



Getting Started Guide: *Getting the most out of your Windows Intune cloud service*

Contents

Overview	3
Which Configuration is Right for You?	3
To Sign up or Sign in?	4
Getting Started with the Windows Management Portals	5
Configure Your Windows Intune Environment	7
Adding Administrators	8
Setting Your Default Policies	10
Planning for Endpoint Protection and Managed Computer Bandwidth Usage	11
Add Users and Groups, Computers, and Mobile Devices to Windows Intune	12
Adding Users and Security Groups	12
Managing User and Device Groups	13
Enrolling Computers	14
Administrator Enrollment	15
User Enrollment	16
Embedding in a Deployment Image	16
Enrolling Mobile Devices	17
Preparing for Device Enrollment	17
Enrolling a Windows RT Device	19
Enrolling a Windows Phone 8 Device	20
Enrolling a iOS Enrollment Device	22
Uploading Applications	22

Mobile Device Line of Business (LOB) Software Publishing	22
Optimizing Your Environment.....	25
Manage Update and Automatic Approvals.....	25
Set up Alert Notifications.....	26
Creating Reports	27
Customizing Report Templates.....	28
Summary	29
Resources:.....	29

Overview

Get the most out of Windows Intune.

This document is designed to help you evaluate the main features of Windows Intune and set up your new Windows Intune environment. To facilitate this process, this document uses an example configuration for a business called Adatum. Throughout this paper, you will see screenshots taken from this environment that illustrate how you can similarly configure your Windows Intune environment. Subsequently, you can implement the documented steps to create and customize your environment to meet your own business needs.

Which Configuration is Right for You?

As with previous releases, Windows Intune can still be operated in classic cloud-only mode, which doesn't require on-premises infrastructure. In this case, your configuration will look like Figure 1.

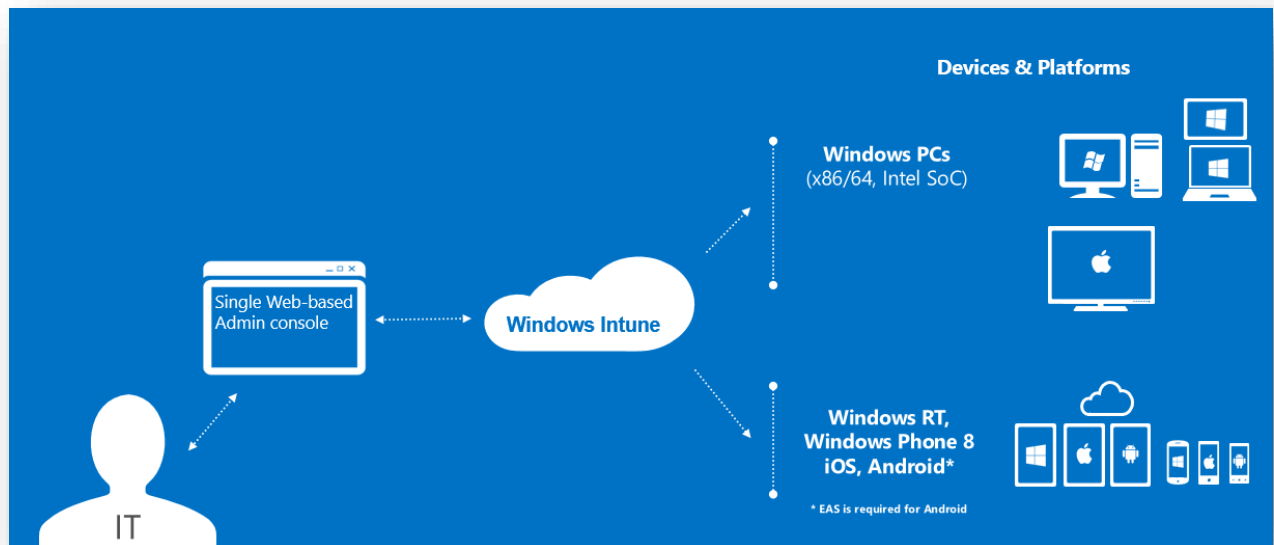


FIGURE 1: WINDOWS INTUNE IN THE CLOUD CONFIGURATION

However, this release of Windows Intune also introduces a new unified configuration option that can integrate this cloud-based environment with Microsoft System Center 2012 Configuration Manager with Service Pack 1 (SP1). This integrated cloud/on-premises solution uses the Configuration Manager console to help you manage personal computers, servers, mobile devices, and even Mac OS computers from a single location—the Configuration Manager console. Add the Windows Intune service to the Configuration Manager management console through a connector. Figure 2 shows an example of how the unified configuration manages all supported platforms.

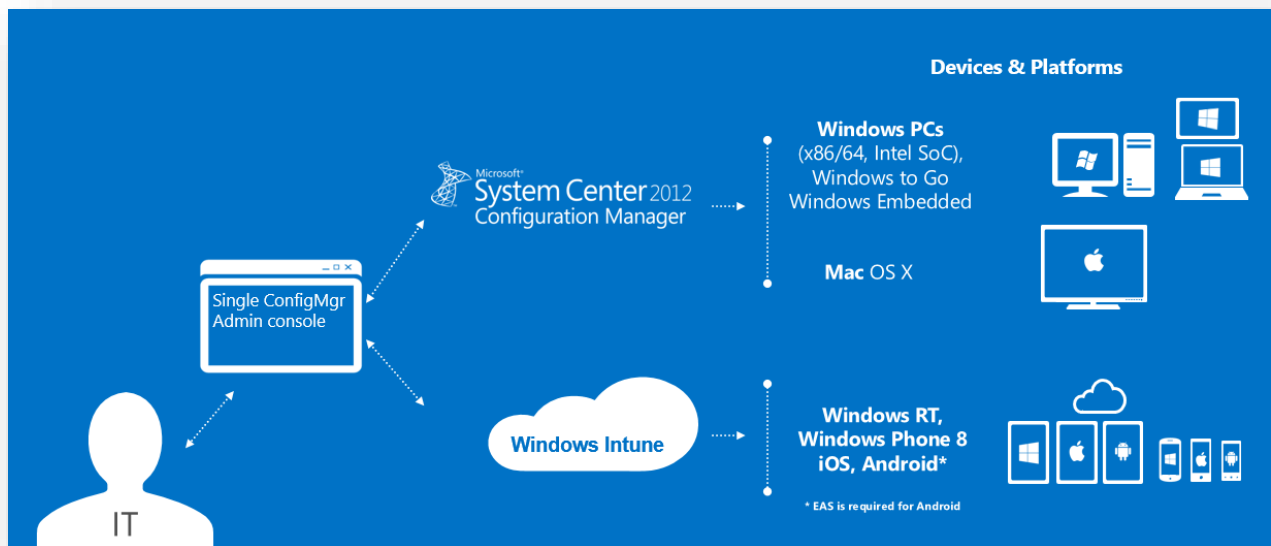


FIGURE 2: WINDOWS INTUNE IN THE UNIFIED CONFIGURATION

If you plan to use this unified configuration, the following website provides detailed technical guidance on how to set up System Center 2012 Configuration Manager: [Getting Started with System Center 2012 Configuration Manager](#)

The remainder of this guide focuses on the cloud configuration and is designed to help you get up and running quickly with your Windows Intune service.

To Sign up or Sign in?

Important

If your organization has an Enterprise Agreement (EA), you should contact your Microsoft representative and he or she will work with you to set up your enterprise trial.

If you are a small or medium sized business without an Enterprise Agreement or equivalent volume licensing agreement with Microsoft, you can sign up for a free 30-day trial of Windows Intune by visiting:

<http://www.microsoft.com/en-us/windows/windowsintune/tryandbuy>

If you click the “get your free 30-day trial now,” button at the top of the page you will be directed to the Sign up page. At the top left of this page is the following message:

If your company is already using Microsoft Online Services for services such as Microsoft Office 365, we recommend that you use the same user ID to sign up for Windows Intune. [Learn more](#) about why it is important to sign up with the same User ID. [Sign in](#)

If your organization already has a Microsoft Online Services organization identifier (OrgID), it is essential that you click the **Sign in** option in this text and authenticate by using the Global Administrator account. This action will ensure that your Windows Intune trial links to your existing Microsoft Online Services account.



Important

You should only complete the details on this Sign Up form and create a new domain name for your organization if you have no existing Microsoft Online Services account.

After you have entered this information, an email will be sent to the email address associated with this account to confirm that the account is active.

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: the Account Portal in Figure 3 and the Admin Portal in Figure 4.

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

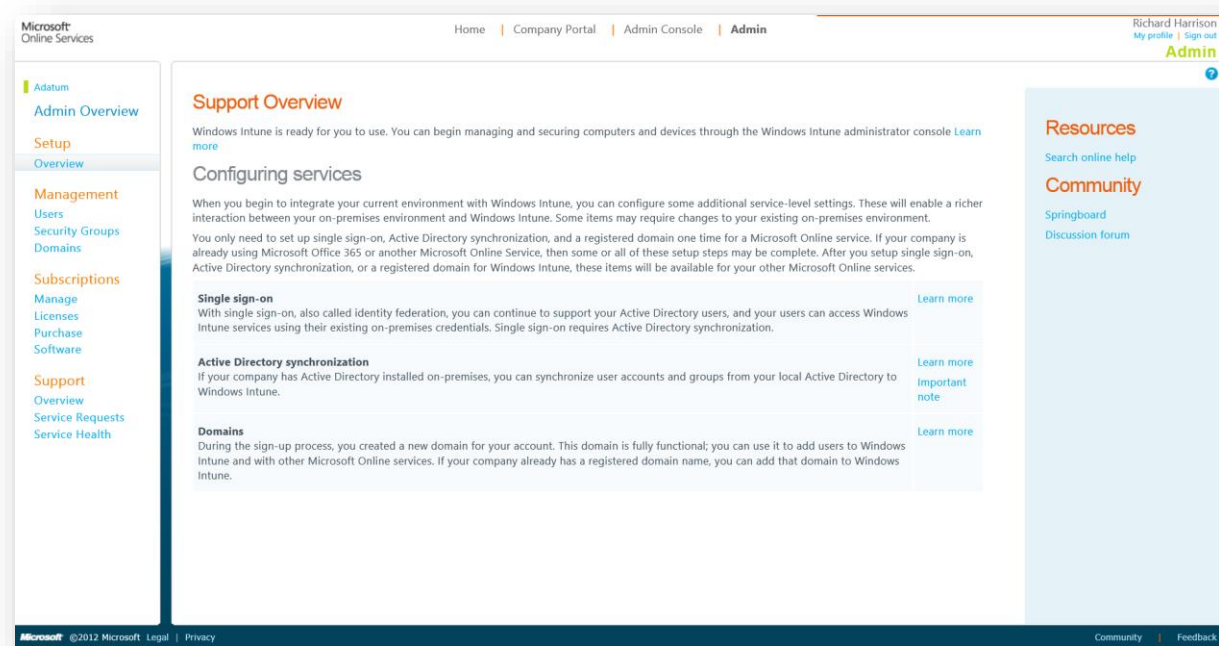
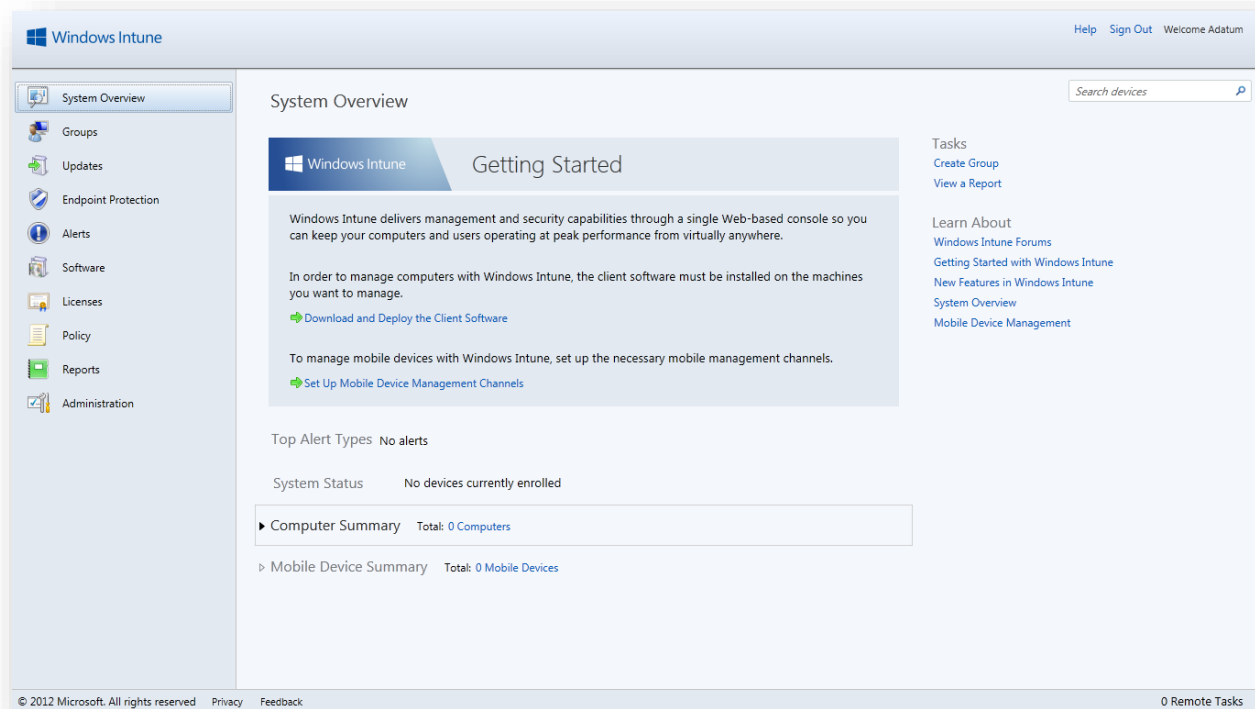


FIGURE 3: WINDOWS INTUNE ACCOUNT CONSOLE

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. It is also where you can set up and configure the link to your on-premise Active

Directory Domain Service (ADDS) instance. In addition, end users can use the portal to change their passwords.



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

FIGURE 4: WINDOWS INTUNE ADMINISTRATION CONSOLE SYSTEM OVERVIEW SCREEN

In the figure above, you can see the three main information panels for Windows 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.

If you are in the process of setting up your Windows Intune solution, you may not have much information to display. However, you can start to familiarize yourself with the workspaces and tasks available in each area until you start enrolling computers.

Configure Your Windows Intune Environment

Now that your account has been set up, there are some steps to go through before you start adding computers and mobile devices to your account.

Adding Administrators

To help ensure an organization can delegate administrative roles effectively, Windows Intune offers two levels of administrator roles. Both provide access to the Windows Intune administrator consoles:

- **Windows Intune Tenant Administrator:** Tenant Administrators have full administrative rights to the Windows Intune administrator console. They can perform all operations in the console, including adding or deleting Windows Intune service administrators. In addition, they can assign other tenant administrators. Note that Tenant Administrators must be assigned in the Windows Intune account portal; you cannot use the Windows Intune administrator console to assign a Tenant Administrator.



Note

When you subscribe to Windows Intune, your first User ID automatically becomes a Global Administrator for Microsoft Online Services and a Tenant Administrator for the Windows Intune administrator console. As a Global Administrator for Microsoft Online Services, you have the same privileges across all Microsoft Online Services for your organization, and you can add other Tenant Administrators for the Windows Intune administrator console.

- **Windows Intune Service Administrator:** Service Administrators have the following two levels of console access:
 - **Full access:** These Service Administrators have full administrative rights to the Windows Intune administrator console and can perform all operations in the console, including adding or deleting other Service Administrators.
 - **Read-only access:** These Service Administrators have read-only rights and cannot modify data in the console; they can only view data in the console and run reports.

You can create Service Administrators by using the Windows Intune administrator console. These administrators must have a user ID and password, and they must be a member of the Windows Intune user group. If an individual does not have a user ID, a Tenant Administrator must create one by using the Windows Intune account portal and then ensure that the individual is a member of the Windows Intune user group.



Note

The Windows Intune Service Administrator and the Service Administrator displayed in the Windows Intune account portal are two different entities. The Service Administrator for Microsoft Online Services that is displayed in the Windows Intune account portal manages the users accounts and groups, service requests, and monitors service status but not necessarily the status of the users and devices managed by Windows Intune.

By default, the subscription owner becomes the Tenant Administrator for your Windows Intune service. The Tenant Administrator is the individual who accepted the Microsoft Online Subscription Agreement (MOSA) at the time of purchase, which entitles him or her to perform all tasks in the Windows Intune administrator console.

We recommend that you create a least one extra Tenant Administrator Account to help delegate tasks and ensure you don't get locked out of your Windows Intune account if you forget your password. To create a Tenant Administrator account:

1. Log on to the Windows Intune Account Console and click the **Users** menu item under **Management**.
2. Click the checkbox next to the user you wish to promote to a Tenant Administrator and click **Edit**, or click **New** to add a new user.
3. Select **Settings** and under **Assign role**, click the **Yes** radio button and select **Global Administrator**. Figure 5 shows this selection.

The screenshot shows the 'Assign role' dialog for user Toby Nixon. The dialog has tabs for 'Details', 'Settings', and 'Group', with 'Settings' selected. Under the 'Assign role' section, there is a question: 'Do you want this user to have administrator permissions?' with 'Yes' selected. A dropdown menu is open, showing a list of roles: '(Select a role)', 'Allows ability to perform tier1 support tasks.', 'Allows ability to perform tier2 support tasks.', 'Allows access to various read only tasks in the directory.', 'Billing administrator', 'Global administrator' (highlighted), 'Password administrator', 'Service administrator', and 'User management administrator'. Below the dropdown, there is a 'Blocked' option which is not selected. At the bottom, there is a 'Set user location' section with a dropdown menu set to 'United States' and 'Save' and 'Cancel' buttons.

FIGURE 5: ADD TENANT ADMINISTRATOR

4. Enter the user's alternate email address and click **Save**

The Tenant Administrator account should not be used for day-to-day IT support and management tasks. For that purpose, you should set up Service Administrators. To add Service Administrators:

1. In the Windows Intune Account Portal, create user accounts for the users that you want to enroll as Service Administrators.
2. Log on to the Windows Intune Administration Console and check that those users appear in the **All Users** group.
3. Click **Administration** and **Service Administrators**.

4. Click **Add Administrator** to display a window similar to that in Figure 6.

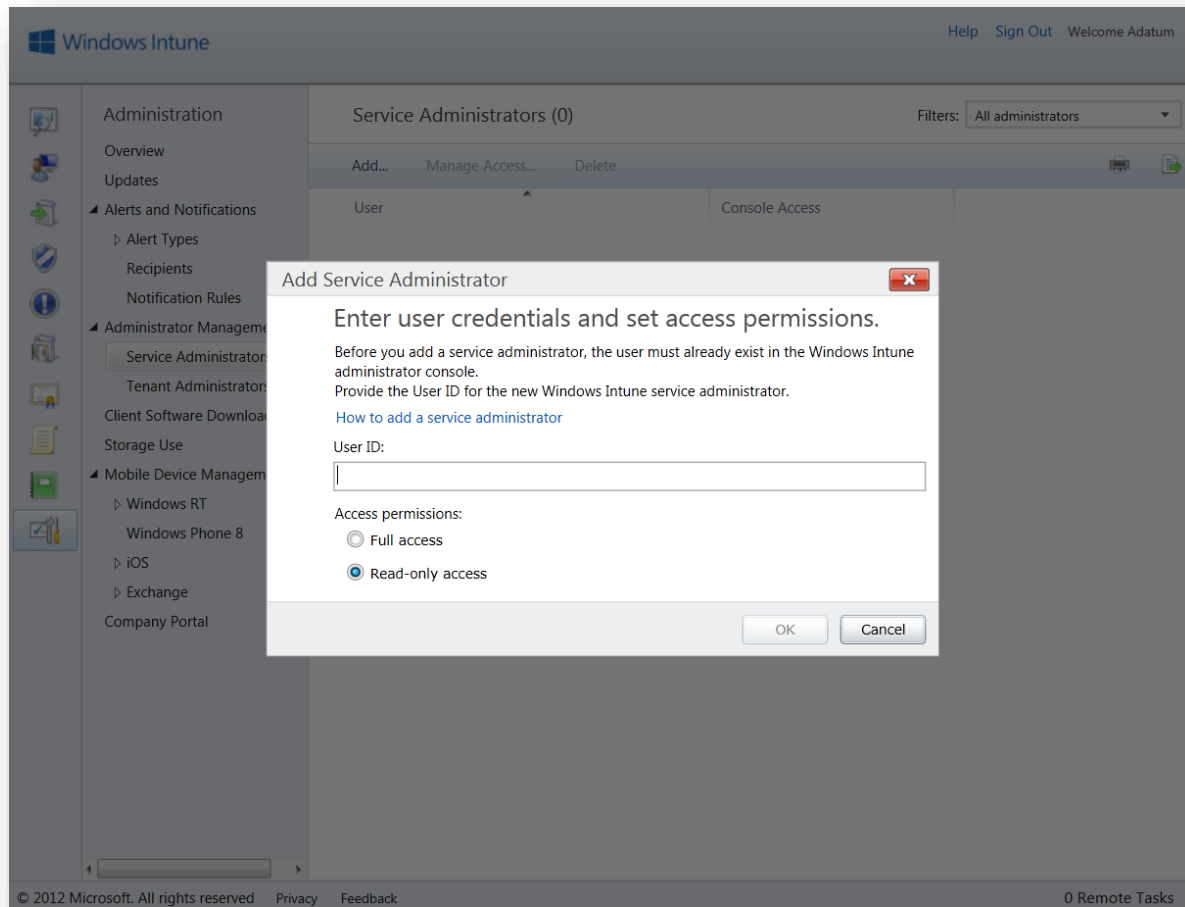


FIGURE 6: ADD SERVICE ADMINISTRATOR

5. Enter the User ID and select the access permissions for that user, then click **OK**.
6. Repeat the previous step for all User IDs that you wish to make Service Administrators of this Windows Intune account.

After you have set up administrators, you can configure the environment into which you will deploy devices. Over the next few pages, we will review some additional steps that you are recommended to perform before you start deploying computers or mobile devices into your account.

Setting Your Default Policies

Windows Intune policies focus on providing you with straightforward settings that help control the security settings on mobile devices, provide computer updates, ensure Endpoint Protection, maintain firewall settings, and enhance the end user experience. These settings apply both to domain-joined computers in any domain and to non-domain joined computers.



Note

To avoid policy conflicts that can result from competing policy management systems, you should ensure that when you deploy the Windows Intune client software, those computers that Windows Intune policy manages do not also receive the same configuration settings from Active Directory Group Policies. For more information, see [Planning Around Group Policy](#) in Online Help.

The following procedure describes how to set up a Windows Intune Agent Settings policy for computers.

▶ To set up the default Windows Intune Policies

1. Open the Windows Intune administrator console.
2. In the workspace shortcuts pane, click the **Policy** icon.
3. Under **Tasks**, click **Add Policy**.
4. In the **Create a New Policy** dialog box, the following policy templates are displayed in the list of templates in the left pane:
 - Mobile Device Security Policy
 - Windows Firewall Settings
 - Windows Intune Agent Settings
 - Windows Intune Center Settings



Note

For detailed information about specific policy settings, see [Policy Settings Reference](#) in Online Help.

5. Select the policy template you wish to set up and click **Create and Deploy a Policy** with the Recommended Settings. To view the settings before you create the policy, click **View the recommended settings that will be used as the default for this policy**.
6. After you configure the settings that you want to apply in your default policy, type a name and an optional description for the policy, and then click **Save Policy**.
7. When prompted to specify whether you want to deploy the policy now, click **Yes**.
8. In the **Select the groups to which you want to deploy this policy** dialog box, select the **All Devices** group or **All Users** group (depending on the policy you have selected) and click **OK**.
9. Repeat these steps as needed for your other default policy settings.

After these policies have been deployed, all users or devices inherit these settings as their baseline policy. You can then review and, if required, edit the details of these policies from the Policy workspace.

Planning for Endpoint Protection and Managed Computer Bandwidth Usage

Before you add computers to the Windows Intune service, consider your requirements for Endpoint Protection. If you have an existing Endpoint Protection application, you should determine whether you want to use Windows Intune Endpoint Protection or continue with the current application. For information about how to implement either approach so that your managed computers are not left in an unsecured state, see [Replacing Your Existing Malware Protection](#) and [Continuing to Use Your Existing Malware Protection](#) in Online Help.

Remember that Windows Intune-managed computers use additional network bandwidth for Windows Intune-related operations. Before you install the Windows Intune client software consider the existing network traffic and the increase that will result from implementing Windows Intune. For information about the variables that affect bandwidth planning for Windows Intune and for comprehensive deployment planning guidance, see [Planning for Client Deployment and Enrollment](#) in Online Help.

Add Users and Groups, Computers, and Mobile Devices to Windows Intune

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 do one of the following:

- Manually add users or security groups, or both, to the account portal.
- Use Active Directory synchronization to populate the account portal with synchronized users and security groups.



Note

For detailed information about the directory synchronization process, see [Setup and Manage Active Directory Synchronization](#) in the Windows Intune Account console

▶ To add users 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 **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**.



Note

You can import multiple user accounts into Windows Intune from a single file source. The file must be a comma-separated values (CSV) file and adhere to the required format. For more information, see [Add Multiple Users with Bulk Import](#) in Online Help.



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).
The available members for the selected list type are displayed under **Available members**.
7. 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.
8. 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**.
9. 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 Administrator Console 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.

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, whereas the **Unassigned Computers** group will contain computers that have not been assigned to a group yet by the systems administrator.

- ▲ Departmental
 - 1_Engineering
 - 2_Sales
 - 3_Marketing
- ▲ Geographic
 - New York
 - San Francisco
 - Seattle
- ▲ Physical
 - Admin Desktops
 - Developer Desktops
 - Executive Laptops

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

These groups can be based on Active Directory Domain Service (ADDS) groups that you have in your domains, but the groups in Windows Intune do not replicate back to ADDS. As a result, you have the flexibility to make changes that can better meet your organization’s needs.

 **Note:** *The numbers in the group names in the Departmental example in Figure 7 are simply there to organize the listing order of the groups. By default, groups display alphanumerically.*

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.
- 3) **Embedding in a deployment image:** The Windows Intune Administrator embeds the Windows Intune service into the operating system deployment images.

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.

Warning

The Windows Intune package contains unique account identifiers. If unauthorized or malicious users gain access to the software package, they can add computers to the account that the embedded certificate represents. To help prevent unauthorized access, we recommend that you employ the following best practices:

- After you download the package, store it in a secure location.
- When you deploy the client software, put the package on a shared, secure location that only provides read-only access to required users. Remove any access permissions for the **Everyone** group.
- Protect the network that contains both the shared location and the destination client by using IPsec or a similar security technology.

To download the client software installation package

1. Open the Windows Intune administrator 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 earlier in this guide, 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.

Important

Do not rename or move the WindowsIntune.accountcert (ACCOUNTCERT) file that is included in the download, as this action will cause the client software installation to fail.

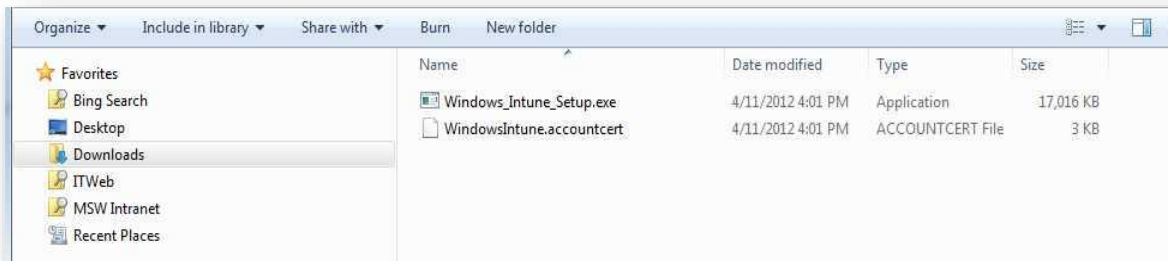
6. After the download is complete, click **Open Folder** and then follow the steps in the next procedure.

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.

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.

4. 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.
5. 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.

Users can access the Windows Intune company portal at the following address:

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

Embedding in a Deployment Image

The standard installation process requires a live internet connection to create a one-to-one relationship with the managed device and complete successfully. As a result, you cannot install the agent into a deployment image for multiple deployments, because it would create duplicate computer accounts in Windows Intune. In this case, you should use the *PrepareEnroll* command-line argument to schedule a task that will attempt to add the computer at a later time. For information about how to complete this type of installation, see [Installing the Client Software as Part of an Image](#) in Online Help.

Enrolling Mobile Devices

Before you can enroll mobile devices, you need to complete a few steps to prepare the account for the mobile devices you will be managing.

Preparing for Device Enrollment

First, you must prepare the Windows Intune service and enable mobile device management through the Windows Intune cloud service.



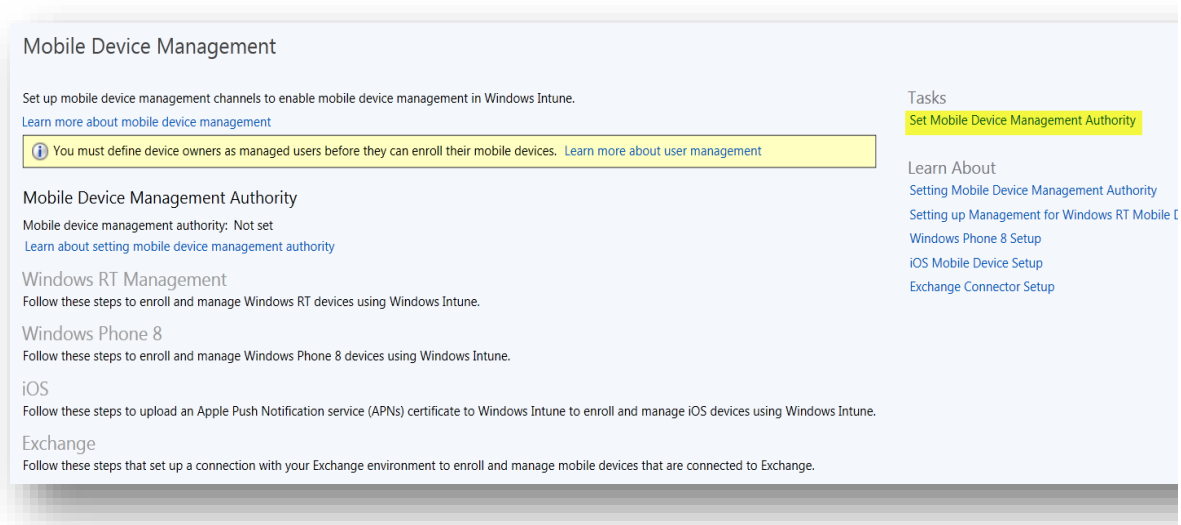
Important

If you intend to manage your mobile devices through System Center 2012 Configuration Manager with SP1, you should stop now and instead complete the MDM preparation from the Configuration Manager management console. For more details on this process see, [Getting Started with System Center 2012 Configuration Manager](#).

▶ To set up cloud-based MDM in the Windows Intune Administrator console

1. Log on to the Windows Intune Administration Console as a Service Administrator with full access.
2. Click the **Administration** workspace.
3. Click the **Mobile Device Management** menu option and then select **Set Mobile Device Management Authority** as highlighted in Figure 9.

FIGURE 9: MOBILE DEVICE MANAGEMENT AUTHORITY



4. At the **Set MDM authority window** select **Yes**.

After you have activated mobile device management in the Windows Intune Administrator console, you will need to complete the setup steps for each mobile device platform you are going to support. If you want to manage iOS devices, you will need to obtain an Apple Push Notification service (APNs)

certificate and then upload it to Windows Intune. For more information on this process see [iOS Mobile Device Management](#) in Online Help.

Setting up your Enrollment Server Address

Mobile devices require access to an enrollment server during the enrollment process. One option is to provide the address to your users so they can enter it manually during device enrollment. Alternatively, you can help automate the process by adding a Domain Name Service (DNS) record to your DNS server. This option requires you to have a verified domain name registered with your Windows Intune account.

For more information on setting up automatic detection of enrollment servers for your users, see [Setting up your DNS server for enrollment](#) in Online Help.

If you choose not to add a DNS record to your DNS server, your users will need to know the address for their device so they can enter it during the enrollment process this address is:

manage.microsoft.com

Windows Intune is now ready to manage your Windows RT mobile devices. However, if you also plan to support Windows Phone 8 or iOS devices, you will need to complete a few more steps to enable the required management channel for these devices.

Windows Phone 8 Device Setup

To manage Windows Phone 8 devices, you must first prepare the necessary code-signing certificate for your organization's applications and upload it to the Windows Intune service. It is deployed automatically during the device enrollment process, so that the device can then "sign" the Windows Phone 8 company portal app. The following table describes how to complete this process.

#	Step	Details
1	Get a Windows Phone Dev Center account and an Enterprise Mobile Code Signing Certificate.	Go to the Windows Phone Dev Center to get a company Publisher ID. Use your Publisher ID to purchase an Enterprise Mobile Code Signing Certificate. Typically these steps are only required once for an organization and will be used by your organization's app developers.
2	Sign your LOB app.	Download the Signtool from the Windows Phone 8 SDK at http://go.microsoft.com/fwlink/?LinkId=268439. To be used by end user mobile devices, the app must be signed by a Certificate Authority that is trusted by the target Windows Phone 8 devices. Use the Signtool app to sign your apps with your organization's Enterprise Mobile Code Signing Certificate.

3	Sign the Windows Phone 8 company portal app.	Download the Windows Phone 8 company portal app and using Signtool, sign the company portal app with your Enterprise Mobile Code Signing Certificate.
4	Upload and deploy the signed Windows Phone 8 company portal app.	From the Windows Intune administrator console, upload the signed company portal app file and deploy to all users.

After you have uploaded the signed company portal app, users who enroll their devices will be able have the portal app automatically downloaded onto their device during the enrollment process.

iOS Device Setup

To enable mobile device management for iOS devices, you must obtain an Apple Push Notification service (APNs) certificate and make it available to Windows Intune. The following table shows how to complete this set up process:

#	Step	Details
1	Download an APNs certificate request.	From the Windows Intune Administrator console, download the Apple Notification service certificate request and save it to your local computer.
2	Get a APNs certificate.	Create a APNs certificate in the Apple Push Certificates portal using the certificate request you created in the first step. Use a company Apple ID associated with an email account that will remain in possession of your company and not an individual. Save the certificate PEM file locally.
3	Upload the APNs certificate.	From the Windows Intune Administration console upload the APNs certificate to your Windows Intune account.

Enrolling a Windows RT Device

To enroll a Windows RT device, users should follow these steps on their device:

1. On the Windows RT device, bring up the Search Charm, select **Settings**, and search for "CompanyApps."
2. Start **Company Apps** and, when prompted, enter their *Windows Intune user ID credentials* and password.

3. If the Auto-enrollment DNS entry was not specified in the Administration console, enter the enrollment servers address for enrollment to complete.

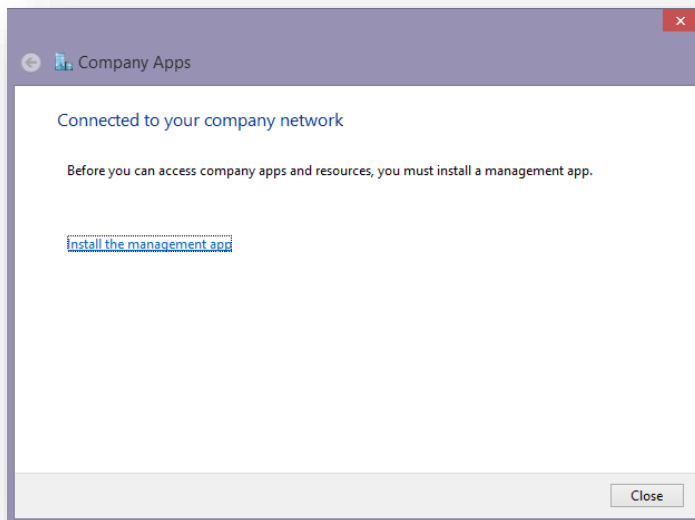


FIGURE 10: COMPLETING THE ENROLLMENT PROCESS

4. After the device has been enrolled, select the link to install the **company portal** application from the Windows Store.

Windows Intune can now manage the Windows RT device, and the authenticated user should be able to access company apps and manage their devices through the company portal.

Enrolling a Windows Phone 8 Device

To enroll a Windows Phone 8 device, users should follow these steps:

1. Initiate enrollment through the Windows Phone 8 device by going to **system settings** and selecting **company apps**, as shown in Figure 11.

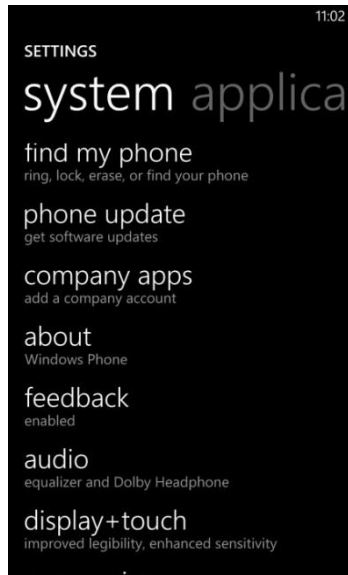


FIGURE 11: COMPANY APPS SETTING

2. The enrollment process prompts users for their company credentials. If the Auto-enrollment DNS entry was not specified in the Administration console, the user must provide the enrollment server's address for enrollment to complete.
3. Successful authentication establishes a relationship between the user, the Windows Phone 8 device, and the Windows Intune service, at which point an authentication certificate will be installed on the device. To enable device management, users should check the box "**Install company app or Hub.**" If users do not check the box they will not be able to download the company portal. Figure 12 shows this setting.

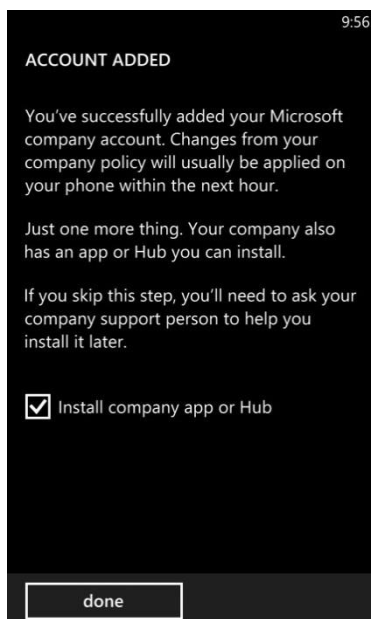


FIGURE 12: ENABLING INSTALLATION OF THE COMPANY PORTAL

4. The company portal then installs on the device, enabling Windows Intune to collect inventory and apply management settings. Users should now have access to LOB apps through the Windows Phone 8 company portal app.

Enrolling a iOS Enrollment Device

To enroll an iOS device, users should follow these steps:

1. Browse to the Windows Intune company portal website directly from the web browser on the device. Alternatively, the administrator can send the user an email invitation that includes a link to the company portal and their User ID details.
2. Enter Windows Intune user credentials to start the enrollment process.
3. Accept the prompt to install the company's management profile.
4. Successful authentication establishes a relationship between the user, the iOS device, and the Windows Intune service.
5. Windows Intune collects inventory and applies management settings and users now have access to LOB apps through the web-based Windows Intune Mobile company portal at:
<https://m.manage.microsoft.com>.

Uploading Applications

As with previous versions of Windows Intune, you can deploy *.exe* and *.msi* applications directly to the Windows PCs being managed by Windows Intune by using the Admin console to deploy applications to device groups.

New in this release, however, is the ability to make *.appx*, *.xap*, web apps, and public store apps (through deep links) available for users to install for themselves from the Windows Intune company portal. These new applications are published to the company portal application or web site so the users can select the apps they need. The following table shows how each platform can access the company portal.

Experience	Windows 8	Windows RT	Windows 7, Vista, XP	Windows Phone 8	iOS	Android
Company Portal App	✓	✓	✗	✓	✗	✗
Web Page	✓ ¹	✓ ¹	✓	✓ ¹	✓	✓

¹-App installation is provided through the company portal app for these platforms.

Mobile Device Line of Business (LOB) Software Publishing

There are two ways to deploy applications to mobile devices with Windows Intune:

- **External link:** Use the Add Software wizard in the Admin console to set up links to applications in the Windows Store, Windows Phone Store, Apple App store, and Google Play. These can then

be published to users through the Company Portal. In addition, you can provide links to web-based applications that will run on the device through the device's own web browser.

- **Software installer:** You can provide a signed application package that is then uploaded by the Administrator to the Windows Intune service directly and then "sideloaded" onto the managed devices. Sideloaded apps enable you to distribute an app directly to a device without going through a public application store.

The following table shows the mobile device platforms to which Windows Intune can sideload and the software file types required for each platform:

Platform	File type
Windows RT	.appx
Windows Phone 8	.xap
iOS	.ipa & .plist manifest file
Android	.apk

To publish applications to these devices requires that you have the necessary certificates and keys in place to enable your signed applications to install. The following section explains the steps required to enable application publishing for each of your supported device platforms.

Windows 8 Application Setup

To enable application publishing for Windows 8, you will first need to obtain your sideloading key. To obtain this key from Microsoft, sign into the Volume Licensing Service Center (VLSC) and complete the steps outlined in the following table.

#	Step	Details
1	Obtain and upload a sideloading key.	Before you can install sideloaded line of business (LOB) apps on Windows 8 devices, you must obtain and activate sideloading keys from the VLSC . For more information about sideloading product activation keys, see Microsoft Volume Licensing . You then upload your sideloading key from the Windows Intune Administration console.
2	Upload code-signing certificate	If you have a certificate from your company's Certificate Authority, log in to the Windows Intune Administrator console and use the Modify Code-Signing Certificate option to specify the code-signing certificate you want to use for your LOB Windows 8 apps. Note that all LOB apps must be code-signed but if you have a public key that is part of a trusted certificate chain you will not need to add an additional code-signing certificate here. You will only need this configuration change if you are signing your applications with a certificate that cannot be verified by the device using one of the public certificate authorities.

Users of managed Windows RT devices will now be able to install your published LOB apps on their devices. To enable these LOB apps to be sideloaded on Windows 8 PCs some additional steps may be required, take a look at the [Windows 8 Sideload Requirements](#) TechNet page for more details.

Windows Phone 8 Application Setup

Sideloaded Windows Phone 8 apps onto a device requires that your developers sign the apps with the Enterprise Mobile Code Signing certificate you obtained during the Windows Phone 8 device set up phase earlier. The following table demonstrates how to complete this process.

#	Step	Details
1	Sign your LOB app.	Use the Signtool app from the Windows Phone 8 SDK to sign your apps with your organization's Enterprise Mobile Code Signing Certificate.
2	Upload and publish LOB apps.	You can now upload your signed LOB apps from the Windows Intune administrator console and deploy them to the target users.

iOS Device Setup

For Windows Intune to manage iOS devices, you will have to obtain an Apple Push Notification service (APNs) certificate and make that certificate available to Windows Intune. Additionally, any LOB applications need to be signed by a valid iOS Developer Enterprise Program certificate so that the iOS device will accept the application. Use the following table to complete this setup process.

#	Step	Details
1	Join the iOS Developer Enterprise Program.	If you plan to develop in-house iOS applications that you wish install with Windows Intune, you must purchase membership in the iOS Developer Enterprise Program. Note: A Dun & Bradstreet (D-U-N-S) Number is required for enrollment. If you are commissioning an external developer to create your line of business iOS applications, you must make sure they are able to sign your application with a valid iOS Developer Enterprise Program certificate.
2	Sign all apps you plan to deploy to iOS devices.	You, or your iOS developer, must sign all apps you want to deploy to iOS devices with the same certificate.
3	Upload and publish LOB apps.	Now the apps can be uploaded using the Windows Intune administrator console. Then by using the Manage Deployment wizard the app can be targeted to the required users.

Optimizing Your Environment

The next section reviews how you can configure elements of your Windows Intune environment to optimize both your users' and your administrators' service experience.

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.

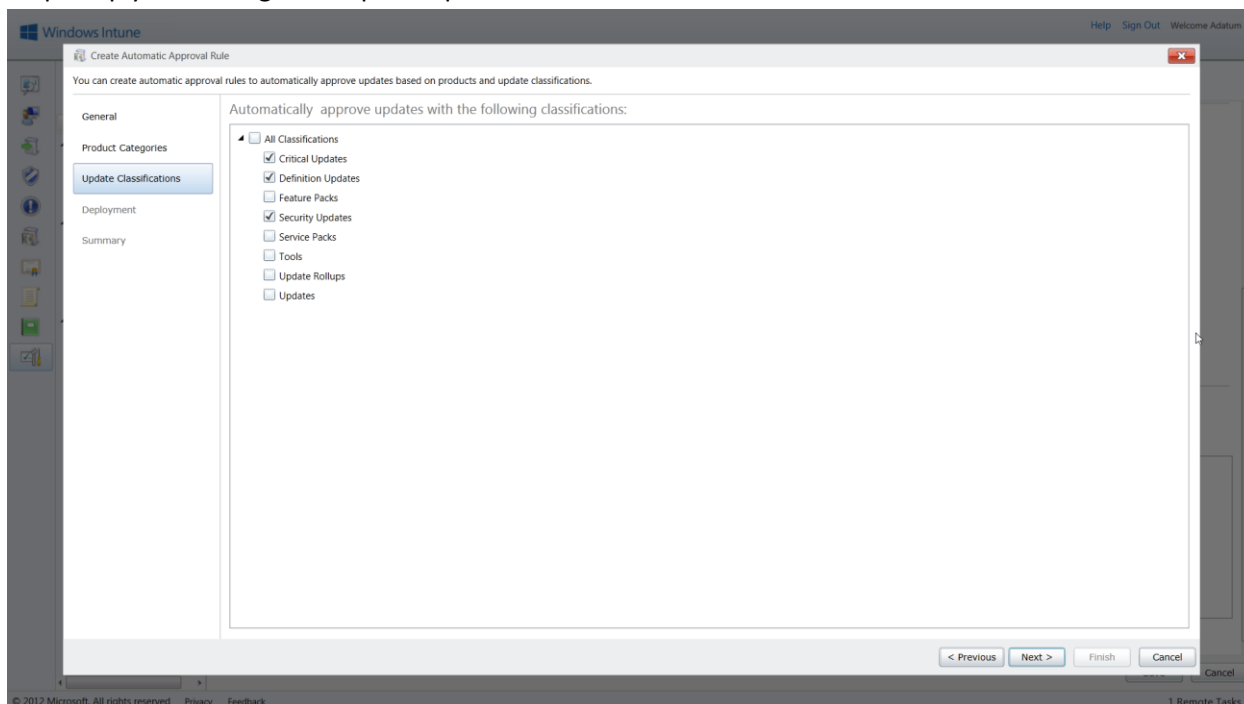


FIGURE 13: APPROVAL RULE CLASSIFICATIONS

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.

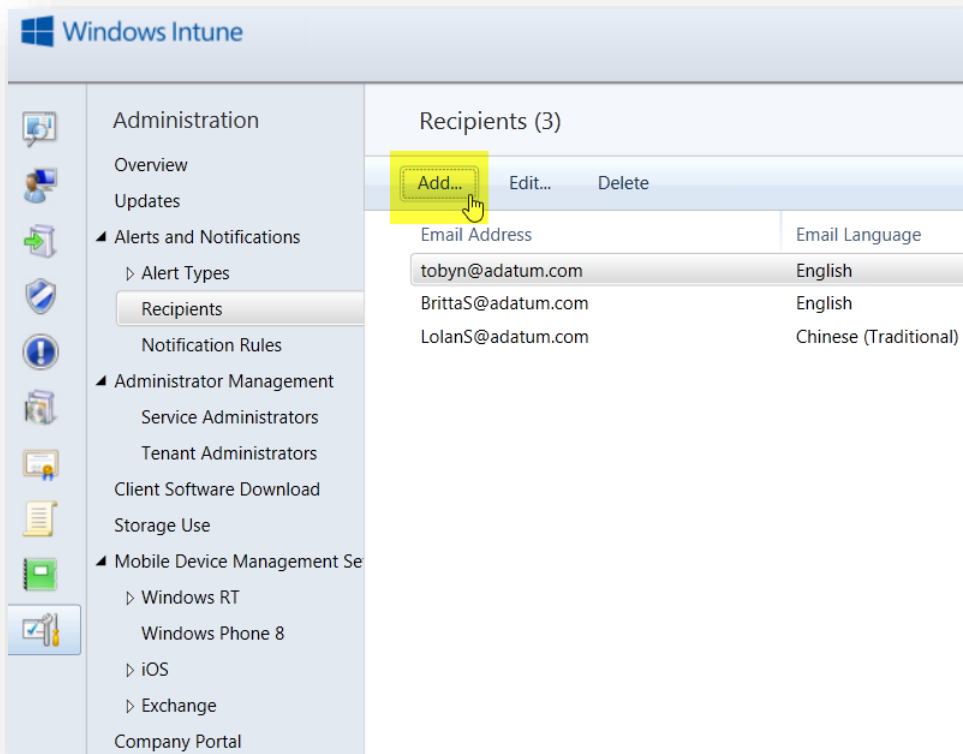


FIGURE 14: ADD RECIPIENT

3. Add the required notification email aliases.

Note: Being an alert recipient does not automatically grant access to the Windows Intune Administration console. If you want to allow any of these recipients to log on to the console, you must add them as an administrator.

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.

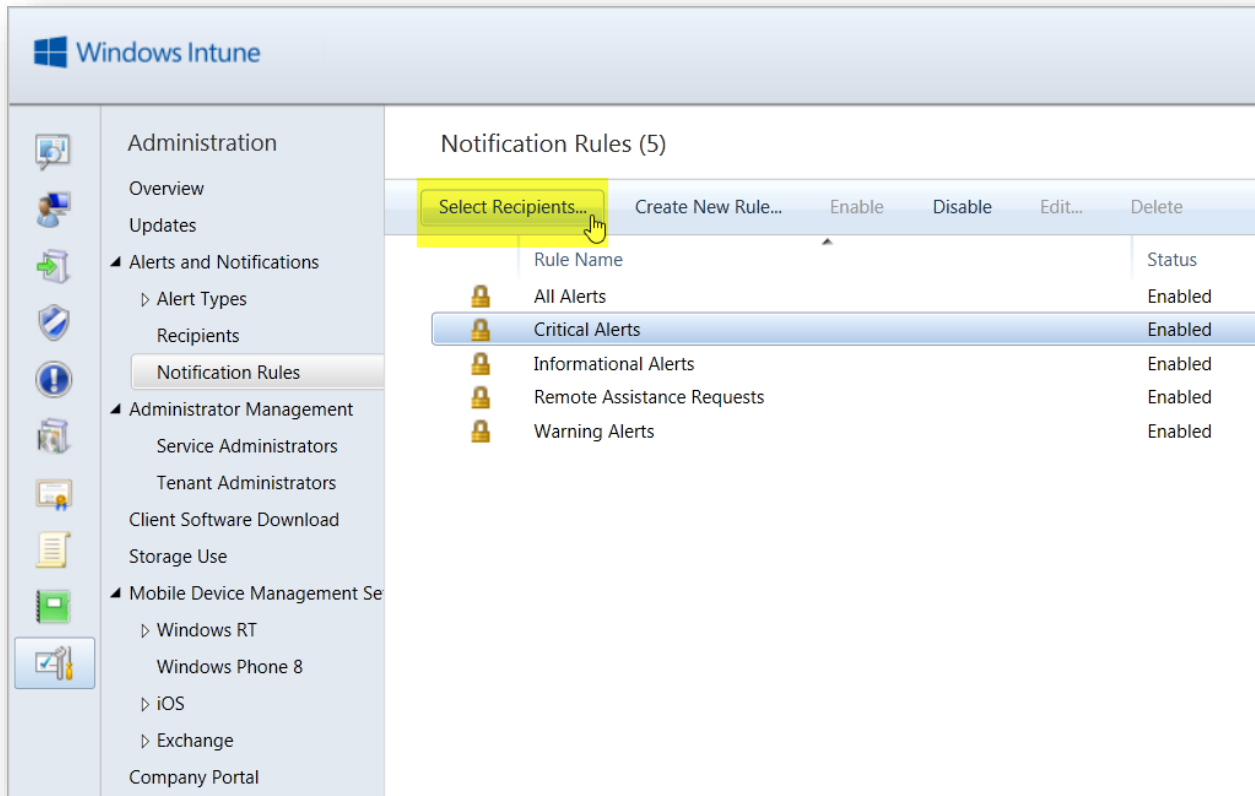


FIGURE 15: SELECT NOTIFICATION RULE

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

We recommend that you set up notifications for Remote Assistance Requests, as these requests usually require an immediate response.

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:

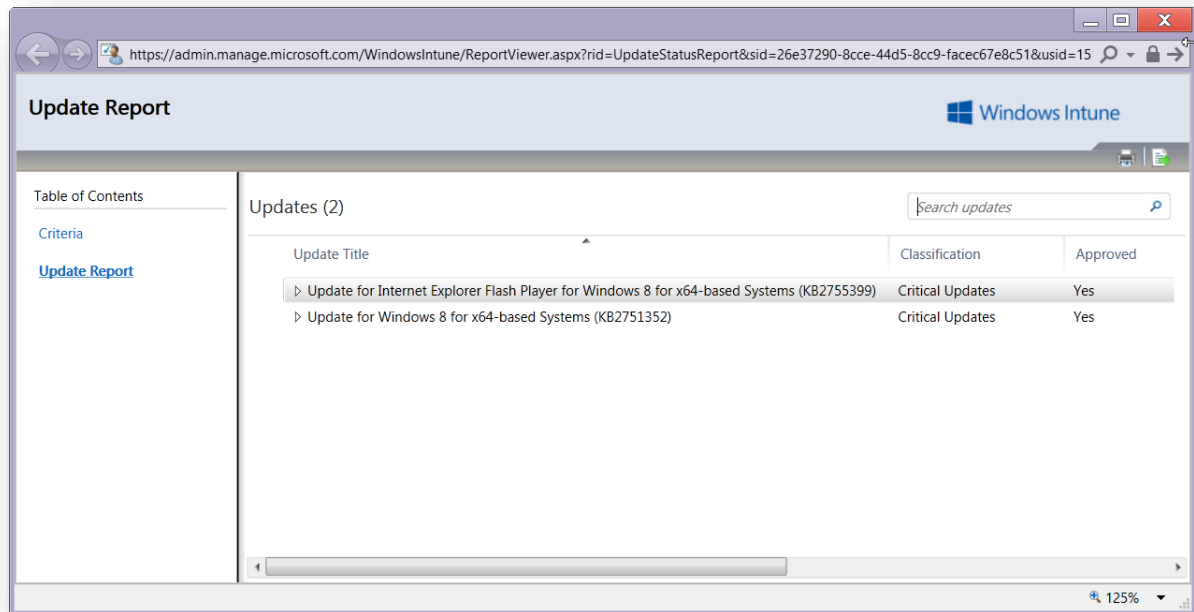
1. Click the **Reporting** workspace tab.
2. Click **Update Reports**.
3. Customize the report settings to look like those in Figure 16.

The screenshot shows the Windows Intune management console. On the left is a navigation pane with icons and labels for 'Reports', 'Overview', 'Update Reports', 'Detected Software Reports', 'Computer Inventory Reports', 'License Purchase Reports', and 'License Installation Reports'. The 'Update Reports' section is selected. The main area is titled 'Update Reports - Create New Report'. It contains a brief instruction: 'To view an Update Report, specify the report criteria, and then click View Report. The report opens in a new window. Only computers appear in the report.' Below this are several configuration options: 'Select update classification:' with radio buttons for 'All' (selected), 'Important updates', and 'High-priority updates', and a 'Select update classification:' dropdown; 'Select update status:' with a dropdown set to 'Pending'; 'Select MSRC rating:' with a dropdown set to 'Not specified'; and 'Select effective approval:' with a dropdown set to 'All'. On the right, there is a 'Select device groups:' section with a text box containing 'All Devices' and an 'Edit...' button.

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

Summary

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. This most recent update extends client support to Windows 8, Windows RT, Windows Phone 8 using Windows cloud services, and Apple iOS devices. Windows Intune can help you support a “bring your own device” environment so your employees can concentrate on their jobs while you help manage their computers and mobile devices—regardless of location.

This guide has taken you through some of the key tasks you can perform to set up and manage your computers during your initial period with the Windows Intune cloud service. We hope you find your time with Windows Intune valuable. Finally, if you would like to learn how System Center 2012 Configuration Manager with SP1 can be configured to use Windows Intune to manage mobile devices in your organization, see [What’s New in Configuration Manager SP1](#) on TechNet Library.

Resources:

Windows Intune website: <http://www.windowsintune.com>

Windows Intune Online Help: <http://onlinehelp.microsoft.com/en-us/windowsintune.latest>

Windows Intune TechNet: <http://technet.microsoft.com/windows/intune>

Windows Intune Team Blog: <http://blogs.technet.com/b/windowsintune/>

Some information relates to pre-released product and services which may be substantially modified before this product is commercially released. Microsoft makes no warranties, express or implied, with respect to the information provided here. Some products and services are not available in all languages or in all countries or regions and may be taken from the English version of prerelease software. Some features and functionality may require use of the Windows Intune service and System Center 2012 Configuration Manager SP1.

© 2012 Microsoft Corporation

