figure 9. You can approve these updates to individual Windows Intune groups or you can approve the updates to higher level groups such as the All Computers group and use inheritance to allow the updates to be approved to all lower level groups.

***Tip****: If you hold down the <CRTL> or <SHIFT> keys while selecting the updates you wish to approve you can select multiple updates to approve at once.*

  
Figure 9: Update Approval

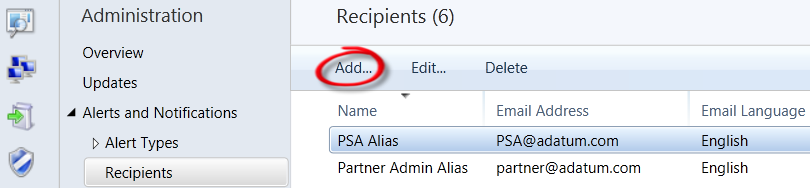
The second type of update you can manage with Windows Intune are 3rd Party updates. For these updates to be approved you first have to obtain the update package (usually an MSI, MSP, or EXE package.) Once you have the update that will update the previous application you will need to select the **Upload** task from the Update workspace. This will start the Update upload wizard that will walk you through the process of creating the update package which can then be approved for deployment in the same way as the Microsoft updates, as shown in Figure 9.

# Set up Alerts Notifications

Windows Intune tracks alerts for your managed computers and you can monitor these via the Alerts workspace or you can have the service email alerts directly to email accounts.

From the Windows Intune Administration Console click the **Administration** workspace tab.

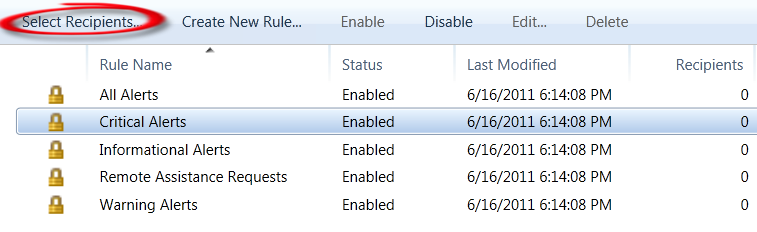
1. Click on **Alerts and Notifications**.
2. Next click **Recipients** and click the Add option as highlighted in Figure 10:

  
Figure 10: Add Recipient

1. Add as many email aliases as you need.

***Note****: Being made a recipient does not allow access to the Windows Intune Administration console. If you wish to allow any of these recipients to logon to the console, you will need to add them as a service administrator.*

1. Next select **Notification Rules** and select the Alert rules you wish to send emails for and then click the **Select Recipients…** option as highlighted in Figure 11:

**  
Figure 11: Select Notification Rule

1. Now you can select which email recipients will receive an email for these alerts.

We recommend that you, as a minimum, set up the *Remote Assistance Requests* for notifications as these alerts are generated by the end user and are typically time critical. You can also use the **Create New Rule…** option to create customized rules to meet your organization’s specific needs, if required.

# Summary

This guide has taken you through the key steps to install the Windows Intune client software on PCs you will manage using the web-based administration console. In the third and final installment, we will help you learn how to assess the health of your computers, create custom reports, deploy software and remote control a managed computer using Windows Intune Remote Assistance. If you are evaluating the 30-day trial and are interested in becoming a Windows Intune, please visit

[www.microsoft.com/windows/windowsintune/pc-management-how-to-try-and-buy.aspx](http://www.microsoft.com/windows/windowsintune/pc-management-how-to-try-and-buy.aspx).

With a paid subscription to Windows Intune, you will also get upgrade rights to Windows 7 Enterprise and future version of Windows. To evaluate Windows 7 Enterprise today, visit:

[technet.microsoft.com/en-us/evalcenter/cc442495.aspx.](http://technet.microsoft.com/en-us/evalcenter/cc442495.aspx)

For guidance and tools to help you in deploying Windows 7 Enterprise with your Windows Intune subscription, visit: [go.microsoft.com/fwlink/?LinkId=180725](http://go.microsoft.com/fwlink/?LinkId=180725). For the latest Windows Intune information, visit the Windows Intune website at: [www.windowsintune.com](http://www.windowsintune.com/)

### Additional Resources:

Windows Intune Online Help: [onlinehelp.microsoft.com/en-us/windowsintune/hh127729.aspx](http://onlinehelp.microsoft.com/en-us/windowsintune/hh127729.aspx)

Windows Intune TechCenter: [technet.microsoft.com/windows/intune](http://technet.microsoft.com/windows/intune)

Windows Intune Team Blog: [blogs.technet.com/windowsintuneblogs.technet.com/windowsintune](http://blogs.technet.com/windowsintune)

Windows Intune FAQ: [www.microsoft.com/windows/windowsintune/windowsintune-faq.aspx](http://www.microsoft.com/windows/windowsintune/windowsintune-faq.aspx)

