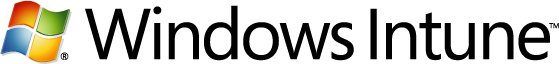
****

**Getting Started Guide: Part Three** *Get insight into your PC environment*

Contents

[Welcome back to the Windows Intune Getting Started Series 2](#_Toc300155398)

[Creating Reports 2](#_Toc300155399)

[Customizing Report Templates 2](#_Toc300155400)

[Creating a Malware Status Report 4](#_Toc300155401)

[Using Workspace Filters 4](#_Toc300155402)

[Creating Software Inventory Reports 6](#_Toc300155403)

[Deploying Software 7](#_Toc300155404)

[Working with Remote Assistance 8](#_Toc300155405)

[Working with Multiple Accounts 10](#_Toc300155406)

[Summary 12](#_Toc300155407)

[Additional Resources: 13](#_Toc300155408)

# Welcome back to the Windows Intune Getting Started Series

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

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

* Add administrators to the administration console
* Set your default policies
* Enroll client PCs
* Organize your computers
* Manage update and automatic approvals
* Set up alerts notifications

This tutorial will help you learn how to assess the health of your computers, create custom reports, deploy software and remote control a managed computer using Windows Intune Remote Assistance.

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

# Creating Reports

How many computers have a particular application or update installed? What malware was blocked? How many computers have less than 2 Gigabytes (GBs) of physical memory installed? Which users needed Remote Assistance over the last month? If you find yourself asking these questions, Windows Intune can help you create reports to get this view. We have developed a set of reports templates you can use or create custom reports based on views within the Windows Intune workloads. All these reports can be printed out or exported as either HTML or comma separated value (CSV) files. This allows you to export the data from Windows Intune and import it into whatever programs you need for further manipulation. For example, you could use Microsoft Excel to take the CSV data and create a detailed and formatted spreadsheet.

### Customizing Report Templates

The following steps will take you through the process of creating a Windows Update report to help identify all computers that have pending Updates waiting to be installed:

1. Click the **Reporting** workspace tab.
2. Click the **Update** reports.
3. Customize the report settings to look like those in Figure 12:

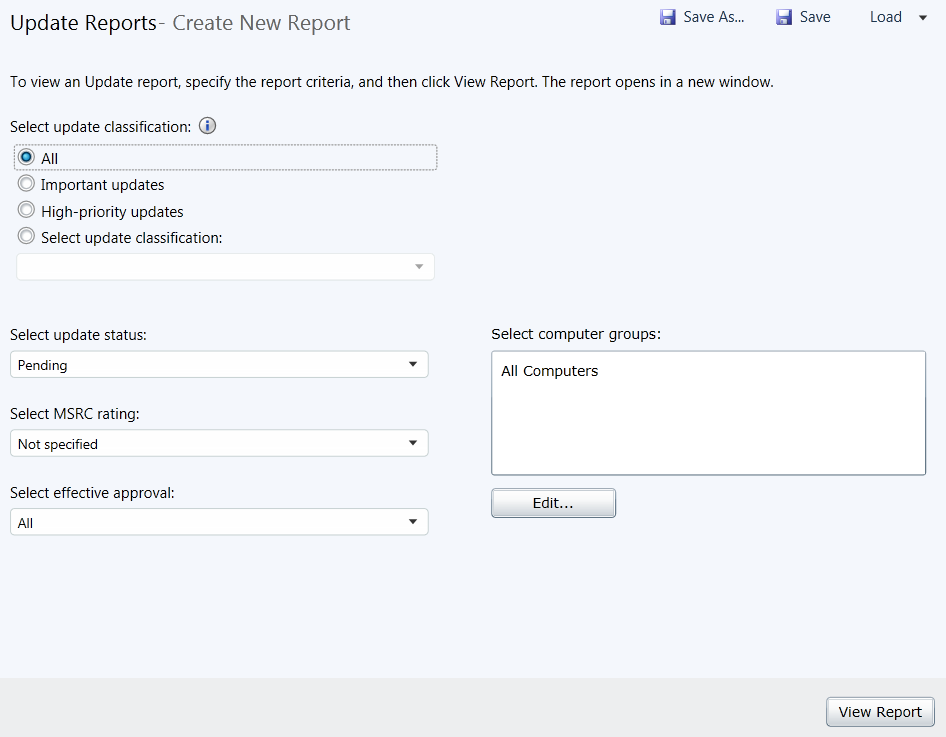


Figure 12: Custom Update Report

1. If you wish to safe this custom report for future use you can click **Save** and provide a name so you can load it in the future
2. To run the report click **View Report.**

This will generate a report similar to that shown in Figure 13. Using this information you can identify those computers that have updates outstanding and start the process of troubleshooting the updates.

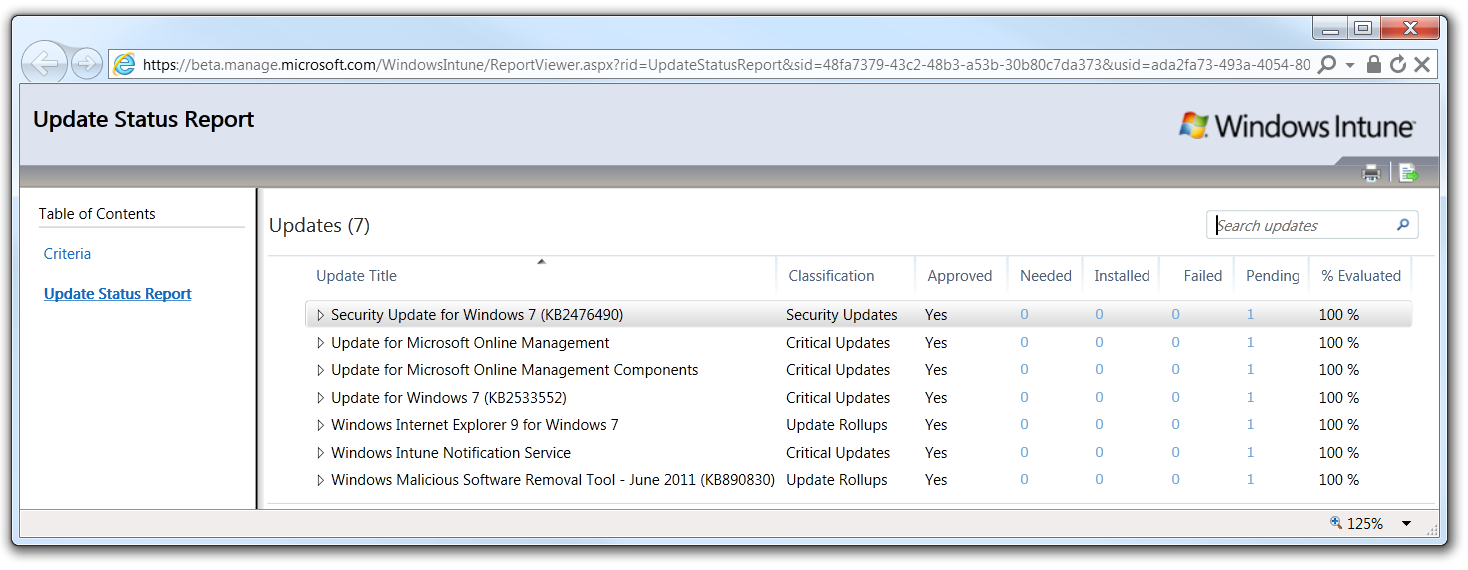
**

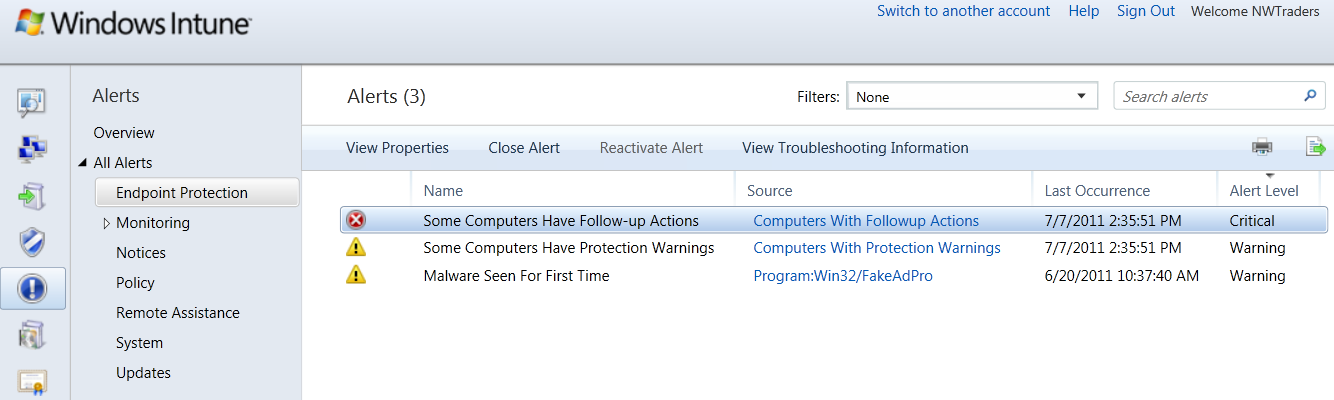
Figure 13: Custom Update Status Report

### Creating a Malware Status Report

The majority of time, the Windows Intune Endpoint Protection feature will generate informational alerts that are designed to give you an up-to-date view of malware that has been detected and removed from any of your managed computers. For those times that some follow up is required, the Alerts will be marked as urgent so you can contact the user and use the Remote Assistance feature to help perform any follow up tasks. The following steps show you how to create a Malware Protection report:

1. Click the **Alerts** workspace tab and select the **Malware Protection** option.

This will display a list of the current malware incidents recorded on all managed computers see Figure 14:

Figure 14: Malware Protection Report

1. To export this view, click the icon in the top right-hand corner of the screen.
2. Select either **HTML** or **CSV** as your preferred export file type and click **Export**.
3. In the **Save As** window enter the path and file name for the export file and click **Save**.

This will create the exported report which you can then use in your preferred reporting or data application as required.

Wherever you see the print or export icons  in the Administration console you can export the data in that view.

### Using Workspace Filters

In this section you will look at the filters that are available in the Administration console Workspaces to help you generate additional reports. The following steps will take you through the process of creating a Computer details report:

1. Click the **Computers** workspace tab and select **All Computers**.
2. From the Filters drop down box, select Hardware classification filter.
3. From the Filters drop down box, select the Computer details and user account filter.

This filter will display a view of the computer in your environment that includes the Chassis type, Manufacturer, Model, as well as the Operating System, Disk Space details, and many more details. By right-clicking on the data columns you can customize exactly which columns appear in the view as shown in Figure 15 below:

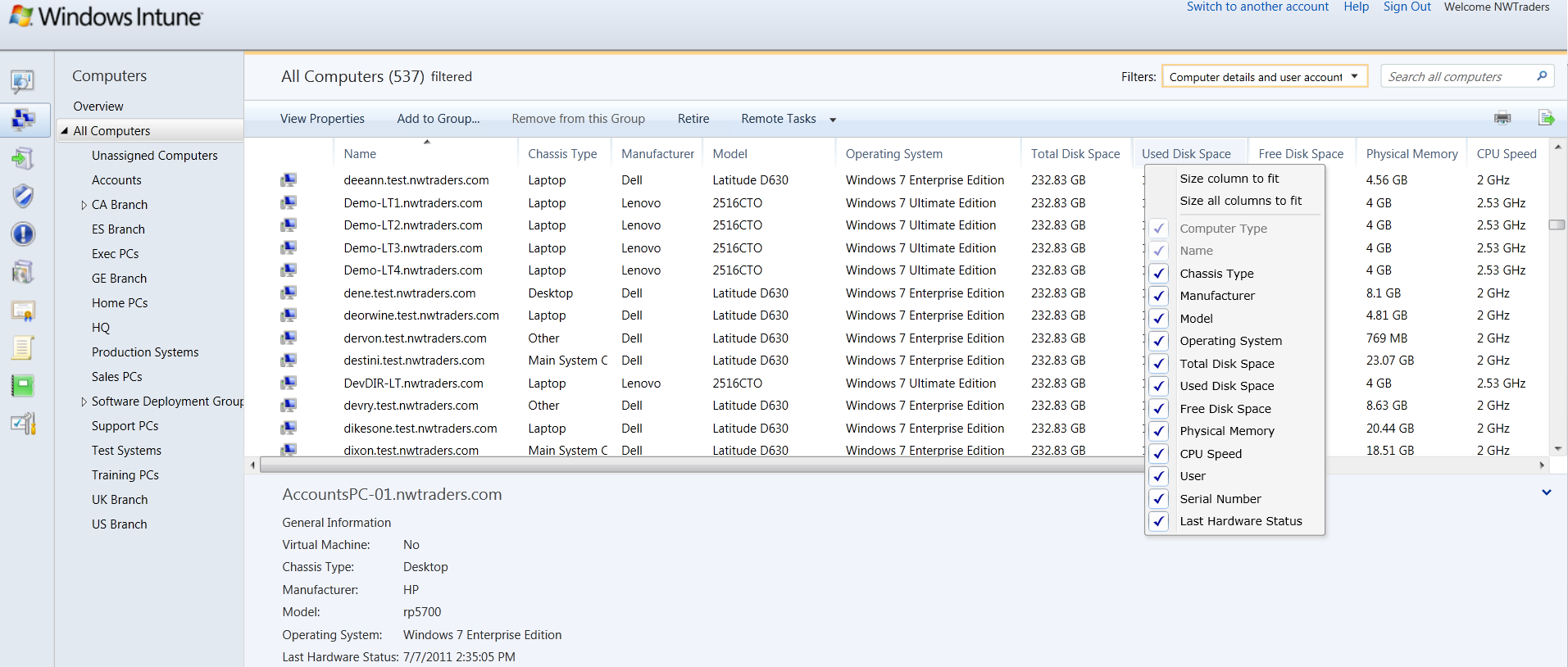
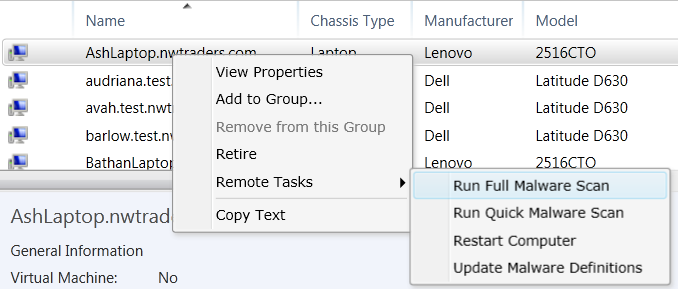


Figure 15: Computer Details and User Account

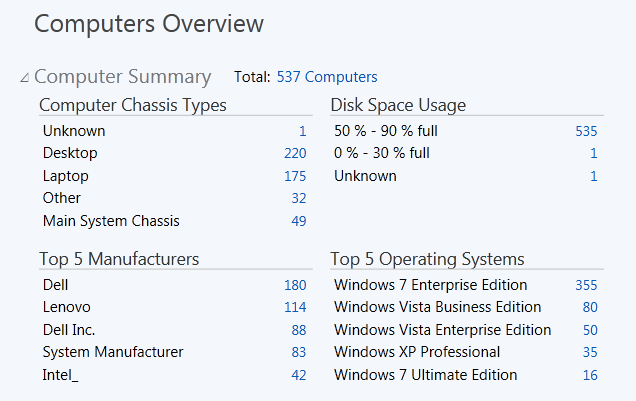
1. Now using the **Print** and **Export** icons described in the previous section, you can create a printed report or export this view to a CSV file.

In addition to using these filters to print or export data you can also perform actions against the computers in the view. For example, if you right-click on any computer in the view you are able to perform a number of tasks on that computers. These tasks include viewing the computer properties, adding the computer to a group or even retiring the computer from the Windows Intune managed service. You can also select the **Remote Tasks** option to instruct that computer to perform one of a number of tasks as soon as possible. If the computer is online it will be performed within a few minutes, if the computer is offline the task will be queued and performed once the computer is next able to check in with the Windows Intune service. Figure 16 shows the four remote tasks that can be sent to a managed computer.

  
Figure 16: Remote Tasks

### Working with the Computers Overview

The Computer workspace can also provide you with rapid access to additional information and tasks that can be performed on these computers. For example if you click on the **Computers** workspace icon you will be taken to the **Computers Overview** view, then click **Computer Summary** option to display current status information on a number of key computers metrics, as shown in Figure 17:

  
Figure 17: Computer Summary

Clicking the **Computer Summary** link will toggle this view on or off as needed. Each of the numbers indicated next to each item in the list is a hyperlink that allows you to drill down to the filtered view that will show you exactly which computers meet have those characteristics.

### Creating Software Inventory Reports

As you install the Windows Intune client software on your computers, a detailed inventory is built of the software installed on them and reported back to the Windows Intune service. Using either the Software workspace or by using the Software report in the Reports workspace, you can review, print, or export this information.

One key piece of information required by many organizations is a computer by computer list of all software installed. The following steps will take you through the process of creating this report in Windows Intune:

1. From the Windows Intune Administration Console, click the **Reports** workspace tab.
2. Select **Software** **Inventory Reports**.
3. Leave all the other customization options at their default “All…” state and click **View Report.**

This will generate a detailed software report identifying and categorizing all software installed on the computers in the Windows Intune environment. As this is a Silverlight-formatted report, you can drill down into the details of which computers have which software installed. To export a full detail report of this information, follow these steps:

1. Click the Export  icon
2. Once the **Export Dialog** Windows opens, select **.csv File**.
3. Uncheck the **Export summary data only** option and click **Export**.

This will export a CSV file containing a list of all software found in the environment and which computers have the software installed. This includes any software recognized by the service and is not limited to just Microsoft products. This information can then be imported into Microsoft Excel to be formatted and customized as required.

# Deploying Software

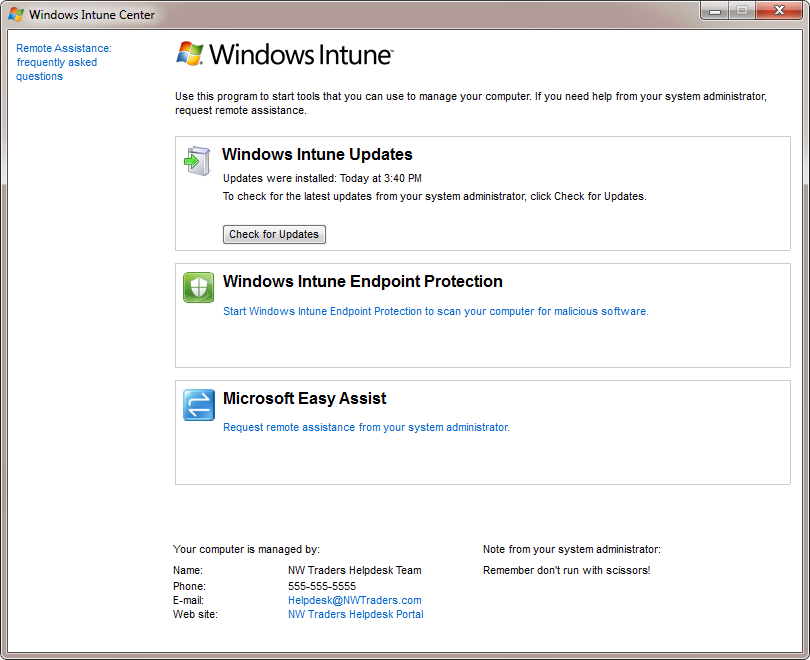
A new feature in Windows Intune is the ability to create, store and then deploy software via the cloud. This process extends the update management process described earlier in this guide to allow you to deploy a new application to a managed computer wherever they are in the world. The process starts at a Windows Intune administrator’s computer that has access to the required software installation files; these can be in the form of either EXE or MSI files. For both file types it is important that they support silent installation, this is where the package can be installed without user interaction. This allows the Windows Intune agents to install the software regardless of whether the computers user has rights to install software or even if they are logged on. The methods to enable a silent installation do vary between software packages, so you will need to check with the software publishers documentation to determine the exact method to use, for example the */Quiet* or */Silent* command line arguments are often used to indicate a silent installation option.

From the **Managed Software** workspace the administrator uses the **Upload** wizard to create the compressed and encrypted package and uploaded it to the Windows Intune service that package is available to be deployed to the Windows Intune groups in the same way as application updates. However it is important to understand that software installation packages are typically larger than software updates and therefore you may need to take steps to help minimize the possible impact of a deployment on a sites Internet connection. To help explain this process, in detail, and document best practices for using working with software deployments with Windows Intune we have created the *Best Practices for Deploying Software with Windows Intune* guide at: [www.microsoft.com/download/en/details.aspx?id=26705](http://www.microsoft.com/download/en/details.aspx?id=26705)

Once you have familiarized yourself with this guide you will have all the information you need to deploy software applications to all your managed computers.

# Working with Remote Assistance

Now let’s take a look at a very useful feature of Windows Intune and that is Remote Assistance (RA). This feature allows you to view and control a managed computer remotely so you can support your users virtually anywhere and regardless of whether you are in the office or on the road. The RA process starts when an end-user opens a request for remote assistance. This is done using the Windows Intune Center client software you installed on the managed computer. Click on the Windows Intune Center and you should see a window similar to that shown in Figure 18:

  
Figure 18: Windows Intune Center

The RA feature uses Microsoft Easy Assist to enable an RA session. Once the user has clicked the Microsoft Easy Assist option, a Remote Assistance Alert is sent to the Windows Intune service.

***Note:*** *Microsoft recommends that you setup E-Mail Notifications for Remote Assistance alerts to ensure that emails are sent to administrators automatically to help minimize the wait time for an end-user. See the “Set up Alerts Notifications” section of the previous guide for information on setting these up.*

The following steps will take you through the process of responding to a RA request:

1. From the Windows Intune Administration console, click the **Alerts** Tab
2. Click Remote Assistance to view Remote Assistance requests.

***Note:*** *RA alerts are set as Critical and they will also appear in the* ***Alerts by Type*** *section of both the Systems Overview workspace and the Alerts Overview workspace.*

1. Click on the RA request to see the details of the request, as shown in Figure 19.

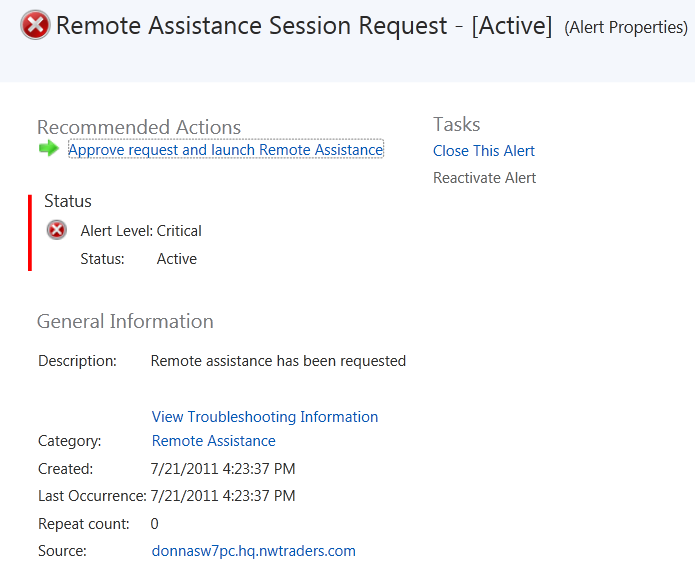
**

Figure 19: Remote Assistance Request Details

1. Under **Recommended Actions**, select the **Approve request and launch Remote Assistance** link.
2. In the **A New Remote Assistance Request is Pending** window, click **Accept the remote assistance request** link.
3. Click **Allow** on the Internet Explorer Security pop-up to allow the rtcearouter.dll to run.
4. Enter a **Display Name,** such as Helpdesk for this RA session; click **Join**

The Microsoft Easy Assist session Window will now open and you will need to wait until the end-users computer is joined to the session. This process can take a few minutes depending on the network bandwidth available. Once the session has been established, the end-user will see the Microsoft Easy Assist control request windows as shown in Figure 20:

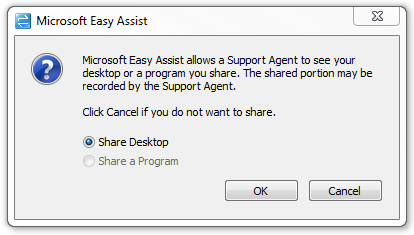
**

Figure 20: Microsoft Easy Assist Control Request Window

At this point the end-user will need to click **OK** to allow you to see their desktop. Once they do this, you will be able to see their desktop in a window on your desktop.

1. To control their desktop, click **Request Control** in the top Left of the RA session window.

The end-user will now be shown the following message in Figure 19:

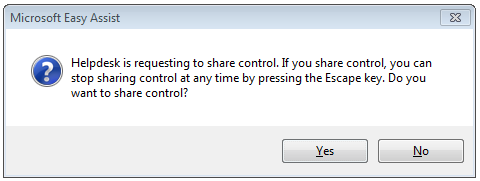


Figure 19: Remote Assistance Control Request

Once the end-user clicks **Yes**, you will be able to control their computer. Also available during the session are the options to chat and transfer files to and from the RA session. These options are accessible using the main session controls. At the end of your support session, Microsoft recommends that you return to the Administration console and close the original RA alert. This way it will be easier to identify new requests when they come in.

# Working with Multiple Accounts

Up to this point we have assumed that you are responsible for a single Windows Intune environment. However, Windows Intune can be used for supporting multiple environments from a single Windows Live ID.

If the Windows Live ID account you logon with has been granted Service (or Tenant) administration rights to *more than one* Windows Intune environment, you will be taken to the Multi-Account Console when you logon, see Figure 22:

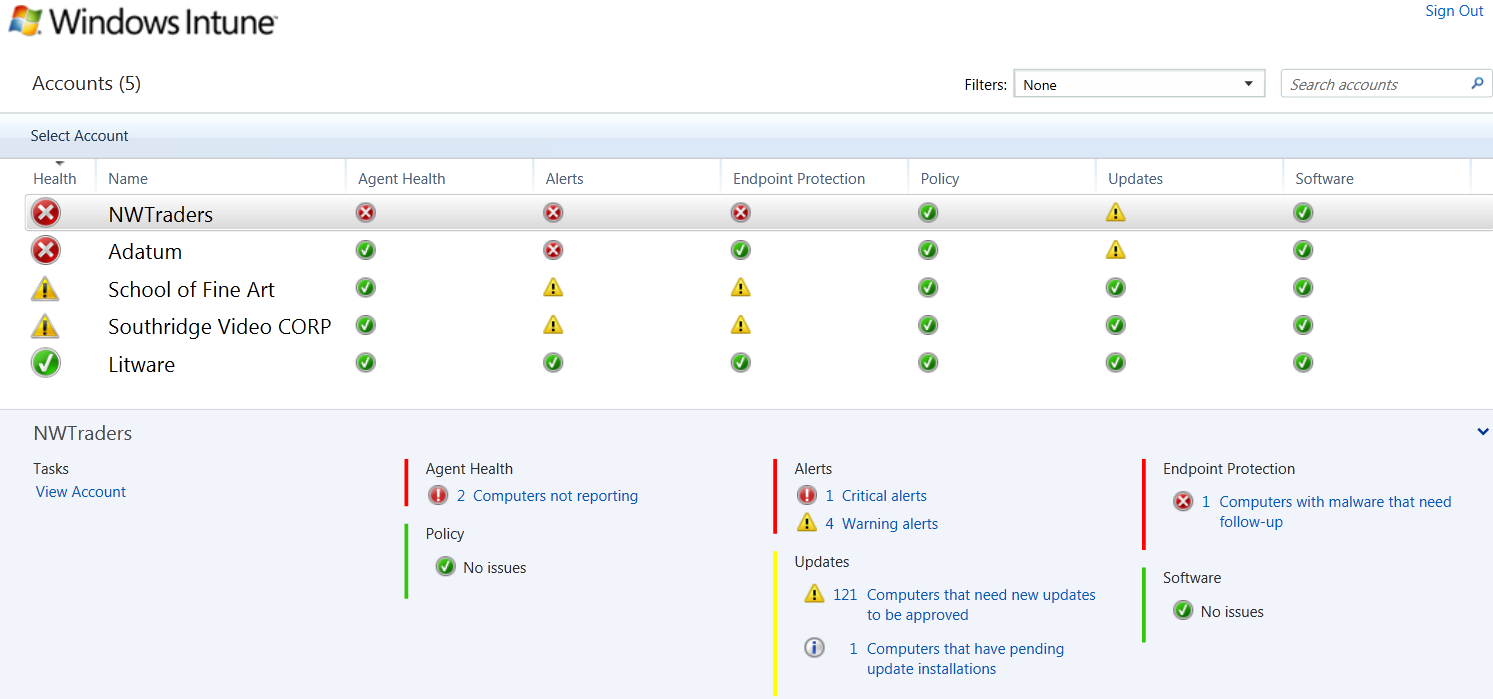
**

Figure 22: The Windows Intune Multi-Account Console

When you log on, the Windows Intune service checks if your LiveID is an administrator for more than one Windows Intune environment. If it is, the service will automatically show the Multi-Account Console so you can select the accounts you wish to manage. This feature was added specifically to help Service Providers or large IT support organizations manage multiple customer accounts.

Each line in the list represents the latest account status of the respective managed accounts. As the list grows, you can use the sort and search features to help get to the information you need fast.

You can quickly find an specific account, even in the longest lists, by typing an account name (or part of one) in the **Search accounts** field.

To get to the details of a specific account, simply click anywhere on the account line in the console and then click the **Select Account** menu option or the **View Account** link and you will be taken to the System Overview view of that account.

You can always be sure of the account you are working in as the the account label is presented in the top right of the Administration Console as highlighted in Figure 23:

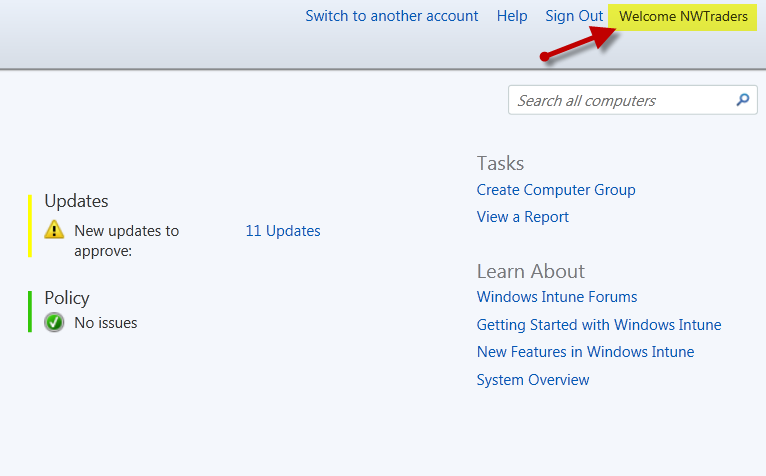


Figure 23: Administration Console Account label

You can switch back to the Multi-account console at any time by clicking the **Switch to another account** hyperlink next to the account label.

The Multi-Account Console is designed to make the task of managing a number of different accounts quick and easy for you.

# Summary

This guide has taken you through some of the key tasks you can perform to manage your computers with the Windows Intune cloud service. For guidance on using the software deployment feature of Windows Intune we recommend you read the *Best Practices for Deploying Software with Windows Intune* guide at: [www.microsoft.com/download/en/details.aspx?id=26705](http://www.microsoft.com/download/en/details.aspx?id=26705)

There are many more tasks and features available that you will discover as you use the service. If you need additional help and guidance we recommend you review checkout the additional resources listed below.

If you are evaluating the 30-day trial and wish to convert to the full Windows Intune service, 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:

<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: [http://blogs.technet.com/windowsintuneblogs.technet.com/windowsintune](http://blogs.technet.com/windowsintune)

Windows Intune FAQ: <http://www.microsoft.com/windows/windowsintune/windowsintune-faq.aspx>

