



# Microsoft Windows Intune Champions Guide Version 2.5

## Contents

You're ready to go .....	3
Cloud based Device Management Configuration Tool .....	4
Getting Started with the Windows Management Portals .....	5
The Account Portal .....	7
The Admin Console Portal.....	10
Add Computers, Users, and Mobile Devices.....	13
Adding Users and Security Groups .....	13
Managing User and Device Groups .....	14
Enrolling Computers.....	16
Mobile Devices .....	17
Manage Update and Automatic Approvals.....	18
Set Up Alert Notifications.....	19
Creating Reports.....	21
Customizing Report Templates .....	21
Using Windows Intune to Distribute Software Applications and Non-Microsoft Updates.....	23
Software Distribution Topics.....	23
PC Rebuilds.....	25

## You're ready to go

Your HubOne consultant will have already setup the following as part of our implementation process:

- Security Update Approval Rules
- Basic alerting to contact local admins and support@hubone.com
- Windows Intune Mobile Device Security Policy
- Windows Firewall Settings Policy
- Windows Intune Centre Settings Policy

**Please Note:** Software Deployment and SOE Development e.g. (PC Builds), are quite complicated technical tasks. These tasks are not undertaken as part of a basic Windows Intune system implementation and will incur extra costs.

# Cloud based Device Management Configuration Tool

Windows Intune provides a cloud-based unified device management service that can help businesses of all sizes manage and secure personal computers and mobile devices worldwide.

Windows Intune can be operated in a number of ways. HubOne clients typically use it in classic cloud-only mode, which doesn't require on-premises infrastructure. In this case, your configuration will look like Figure 1.

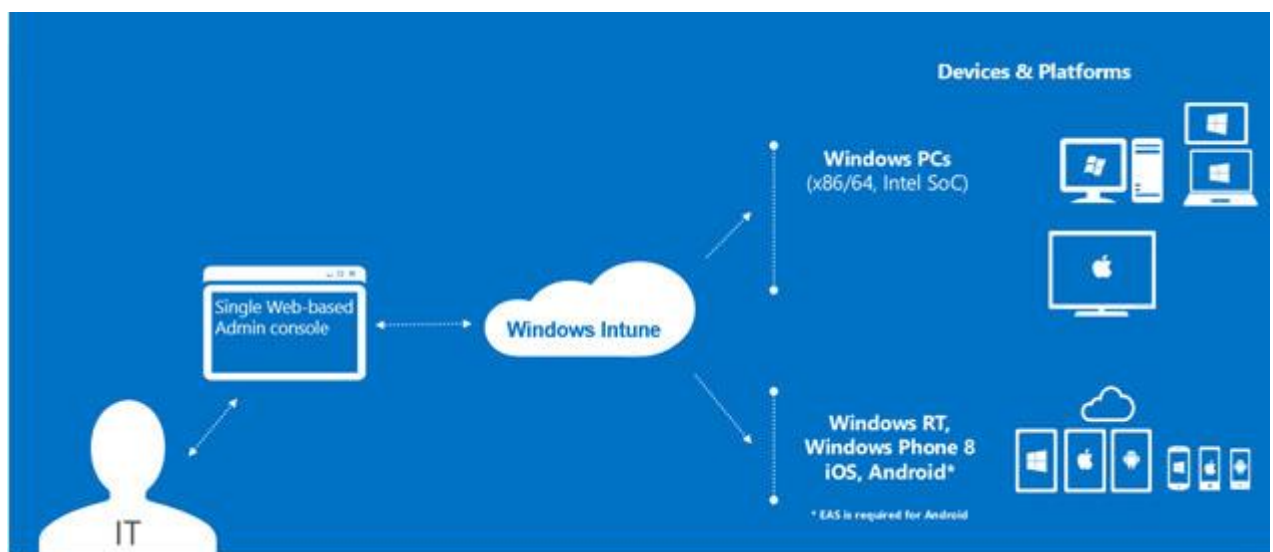


Figure 1. Windows Intune in the Cloud Configuration

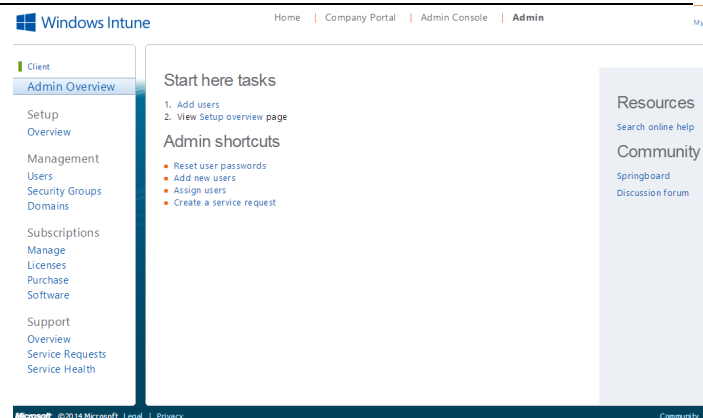
# Getting Started with the Windows Management Portals

There are two Administrator management portals that you can use to access the various features of your Windows Intune service.

## Account Portal:

<https://account.manage.microsoft.com>

The Account Portal is a common configuration interface that administrators can use to manage users, groups, and domains for all Microsoft Online services, including Windows Intune and Office 365. With this online portal, you can check the status of your subscriptions, add new subscriptions, and activate new user accounts. In addition, end users can use the portal to change their passwords.

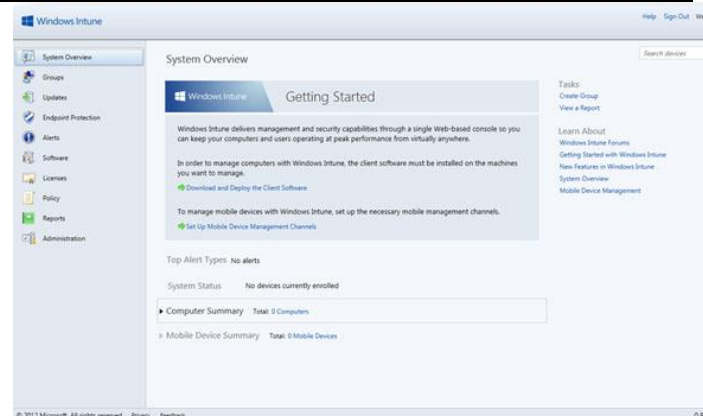


## Admin Console Portal:

<https://admin.manage.microsoft.com>

In the Admin Console Portal you manage devices and settings for Intune.

On the left is the Navigation panel, which contains links to Windows Intune workspaces. (Note that each feature in Windows Intune has a workspace.) In the middle of the screen is the main information panel that provides the detailed view for the workspace, which in this example is the Systems Overview workspace. Finally, on the



right is the Tasks panel, which generates a context sensitive list of available tasks for the selected workspace	
--	--

## The Account Portal

Windows Intune

Home | Company Portal | Admin Console | **Admin**

Site Admin  
My profile | Sign out  
**Admin**

**Client**

**Admin Overview**

Setup Overview

Management

Users

Security Groups

Domains

Subscriptions

Manage Licenses

Purchase Software

Support Overview

Service Requests

Service Health

**Start here tasks**

1. Add users
2. View Setup overview page

**Admin shortcuts**

- Reset user passwords
- Add new users
- Assign users
- Create a service request

**Resources**

Search online help

**Community**

Springboard

Discussion forum

Microsoft © 2014 Microsoft Legal | Privacy

Community | Feedback

Account Portal: <https://account.manage.microsoft.com>

<p><a href="#">Admin Overview</a></p> <p>Contains a number of Shortcuts to Frequently used options</p>	<p>Start here tasks</p> <ol style="list-style-type: none"> <li>1. <a href="#">Add users</a></li> <li>2. View <a href="#">Setup overview</a> page</li> </ol> <p>Admin shortcuts</p> <ul style="list-style-type: none"> <li><a href="#">Reset user passwords</a></li> <li><a href="#">Add new users</a></li> <li><a href="#">Assign users</a></li> <li><a href="#">Create a service request</a></li> </ul>
<p><a href="#">Setup Overview</a></p> <p>Contains a number of Shortcuts to advanced setup options</p>	<p>Support Overview</p> <p>Windows Intune is ready for you to use. You can begin managing and securing computers and devices through the Windows Intune administrator console</p> <p>Configuring services</p> <p>When you begin to integrate your current environment with Windows Intune, you can configure some additional service-level</p>

	settings. These will enable a richer interaction between your on-premises environment and Windows Intune. Some items may require changes to your existing on-premises environment.				
<div>Management - Users</div> <div>Manage the users on Windows Intune</div>	<div>Users</div> <div>Active   Deleted</div> <div>Single sign-on: <a href="#">Set up</a>   <a href="#">Learn more</a></div> <div>Active Directory® synchronization: <a href="#">Set up</a>   <a href="#">Learn more</a></div> <div><a href="#">New</a>   <a href="#">Edit</a>   <a href="#">Reset password</a>   <a href="#">Delete</a>   <a href="#">Activate synced users</a></div> <div><div>View: All users</div></div> <div><div><input type="checkbox"/></div><div>Display name</div><div>User name</div></div>				
<div>Management - Users</div> <div>Manage your Intune groups</div>	<div>Security groups</div> <div>Single sign-on: <a href="#">Set up</a>   <a href="#">Learn more</a></div> <div>Active Directory® synchronization: <a href="#">Set up</a>   <a href="#">Learn more</a></div> <div><a href="#">New</a>   <a href="#">Edit</a>   <a href="#">Delete</a></div> <div><div><input type="checkbox"/></div><div>Display name</div></div>				
<div>Management - Domains</div> <div>Manage the domain names that you use in Intune</div>	<div>Domains</div> <div>Your Microsoft Online Services account comes with a domain name—<i>contoso.onmicrosoft.com</i>—but if you have your own domain name already, you can usually use that domain name with Microsoft Online Services services too. To add your domain, click <b>Add a domain</b>.</div> <div>Note: Users of Office365 through Telstra CANNOT use their Office365 domain name in Intune.</div>				
<div>Subscriptions - Manage</div> <div>Billing and Subscription Management</div>	<div>Billing and subscription management</div> <table><tr><th>Subscription</th><th>Quantity</th></tr><tr><td><a href="#">Windows Intune™ - Trial</a></td><td>100 device licenses</td></tr></table>	Subscription	Quantity	<a href="#">Windows Intune™ - Trial</a>	100 device licenses
Subscription	Quantity				
<a href="#">Windows Intune™ - Trial</a>	100 device licenses				
<div>Subscriptions - Licences</div> <div>View how many Licences you have</div>	<div>Licenses</div> <table><tr><th>Name</th><th>Valid</th></tr><tr><td>Windows Intune</td><td>100</td></tr></table>	Name	Valid	Windows Intune	100
Name	Valid				
Windows Intune	100				
<div>Subscriptions - Purchases</div> <div>Buy more licences</div>	<div>Purchase subscriptions</div> <div>Windows Intune</div> <div>Windows Intune™ simplifies how businesses manage and secure PCs at cloud services and System Center Configuration Manager.</div>				

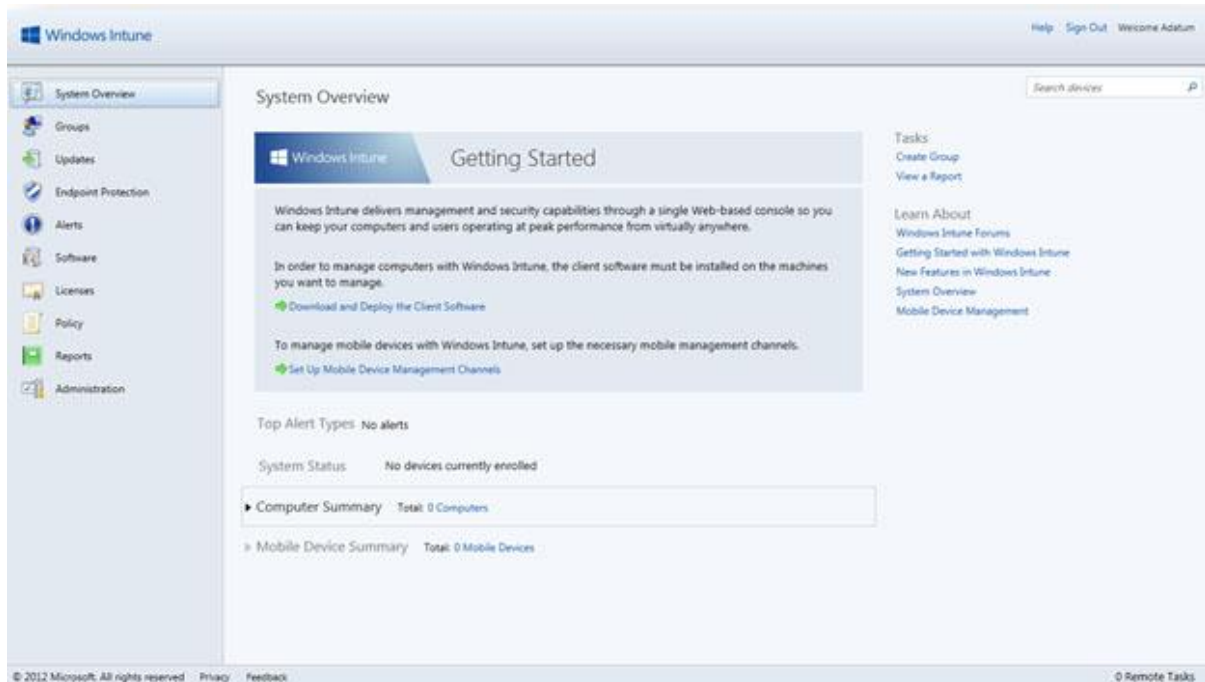


<div>Subscriptions - Software</div> <div>Download your Windows software and licence keys</div>	<div><div>Microsoft®Online Services</div><div>Customer Portal</div><div>Download Products</div><table><tr><th>Product Name</th><th>Details</th><th>Product Key</th><th>Download</th></tr><tr><td> Windows Intune</td><td></td><td></td><td></td></tr></table></div>	Product Name	Details	Product Key	Download	Windows Intune																
Product Name	Details	Product Key	Download																			
Windows Intune																						
<div>Support - Overview</div> <div>Get help</div>	<div>Help and community</div> <div><a href="#">Get support from the Microsoft Online Community</a></div> <div>Delegated administrators</div> <div><a href="#">Manage your delegated administrators</a></div>																					
<div>Support – Service Requests</div> <div>Contact the Intune Support team</div>	<div>Thank you for contacting Support</div> <div> Windows Intune</div> <div><div>Windows Intune cloud service</div><div><div> Phone Support</div><div> Click here to find your local phone support numbers for <b>technical and non-technical</b> is:</div><div> E-mail Support</div><div> Click here for <b>non-technical</b> questions or issues including product questions before you t *Available in Arabic, Dutch, English, French, German, Hebrew, Italian, Japanese, Korean, Traditional Chinese (Hong Kong), Turkish only</div><div> Click here for <b>technical</b> questions or issues with the Windows Intune cloud service *Available in English and Japanese only</div></div></div>																					
<div>Support – Service Health</div> <div>View the service health dashboard</div>	<div> Windows Intune</div> <div><div>Current Status</div><div>The current service status is shown in the following table. Move the pointer over the status icon to view more information when available.</div><table><tr><th>Status</th><th>Service Instance</th><th>Details</th></tr><tr><td></td><td>Asia 01</td><td>The service instance is running normally.</td></tr><tr><td></td><td>Asia 02</td><td>The service instance is running normally.</td></tr><tr><td></td><td>Asia 03</td><td>The service instance is running normally.</td></tr><tr><td></td><td>Asia 05</td><td>The service instance is running normally.</td></tr><tr><td></td><td>Europe 01</td><td>The service instance is running normally.</td></tr><tr><td></td><td>Europe 02</td><td>The service instance is running normally.</td></tr></table></div>	Status	Service Instance	Details		Asia 01	The service instance is running normally.		Asia 02	The service instance is running normally.		Asia 03	The service instance is running normally.		Asia 05	The service instance is running normally.		Europe 01	The service instance is running normally.		Europe 02	The service instance is running normally.
Status	Service Instance	Details																				
	Asia 01	The service instance is running normally.																				
	Asia 02	The service instance is running normally.																				
	Asia 03	The service instance is running normally.																				
	Asia 05	The service instance is running normally.																				
	Europe 01	The service instance is running normally.																				
	Europe 02	The service instance is running normally.																				

## The Admin Console Portal

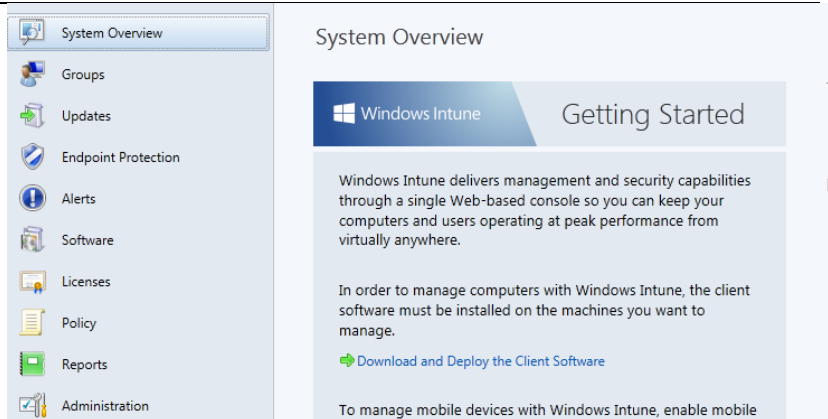
Windows Intune provides a cloud-based unified device management service that can help businesses of all sizes manage and secure personal computers

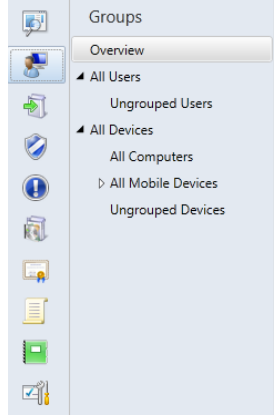
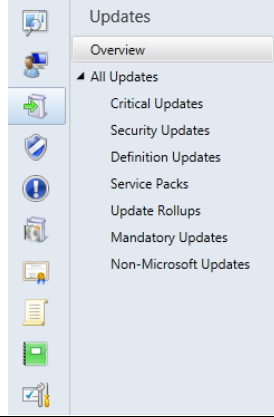
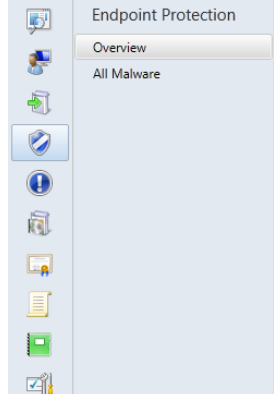
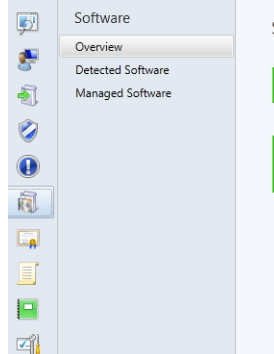
Admin Console Portal: <https://admin.manage.microsoft.com>



### System Overview

Contains a number of Shortcuts to Frequently used options



<p><b>Groups</b></p> <p>Manage Grouped users or Devices</p>		<p><b>Groups Overview</b></p> <p>▶ Computer Summary Total: 0 Computers</p> <p>▶ Mobile Device Summary Total: 0 Mobile Devices</p> <p>Alert Status ✓ No devices with alerts</p> <p>Update Status ✓ No issues</p> <p>Endpoint Protection Status ✓ No issues</p>
<p><b>Updates</b></p> <p>Manage all updates</p>		<p><b>Updates Overview</b></p> <p>Update Status ✓ No issues</p> <p>Cloud Storage Status Space used: 0 GB of 20 GB (0% used) ✓ No issues. <a href="#">Manage storage</a></p>
<p><b>Endpoint Protection</b></p> <p>Manage anti-virus software on enrolled machines</p>		<p><b>Endpoint Protection Overview</b></p> <p>Malware Status ✓ No issues</p> <p>Computer Status ✓ No issues</p> <p>Learn About <a href="#">Malware Protection</a> <a href="#">Endpoint Protection</a> <a href="#">How to Schedule Updates</a> <a href="#">How to Configure Updates</a></p> <p>Top Malware These instances: Name None</p>
<p><b>Software</b></p> <p>Manage detected software and Deploy new software</p>		<p><b>Software Overview</b></p> <p>Software Status ✓ No issues</p> <p>Cloud Storage Status Space used: 0 GB of 20 GB (0% used) ✓ No issues. <a href="#">Manage storage</a></p> <p>Search managed software</p> <p>Tasks <a href="#">Step 1: Add Software</a> <a href="#">Step 2: Manage Deployment</a></p> <p><a href="#">Learn About Software Overview</a></p>

<p><b>Licences</b></p> <p>Track all your software licences</p>		<p><b>Licences Overview</b></p> <p>Search agreements</p> <p>Microsoft Volume Licensing Agreements</p> <p>View license agreement information for software that was purchased through Volume Licensing agreements and that is installed on your managed computers.</p> <p>There are no Microsoft Volume Licensing agreements. Add agreements to allow the service to retrieve the most current license information.</p> <p>Add Agreements</p> <p>Other Software Licensing Agreements</p> <p>View license agreement information for non-Microsoft software or Microsoft software that was purchased from retailers and that is installed on your managed computers.</p> <p>There are currently no other software licensing agreements.</p> <p>Tasks</p> <ul style="list-style-type: none"> <li>Add Volume Licensing</li> <li>Add Other Software Ag</li> <li>Create License Group</li> <li>View Purchase Report</li> <li>View Installation Report</li> </ul> <p>Learn About</p> <ul style="list-style-type: none"> <li>Licences Overview</li> <li>Microsoft Privacy Policy</li> </ul>
<p><b>Policy</b></p> <p>Manage the various settings using in Intune</p>		<p><b>Policy Overview</b></p> <p>Search policies</p> <p>Policy</p> <p>No issues</p> <p>Getting Started with Policy</p> <p>The Policy workspace lets you configure policies that manage settings on computers and mobile devices. You create policies based on templates. You can specify a value for each setting in a policy, or decide not to configure values for some settings so that they are left to the discretion of the end-user, managed by another policy, or configured by another method. After you configure a policy for computers, you can deploy it to groups of devices. After you configure a mobile device policy, you can deploy it to groups of users.</p> <p>To create a policy, click "Add Policy."</p> <p>Tasks</p> <ul style="list-style-type: none"> <li>Add Policy</li> <li>View Policies</li> </ul> <p>Learn About</p> <ul style="list-style-type: none"> <li>Policy Overview</li> <li>Interaction with G</li> </ul>
<p><b>Reports</b></p> <p>Various reports on software hardware etc.</p>		<p><b>Reports Overview</b></p> <p>Search reports</p> <p>Update Reports</p> <p>Update Reports display the software updates that succeeded on computers in your organization, in addition to the updates that failed, are pending, or are needed. Filter updates based on criteria such as update classifications.</p> <p>Detected Software Reports</p> <p>Detected Software Reports display software installed on computers in your organization and include the software versions. Use this report to plan software purchases, and to understand the software needs of users in your organization.</p> <p>Computer Inventory Reports</p> <p>Computer Inventory Reports display information about computers in your organization. Filter computers based on criteria such as disk space or processor speed. Use this report to plan hardware purchases, and to understand more about the hardware needs of users in your organization.</p> <p>Mobile Device Inventory Reports</p> <p>Mobile Device Inventory Reports display information about mobile devices in your organization. You can filter mobile devices based on information such as device platform and view inventory on jailbroken or rooted devices.</p> <p>Learn About</p> <ul style="list-style-type: none"> <li>Reports Overview</li> </ul>
<p><b>Administration</b></p> <p>Download the Intune Client, manage alerts and administrators</p>		<p><b>Alerts and Notifications</b></p> <p>Configure Alert Types</p> <p>You can change the recommended default alert settings by enabling alert types that are important and by disabling alert types that are not important in your environment. Additionally, you can configure alert thresholds for alert types. Note: Certain alert types cannot be configured.</p> <p>Select Recipients for Email Notifications</p> <p>If you have administrative rights and permissions on the console, you can receive email notifications when specific alerts are raised. You can specify additional recipients who only can receive email notifications.</p> <p>Associate Recipients with Notification Rules</p> <p>A notification rule dictates for which types of alerts a notification email can be sent. For each rule, you can select the recipients who should receive these emails. You can select any number of recipients for each rule, and a recipient can be selected for multiple rules.</p> <p>Learn About</p> <ul style="list-style-type: none"> <li>Alerts Overview</li> </ul>

For more information see [Microsoft's Intune Library](#).

# Add Computers, Users, and Mobile Devices

Your environment should now be ready for you to add users and enroll computers or mobile devices.

## Adding Users and Security Groups

Windows Intune uses two types of groups to manage policies, software distribution and updates: User Groups and Device Groups. With User Groups, you can make licensed software available to users and target mobile device security policies to the required user accounts. With device groups, you can deploy software and updates, Windows Intune Agent Settings, and Windows Firewall Settings policies.

You can provide users with access to the Windows Intune company portal. This portal can help users perform common tasks without involving the IT help desk, allows them to add or remove their own devices, and install available licensed software applications.

For users and security groups to appear in the Windows Intune administrator console, you must sign in to the Windows Intune account portal and manually add users or security groups, or both, to the account portal.

To add users manually to the Windows Intune account portal:

1. Open the Windows Intune account portal. <https://account.manage.microsoft.com>
2. In the header, click **Admin**.
3. In the left pane, under **Management**, click **Users**.
4. On the **Users** page, click **New**, and then click **User**.
5. On the **Details** page, complete the user information. Click the arrow next to **Additional details** to add optional user information such as job title or department, and then click **Next**.
6. On the **Settings** page, if you want the user to have an administrator role, select **Yes**, and select an administrator role from the list.
7. Under **Set user location**, select the user's work location, and then click **Next**.
8. On the **Group** page, under **Windows Intune user group**, ensure that the name of the user is selected.
9. On the **Send results in email page**, select **Send email** to send a user name and temporary password (which Windows Intune creates automatically) for the newly created user to yourself and the recipients of your choice by email. Enter email addresses separated by semicolons (;), and then click **Create**. You can enter a maximum of five email addresses.
10. On the **Results** page, the new user name and a temporary password are displayed. After you review the results, click **Finish**.

To add security groups manually to the Windows Intune account portal:

1. Open the Windows Intune account portal.
2. In the header, click **Admin**.
3. In the left pane, under **Management**, click **Security Groups**.
4. On the **Security Groups** page, click **New**.
5. On the **Details** page, type a display name and description for the group, and then click **Save**.
6. On the **Select members** page, from the **List type** list, select which type of members you want to add to the new security group: **Users** or **Groups** (other security groups).
7. The available members for the selected list type are displayed under **Available members**.
8. Select the check box next to each member that you want to add, and then click **Add**. The added members are displayed in the **Selected members** list.
9. To remove a member from the **Selected members** list, select the check box next to the member that you want to remove, and then click **Remove**.
10. After the list of members is complete, click **Save and Close**.

After you have set up and activated the user accounts, switch back to the Windows Intune Admin Console <https://admin.manage.microsoft.com> and plan the organization of your User and Device groups.

## Managing User and Device Groups

The following steps take you through the process of configuring groups to help organize the users and devices you have added to the service. After viewing this example, you can customize this procedure to meet your organization's needs.

Hubone recommends: Using a single group called All Computers

1. From the *Windows Intune Admin 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, whereas the **Unassigned Computers** group will contain computers that have not been assigned to a group yet by the systems administrator.
3. Click on the **Create Computer Group** link in the **Tasks** panel on the right.
4. In the **Name** box type "HQ."
5. In the description type "Our HQ site computers."
6. 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.
7. Now scroll down the page until you can see the **Members** section of the page.
8. Click the **Add...** button and select computers to add to the group.
9. Click **OK** to add the computers and click **Create Computer Group**.
10. Click on the new group in the list to the left to show the status of computers in that group.
11. 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 can use to organize your computers. Both managed users and devices can be members of multiple respective groups. This arrangement helps provide a great deal of flexibility in how you can use groups.



Figure 7. Grouping Examples

## Enrolling Computers

You can enroll computers in Windows Intune in three ways:

1. **Administrator Enrollment:** The Windows Intune Administrator sets up the computer enrollment on behalf of the computer's user.
2. **User Enrollment:** The device user self-enrolls a computer through the Windows Intune company portal.

### *Administrator Enrollment*

Before you can manage a computer by using Windows Intune, you must download and install the Windows Intune client software package on the computer, which can be a physical computer or a virtual machine.

To download the client software installation package:

1. Open the Windows Intune admin console.
2. In the workspace shortcuts pane, click the **Administration** icon.
3. In the navigation pane, click **Client Software Download**.
4. Ensure that the targeted computer meets the minimum software and hardware requirements that are described in *Configure Your Windows Intune Environment*.
5. Click **Download Client Software**. The client software is contained in a compressed (zipped) folder that can be opened or saved. When you are prompted to choose what you want to do with the `Windows_Intune_Setup.zip` compressed folder, click **Save**, and then save the folder to a secure location.\.\.
6. After the download is complete, click **Open Folder** and then follow the steps in the next procedure.

To install the client software on a computer:

1. Open the folder where you saved the installation package.
2. Double click the `Windows_Intune_Setup.zip` compressed folder, and then click **Extract all files**.
3. In the *Select a Destination and Extract Files* dialog box, browse to a secure location to which the Windows Intune setup files will be extracted, and then click **Extract**. When the extraction is complete, a new window opens showing the files in the specified destination folder similar to that shown in Figure 8.



4.

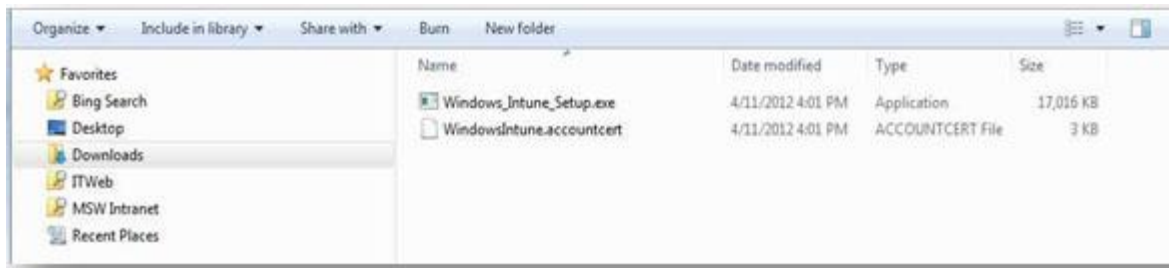


Figure 8. Windows Intune Setup Files

You can copy the files to a network share, a thumb drive, or deploy the files by using an electronic software deployment (ESD) system. However, it is important to keep both files together because the ACCOUNTCERT file is required by the setup application when it runs.

5. If you want to use a standard installation process, ensure that you are logged on to the targeted computer with an account that is a member of the local Administrators group, double-click the Windows\_Intune\_Setup.exe file, and then follow the instructions in the Setup Wizard to complete the installation.
6. After the installation is complete, restart the computer. A restart is needed to complete the installation of the protection and update agents, and to download any required endpoint protection definitions or other agent updates.

The managed computer should appear in the Windows Intune administrator console within a few minutes, but it can take up to 30 minutes for the agents to be completely installed and to report inventory and status updates. Repeat the following procedure on every computer that you want to add in the Windows Intune service.

### User Enrollment

For a user to self-enroll a computer he or she must first access the Windows Intune company portal and log on using their Windows Intune user ID.

## Mobile Devices

**Hubone Recommends:** Mobile device management is quite tricky and should really only be contemplated for complex environments where the devices are owned and managed by the Business.

## Manage Update and Automatic Approvals

You can now use the groups that you created previously to deploy both Windows Intune Policies and Microsoft updates. If you want to manage closely the updates that Windows Intune can control, then you can use the Approve or Decline options in the updated workspace. However, if you want to ensure that critical or security updates install on your managed computers, you can use the Windows Intune auto-approval rules. The following steps take you through the process of setting up an auto-approval rule that automates the process of approving updates within 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* and then click **Next**.
4. Check the **All Categories** option and click **Next**.
5. Select the update classifications that you wish to approve automatically. We recommend that you select the categories shown in Figure 13 for automatic approval, because these categories help keep your managed computers protected from new threats or vulnerabilities.

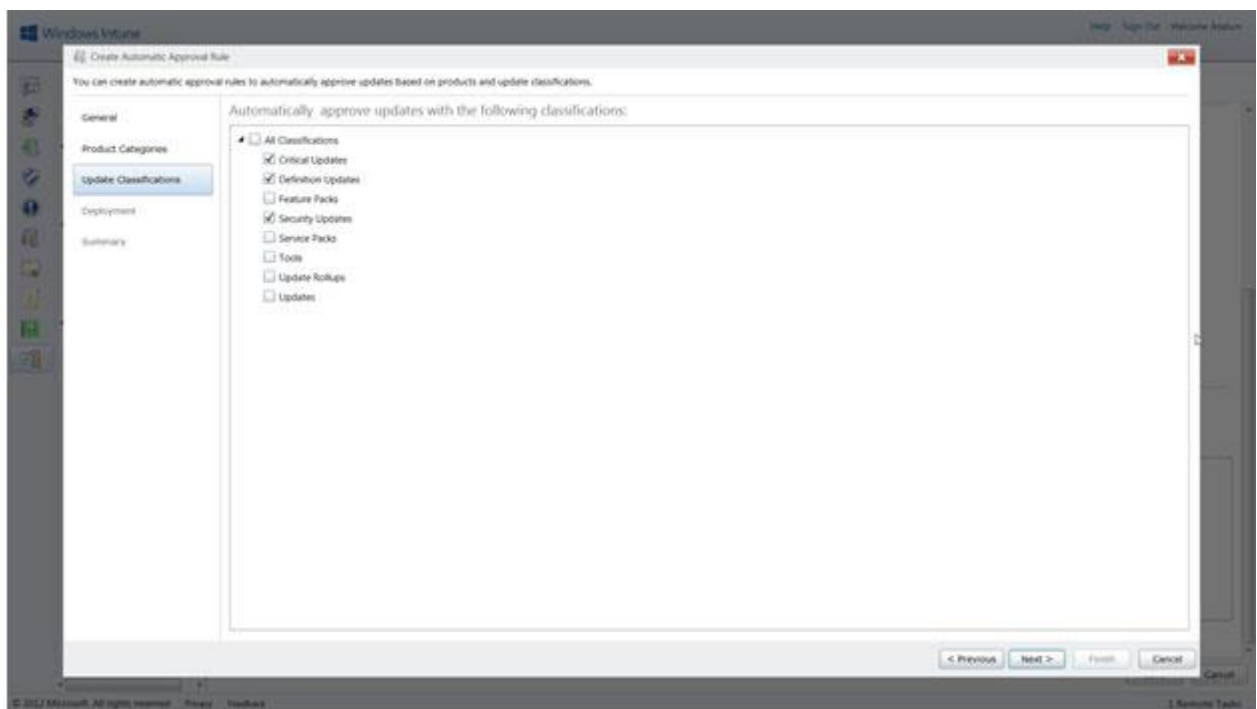


Figure 13. Approval Rule Classifications

6. When you have selected the classifications you want to automate, click **Next**.
7. Select the groups to which you want to deploy this rule. For example, to deploy the rule to your managed computers, select the **All Computers** group.
8. Click **Finish**.

9. Click **Run Selected** to force this rule to evaluate all updates currently on the system and make those updates available to the managed computers the next time they check in (every eight hours by default). Alternatively, if you click **Save** at this point, the rule will only apply to future updates as they are released.

As managed computers check back with the service, they receive instructions to apply critical and security updates as soon as those updates are available. Use the Updates workspace to review and approve updates that you wish to apply manually.

---

## Set Up Alert Notifications

Windows Intune tracks alerts for your managed computers, which you can monitor through the Alerts workspace or by having the service send the alerts directly to nominated email addresses.

To configure alert notifications, in the Windows Intune Administration Console click the **Administration** workspace tab.

1. Click on **Alerts and Notifications**.
2. Click **Recipients** and click the **Add** option as highlighted in Figure 14.

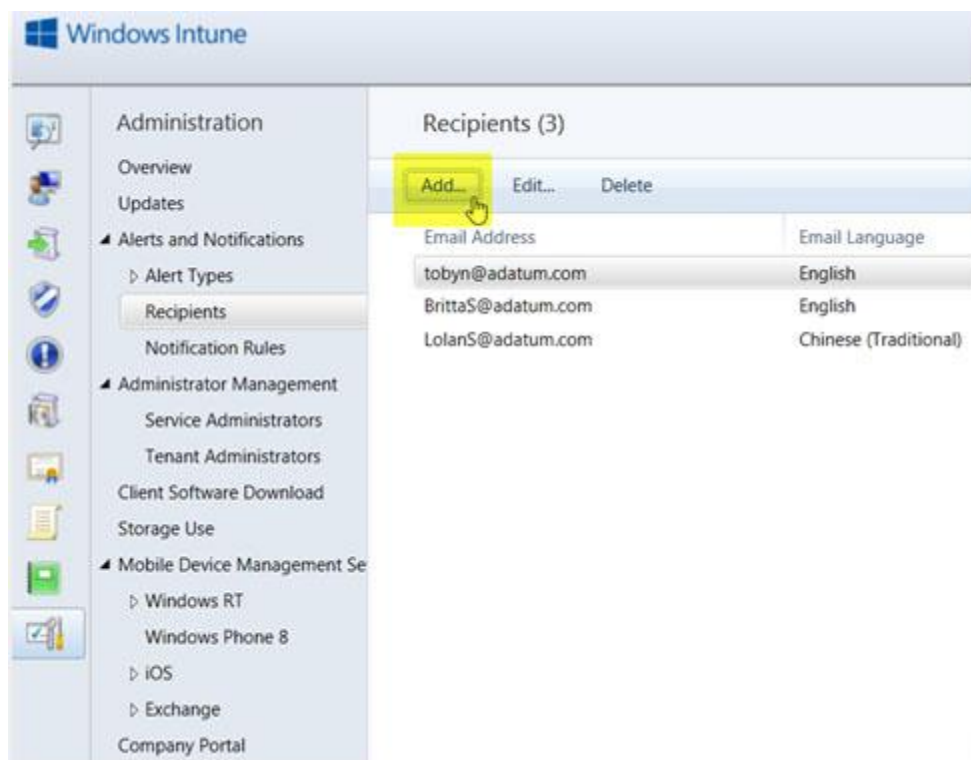


Figure 14. Add Recipient

3. Add the required notification email aliases.
4. Next select **Notification Rules** and select the Alert rules for which you want to send emails.
5. Click **Select Recipients** as highlighted in Figure 15.

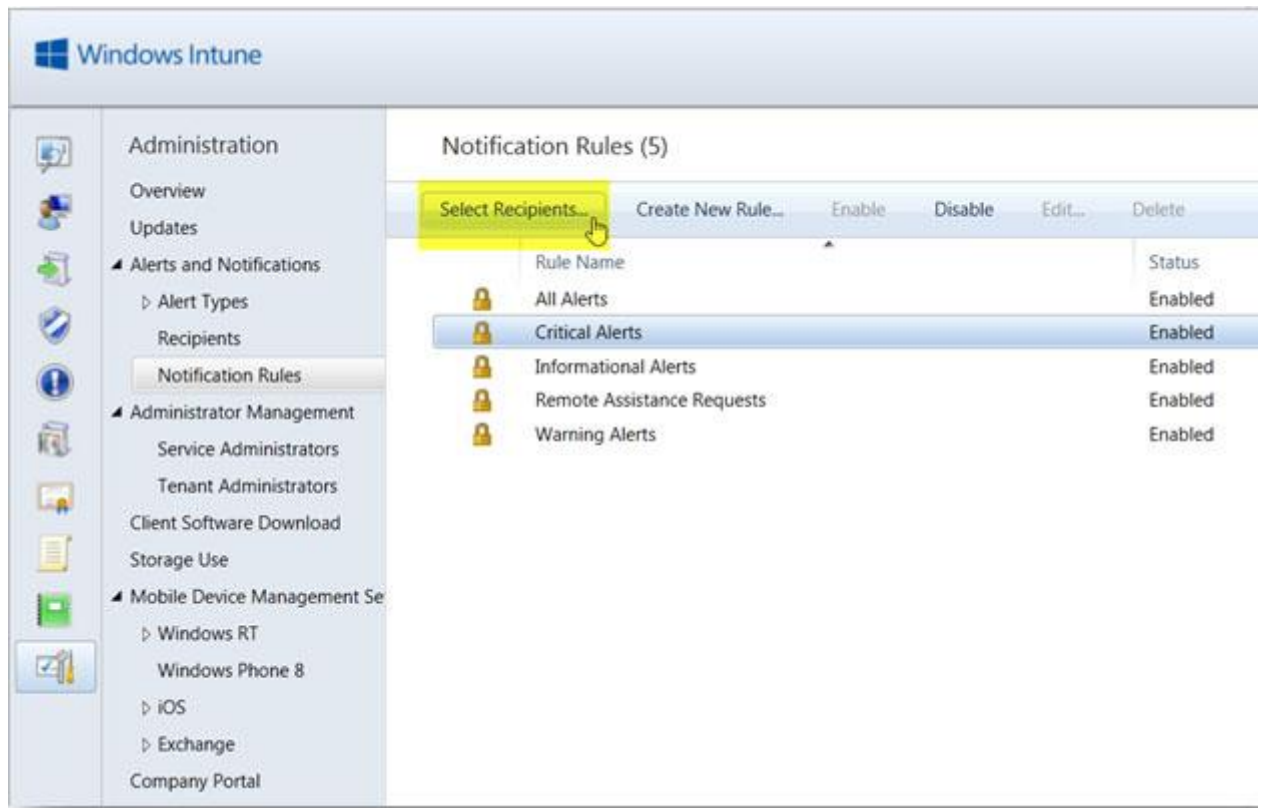


Figure 15. Select Notification Rule

6. Select the email recipients who will receive an email for these alerts.

## Creating Reports

Reports can help you answer a range of questions, such as how many computers have a particular application or update installed, what malware was blocked, or which users needed Remote Assistance over the last month. Windows Intune provides a set of built-in report templates that can be used as-is, or you can create custom reports based on views within the Windows Intune workloads.

These reports can be printed or exported, either in HTML format or as comma separated value (CSV) files. With the export feature, you can take Windows Intune data and import it into whatever program you use for analysis. For example, you can import the data into Microsoft Excel and create tables and graphs for use in management presentations.

---

## Customizing Report Templates

The following steps show how to create a Windows Intune Update report to identify computers that have pending updates:

1. Click the **Reporting** workspace tab.
2. Click **Update Reports**.
3. Customize the report settings to look like those in Figure 16.

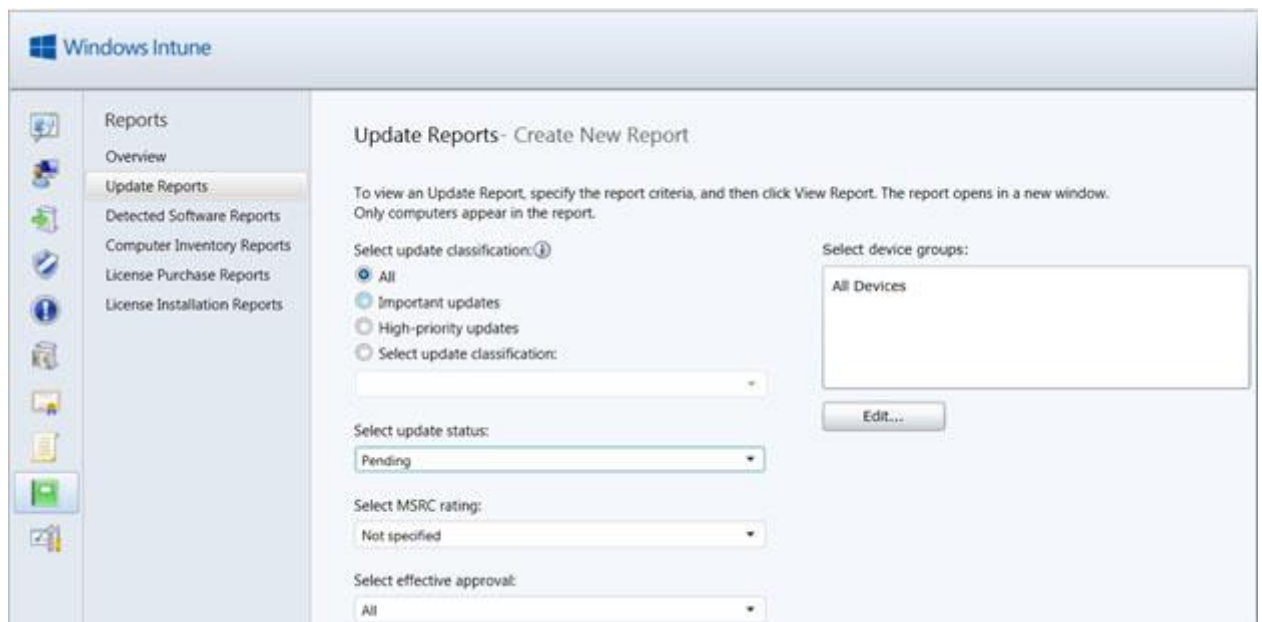


Figure 16. Custom Update Report

4. Click **View Report**

This action generates a report similar to that shown in Figure 17. This information can help you identify and troubleshoot computers with outstanding updates.



Update Title	Classification	Approved
> Update for Internet Explorer Flash Player for Windows 8 for x64-based Systems (KB2755399)	Critical Updates	Yes
> Update for Windows 8 for x64-based Systems (KB2751352)	Critical Updates	Yes

Figure 17. Custom Update Status Report

# Using Windows Intune to Distribute Software Applications and Non-Microsoft Updates

Hubone Note: Whilst application deployment is possible via Windows Intune, we would recommend that this is only undertaken by trained administrators.

Windows Intune lets you deploy and install software on computers and mobile devices in your organization. You can accomplish two types of installations using Windows Intune: a **required install** which automatically installs or pushes the software to managed computers, and an **available install** which deploys the software, or a link to the software, to the Windows Intune company portal so that users can choose whether to install it on their computers or mobile devices. These two types of installations necessitate different considerations when deploying software.

The following terms help in understanding the process:

- **Managed software** is any software that you deploy to your organization using Windows Intune.
- **Detected software** lists an inventory of any product or program that exists on managed computers.
- **Required install** is any software that you deploy using Windows Intune that you want to be installed without user interaction on the users' computer.
- **Available install** is any software that you deploy to be made available for targeted users on the Windows Intune company portal or on mobile devices.

## Software Distribution Topics

The topics in this section include step-by-step procedures for software distribution.

- [Checklist for Deploying Software using Windows Intune](#)

Follow these tasks learn about and configure your software deployments.

- [Planning for Software Distribution in Windows Intune](#)

The content in this section describes the necessary prerequisites for deploying software.

- [Adding and Deploying Software in Windows Intune](#)

The content in this section describes the process to add and deploy software by using Windows Intune.

- [Monitoring the Deployment Status in Windows Intune](#)

The content in this section describes how to monitor the status of software in Windows Intune administrator console after you have deployed your software.

- [Troubleshooting Software Distribution in Windows Intune](#)

The content in this topic describes troubleshooting procedures for the software distribution process.



## PC Rebuilds

Hubone Note: Whilst PC Rebuilds are possible using your software licenced via Windows Intune, we would recommend that this is only undertaken by trained staff.

### Typical Steps Required to build a PC

- Download software - Your Windows ISO image and licence file are available from the subscriptions section of the Account Portal:  
<https://account.manage.microsoft.com>
- Burn image onto USB key or DVD
- **Important:** Make a note of what devices are installed on the machines to be rebuilt. It may be a good idea to copy any existing drivers if they are in a convenient folder on the machine.
- **Important:** Make sure you are connected to your network with a physical cable, your wireless drivers may not work at first
- Using your new Windows DVD/USB Key build the machines with a clean Windows install
- Call the default user USER with a password of NewBuild123
- Reinstall/Download any manufacturers drivers required to get the machines to work.
- Join your Active Directory domain (If required – you will need the Domain Administrator Password)
- Install Windows Intune Client
- Install Office2013
- Install any other software you need
- Install printers