****

**Getting Started Guide: Part One** *Configure your Windows Intune environment*

Contents

[Welcome to the Windows Intune Getting Started Series 2](#_Toc300148826)

[Setup 2](#_Toc300148827)

[Getting Started with the Administration Console 2](#_Toc300148828)

[Adding Administrators 4](#_Toc300148829)

[Setting Your Default Policies 5](#_Toc300148830)

[Summary 7](#_Toc300148831)

[Additional Resources: 7](#_Toc300148832)

#

# Welcome to the Windows Intune Getting Started Series

Learn how you can get the most out of Windows Intune with the Getting Started Guide series, a set of tutorials designed to help you set up your new Windows Intune environment and explore the main features of Windows Intune.

In this document, the first of three tutorials, we will help you set up your Windows Intune environment so that you can manage and secure enrolled PCs through the web-based administration console. The second tutorial will help you install the client software on PCs you will manage and configure groups to help organize the computers you have added to the service. In the final tutorial, you will learn how to assess the health of your computers and take action on a day-to-day basis.

To help in illustrating the guidelines and recommendations in this guide, we have created a number of demonstration environments throughout the document; 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.

# Setup

During the Windows Intune signup process, you will be asked to provide a Windows Live ID and basic contact information to identify you as the owner of the subscription agreement. Once this information has been completed, an email will be sent to the Live ID’s email address confirming the account is active. You can click on the link included in your email or simply browse to: [manage.microsoft.com](http://manage.microsoft.com/).

Windows Intune requires no new network or server infrastructure and minimal PC hardware requirements – basically no more than those needed for the operating system itself. In order to manage PCs with Windows Intune, the client computers just need to have Internet access and the Windows Intune client software installed on the PC. As an administrator of the service, you should also make sure the browser you will be using to manage Windows Intune has Silverlight 4.0, or later, installed.

# Getting Started with the Administration Console

When you logon to the service, you are presented with the Windows Intune System Overview page in the Windows Intune Administration console; this Silverlight application will provide you with rapid access to the management features of Windows Intune. The screen will look similar to that shown in Figure 1:



Figure 1: Windows Intune Administration Console System Overview screen

In this screen, you can see the three main information panels for Windows Intune. On the left is the Navigation panel that contains the links to the Windows Intune workspaces. Workspaces is how we refer to the various features of Windows Intune. You can click on **Computers** to create computer groups; manage **Updates** or **Endpoint Protection**, view **Alerts** for potential issues; gather insight into **Software** inventory across  managed PCs and deploy new software to PCs; view the status of installed Microsoft **Licenses** against entitlements; set a basic security **Policy** such as firewall management; create and save customized template-based **Reports** on items such as software and hardware inventory and licensing compliance;  and lastly,  complete  **Administration** tasks that can include deploying the client software on each PC or adding administrators. In the middle of the screen is the main information panel that provides the detail view for the workspace (in this example the Systems Overview workspace). Finally, on the right is the Tasks panel that provides a context sensitive list of available tasks for that view as well as points to additional information to help guide you through the task as needed..

At this point you have no computers enrolled into the system so there is not much information here, but you can start to familiarize yourself with the workspaces and tasks available in each.

For example, if you click on the **Computers** icon in the navigation panel and then select **All Computers,** you will see the All Computers view that shows the two default computer groups; *All Computers* and *Unassigned Computers*, as shown in Figure 2. As you start adding computers to your account this list will show you all computers you are managing.



Figure 2: Computers Workspace view

So take a few minutes to click through the navigation panel and administration console to get a feel for how the administration console is laid out.

Before you start adding computers to your account there are a few additional steps we recommend to help you get your environment ready for day to day management tasks. Over the next few pages, we will walk you through the steps we recommend you take as well as provide you with insight on the main features of the Windows Intune service.

# Adding Administrators

By default, the subscription owner is made the Tenant Administrator for your Windows Intune service. The Tenant Administrator is the individual who accepted the Microsoft Online Subscription Agreement (MOSA) in the Microsoft Online Services Commerce Portal (MOCP) at the time of purchase and is entitled to perform all tasks in the Windows Intune administration console. If the customer adds a “service administrator” in MOCP, this administrator also has full service administration access in the Windows Intune administrator console.

To add additional administrators that can perform day to day management tasks in Windows Intune – these are referred to as Service Administrators - you will need to do the following:

1. Logon to the Windows Intune Administration Console and click **Administration***.*
2. Click **Administrator Management.**
3. Click **Add Administrator**, you will then see a window similar to that in Figure 3:

**

Figure 3: Add Administrator

1. Enter a valid Windows Live ID in the **Windows Live ID:** box and click **Full access** if you wish to give this Live ID the ability to modify the Windows Intune settings or click **Read-only access** (this is the default) to only allow this ID the ability to view the information in the console then click **OK**.

For customers that are working with a service provider, this is where you can also add your service provider’s Windows Live ID to enable them to manage your account.

Repeat the previous step for all Windows Live ID’s that you wish to make Service Administrators of this Windows Intune account.

# Setting Your Default Policies

Windows Intune policies are focused on providing you with fast and straightforward settings that control the updates, endpoint protection, firewall settings, and the end user experience. These will work no matter what domain your computers are joined to or even if they are non-domain joined.

As these policies can be used to modify the default client behavior during the enrollment process it is recommended that you create a default Windows Intune Agent Settings policy for all computers to establish this baseline.

**Note:** *For many years Microsoft has provided a feature called Group Policy to help manage Windows computers. We recommend that you do not use both Group Policy and Windows Intune policies on the same computers. However, if you wish to do this, Group Policy will take precedence over Windows Intune policies and a policy conflict alert will be generated in the console. For more information see the “Plan for Deployment in Enterprises that are managing by using Group Policy” page in the* ***Policy*** *section of the Windows Intune online help here:* [onlinehelp.microsoft.com/windowsintune](http://onlinehelp.microsoft.com/windowsintune)

The following steps will take you through the process of setting up a set of default Windows Intune policies.

1. From the Windows Intune Administration Console click the **Policy** workspace tab.
2. Under the **Tasks** panel click “**Create a New Policy**”. At the Create New Policy Wizard, highlight the Policy Templates.

You can see here that we have three types of policy we can create: Agent settings, Tools settings, and Firewall settings.

1. Select the **Windows Intune Agent** **Settings** template and click **Create Policy.**

The Agent settings will control the endpoint protection and software update settings for the agents on the managed computers. You can Scroll down the settings and review the available settings such as Scan Schedule for malware, SpyNet membership, and Update detection frequency. If you click the information icon next to each setting you can read details of the setting along with a recommended value, where appropriate, as shown in Figure 4.

**

Figure 4: Online Policy details

1. *Once you have configured the settings you wish to apply in your default policy click* ***Save Policy****.*
2. *At the Deploy Policy window click* ***Yes*** *and then select the* ***All Computers*** *group to deploy this policy to all computers you are managing.*

You can now repeat this process for both the **Windows Intune Center Settings** and **Windows Firewall Settings** policy templates. The Windows Intune Center Settings allow you to configure the contact information that will appear in the Windows Intune Center on the client computers. You can set details such as email addresses or telephone numbers for clients to contact if they need IT support. The Windows Firewall Settings policy allows you to control the computers’ local Windows Firewall and create exceptions to open specific firewall ports that will enable or disable features such as File and Print services or remote administration.

Once you have the default policies in place, you can apply more specialized policies to other groups in your organization if required. If you do this, all policies will be applied to the computers in those groups but it is the policy that is applied lowest in the group hierarchy that will take precedence if a policy setting is conflicting.

# Summary

This guide has taken you through some of the key tasks to get you started setting up your Windows Intune environment ready to manage and secure enrolled PCs. In the second installment, you will learn how to install the client software on your managed PCs and set up computer groups within the administration console. 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)

