Microsoft Windows Intune 2.0: Quickstart Administration

Chapter No. 9
"Monitoring and Responding to Windows Intune Alerts"
In this package, you will find:
A Biography of the author of the book
A preview chapter from the book, Chapter NO.9 "Monitoring and Responding to Windows Intune Alerts"
A synopsis of the book’s content
Information on where to buy this book

About the Author

David Overton has been in the IT industry for over 25 years and has worked at Microsoft in the UK for more than eleven years. David fell in love with Small and Medium Business when he was given responsibility for engaging with journalists at the time of the launch of Small Business Server 2003 in the UK. He has also written "Small Business Server 2008 Installation, Migration and Configuration". For the next four years, David was responsible for improving SBS deliveries by Microsoft partners. David has since has moved on to other roles inside Microsoft, but still continues work with a number of small and medium businesses and Microsoft partners.

David's role at Microsoft includes working with organizations who are moving towards cloud based computing models and he personally became involved with the Windows Intune product as a result and now leading to this book after working with both the UK and US teams in his role.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
Besides his day job, David is also a writer: he has written for consumer publications, Windows XP and Windows Vista magazines, and he blogs at http://davidovertont.com, where he helps readers find solutions to questions and problems. In 2009, David published his first book on SBS 2008 which was well received.

When not working or writing David likes to spend time with his family and also tries to fit in sailing any time of the year in any weather.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
Microsoft Windows Intune 2.0: Quickstart Administration

Microsoft Windows Intune is a cloud service solution that simplifies how small and mid-sized businesses manage and secure PCs using Microsoft cloud services and Windows 7—so your computers and users can operate at peak performance all the time.

This step-by-step guide will show you how to plan, set up, and maintain Windows Intune, showing you how to manage a group of PCs (either one business or several) from the base operating system, through to the patches, anti-malware solution and deployed software and policies from a central console, using the Windows Intune service.

This book takes you through all the steps to plan, set up and maintain Windows Intune and how to manage a group of PCs. The book starts by providing an overview of cloud computing and PC management. The book then dives into topics such as Windows Intune features, signing up for Windows Intune and installing the client software, configuring Windows Intune, proactive management, and monitoring and dealing with alerts, including remote assistance among others. As Windows 7 is part of Windows Intune, the book will also cover the minimum steps required to move from Windows XP to Windows 7 while keeping user settings and preferences.

What This Book Covers

Chapter 1, Overview of Cloud Computing, explores the new cloud computing and cloud-based services world that we are moving rapidly towards and includes Windows Intune. Before we can embark on this journey it is important that we understand the benefits and pitfalls that cloud services bring with them and how they apply to us. One mechanism to help protect us against the uncertainties is the use of Service Level Agreements, which are explained for Windows Intune.

Chapter 2, Introduction to PC Management Concepts, introduces the important concepts behind PC management, with a focus on ensuring that the needs of the business are the fundamental driver of the IT policy we implement with Windows Intune. We then explore how the IT policy decisions are taken to reflect these needs and are then able to demonstrate that they are delivering on them.

Chapter 3, Overview of Windows Intune Features, describes the features within Windows Intune, ensuring that we can take advantage of all of the benefits it has to offer, including anti-malware software, update management for both the Windows Operating System, and Windows applications, software distribution, system alerts and reporting.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
Chapter 4, Signing Up for Windows Intune and Installing the Client Software, walks through the Microsoft Online Services Portal, configuring the service administrators, and if desired, assigning a partner to assist us. We also download and install the Windows Intune client software and ensure it is up and running on each computer.

Chapter 5, Configuring Windows Intune, runs through the configuration steps for Windows Intune. This starts by adding additional administrators to the system to allow multiple system’s managers. We then configure the computer groups for the management process. We enable the alerts that Windows Intune will raise and configure who they are sent to. Finally, we configure the Microsoft and non-Microsoft software license purchases so Windows Intune can report on compliance to this.

Chapter 6, Configuring Management Policy, enables us to construct the policies that Windows Intune uses to configure each computer. This covers firewall, anti-malware, and operating system and software updates. The Windows updates section includes configuring which update categories are checked on each computer to see if they are required and the deployment policy options, either manual or automatic approval.

Chapter 7, Software Deployment, using Windows Intune can be a complex process as all software must be installed silently and with all the files in one location. We explore the process, setting up the command switches and including the right files for a number of common applications as working examples.

Chapter 8, Tracking and Reporting, is a key activity to demonstrate that we are delivering a useful service. We explore the activities required to track the hardware and software managed by Windows Intune and then the reporting options for software use, alerts, and hardware tracking. Since custom reports are often desired, we also look at how these could be delivered into a spreadsheet and then enable greater insight if desired.

Chapter 9, Monitoring and Responding to Windows Intune Alerts, requires different responses depending on the alert and the level. We will examine how to monitor the computers and deal with the special case of remote assistance alerts that a user can request and require an almost immediate response due to the fact that someone is waiting for us.

Chapter 10, Resolve Problems Using Microsoft DaRT, is an optional purchase with Windows Intune that is delivered as part of the Microsoft Desktop Optimization Pack. It can be used to resolve deep technical issues that stop a computer booting or being accessed by a user. We will understand how we can repair a system, change passwords, and edit the devices configured on a computer. This is a critical for all IT desktop managers.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
Chapter 11, Deploying Windows 7 Enterprise Edition, is something many of us will have to do and is made easier as Windows Intune includes the license required to update to the latest version of Windows. We will cover the process of migrating from Windows XP to Windows 7 Enterprise Edition. This includes moving the user settings from one system to another and then updating Windows Intune.

Chapter 12, Integration with Existing Microsoft Products, is an area we explore as many of us will use Windows Intune with other Microsoft technologies. We examine how Window Intune interacts with other Microsoft products and whether they are a natural fit for use with Windows Intune.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
Monitoring and Responding to Windows Intune Alerts

So far we have examined the configuration of the computers with policies to control their behavior. As we manage these computers, they will report back to Windows Intune against those policies in the form of reporting and alerts. We have looked at the reporting, which provides a snapshot of the computer estate. In this chapter, we will examine the real-time nature of PC management as we explore the alerts that Windows Intune raises which require action on our part, exploring how we both monitor and respond to them.

In the previous chapters, we have configured the computers to minimize the situations where alerts will be raised through good practices of updates, firewall, and anti-malware management. Problems will still arise with users' computers, whether this is a request for assistance, a computer that will not boot, or some other warning picked up by Windows Intune. These need to be categorized and responded to in a timely manner. Some can be closed and filed depending on circumstances, while others require a visit to the computer itself with other tools to further diagnose and resolve.

In this chapter, we will discuss this in the following sections:

- General Windows Intune alerts
- Malware alerts
- Remote Assistance alerts

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
General Windows Intune alerts

Windows Intune will raise an alert in a number of situations where we, as the administrators, need to either be aware of an event or respond directly to it. The alerts will appear in a number of the screens and reports in Windows Intune. Windows Intune has seven alert categories:

- Endpoint Protection
- Monitoring
- Notices
- Policy
- Remote Assistance
- System
- Updates

Some of these alerts require special attention and have their own section, while others can be generically dealt with. The two areas that need some special attention are the Endpoint Protection alerts relating to malware and remote assistance, as the actions taken here always need to be decisive. We have also already tackled the update alerts in the previous chapter.

Before we examine alerts in more detail, I thought I should share a quick, but obvious, note. The reporting of alerts from the client computer to Windows Intune requires an Internet connection from the client computer, so we are unlikely to see an alert saying that the user's PC is having network trouble. However, if a computer has not checked in with Windows Intune for a while, we will see an alert for this from Windows Intune, pointing to a machine that has not been turned on for a while, or with problems! It is more likely that a user will contact us via other means if they are having a networking problem, but we should remember to tell users to do that in that situation rather than them requesting remote assistance and wondering why we don't respond!

Monitoring alerts

There are two ways to monitor alerts once they have been enabled and the notification has been completed. The two choices are to either look at the console and refresh, or wait for notifications to arrive via e-mail. The e-mail notifications look similar to the one in the following screenshot. Clicking the link takes us to the Windows Intune console.
To view the alerts in the Windows Intune console, go to the **Alerts** workspace and go to **All Alerts**. We can choose which alerts are displayed by changing the **Filters** selection at the top of the screen. All the filters shown open alerts, except for the filter choice of **Closed**. The filter choice of **None** shows all open **Critical**, **Warning**, and **Informational** alerts.

![Windows Intune Console](image)

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
Monitoring and Responding to Windows Intune Alerts

We can also view alerts specific to the category by selecting one of the items below All Alerts selection tree. For example, in the Monitoring category, we can see one alert at the moment:

Finally, we can view alerts that relate to a specific computer by looking at the Alerts tab in the Computers workspace.
Responding and closing alerts

Once we have an alert to deal with, we need to respond in some way. By clicking on the alert, the details pane is displayed. Under the **Recommended Actions**, there will either be a link to **Click here to take action** or one to **View Troubleshooting Information**.

If we click the information link, a window will open that, depending on the problem and potential solution, will show either a link to the Windows Intune help file or a link to carry out the action if appropriate. In the following example, the alert is for malware and a link to information on the specific malware that was seen. We can see that the following information does not show us a specific action for malware. We will discuss how to respond to malware a little later in this chapter.
Once we have resolved the alert, it needs to be closed to remove it from the console and to enable us to demonstrate that we have resolved an issue with computers that we manage. Windows Intune will not close the alert for us unless one of these criteria is met:

- Windows Intune can detect that the issues have been resolved
- 45 days have passed since the alert was opened

To manually close an alert, follow these steps, but be careful to close the right one. While we can re-activate a closed alert in Windows Intune, if the alert is closed by mistake then we may miss taking important action.

1. Open up the Windows Intune console and find the alert to close. We can select more than one alert if desired here.

2. Click Close Alert in the toolbar, or right-click on the alert and select Close Alert from the menu.

We can also close an alert when we have opened it fully and are looking at the Alert Properties by clicking the Close This Alert link under Tasks.
The automated closing of alerts, when an issue has been resolved, can be a little confusing as we see alert e-mails, but then they don't exist in the console. This is most common when malware and policy issues occur as Windows Intune can detect the resolution of these. It is always worth checking the closed alert log to ensure these do not require further action or highlight an underlying issue, such as network or security, that needs resolving. A good example of where we might see this is with the **Unable to Update Policies** alert which are generated when a user's computer is not in contact with Windows Intune. The alert e-mail looks similar to the following screenshot:

![Alert Screenshot](https://manage.microsoft.com/Site/App.aspx?accountid=c9df365-b47b-44be-abea-34a0d8f7fb#P=/alerts/alert/&A={AL-201817})

This is the type of alert that will be automatically closed once connectivity is resolved and the policies updated.

**Malware alerts**

Malware alerts fall into two broad categories; those that indicate a problem with the anti-malware software that installs as part of Windows Intune and those that indicate the anti-malware software has detected and responded to a malware threat.

The alerts I have seen are:

- Anti-malware software issue
  - Some computers have protection warnings
- Malware detection
  - Malware seen for first time
  - Some computers have recently resolved malware

For More Information:

Monitoring and Responding to Windows Intune Alerts

The first alert requires investigation to ensure the machine in question is properly protected, but something as simple as a user cancelling a full scan will generate this error. A quick call to the user or visit from a technician to look at the Windows Intune software will resolve this. This alert can automatically close if the situation is resolved.

For the malware detection alerts, these need closer management. When a user first encounters malware they are prompted by Windows Intune to remove it. At this point, the first alert will be sent. The user is prompted with a choice as to the action to take. If the malware Alert Status is considered to be Medium or Low, then the user may Allow the files to remain as the Recommended action. Once the user has made the choice, the second alert is sent stating that a recent malware issue has been resolved, whether the file was allowed to stay on the hard disk or not.

The only time when a file should be allowed is when it is misevaluated as a virus. The best way to resolve this is to create an exception policy in Windows Intune specific to the computers and the program of filename.

Once we are satisfied that the situation is correctly resolved, we can close the alert in Windows Intune if it does not do this itself.

Testing malware checks are working

To test that various aspects of an anti-malware system are working, it is vital that we do not use a live virus. Just as in the medical world, the IT world has a universally accepted virus file that does not cause harm and can be used for testing. This is simply a file that has the signature of a dummy virus, not a virus itself. This can be downloaded from EICAR at http://davidoverton.com/r.ashx72O. Downloading any of these files should trigger Windows Intune Endpoint Protection or any other anti-malware solution.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
Distributing this file is a little tricky as the download will be blocked by default by Windows Intune, as will copying the file, which means that disabling the malware protection is required to obtain the file.

### Actions following malware instance

Once we know that a computer has had a malware incident, we need to gain confidence that the issue has been resolved. Through policy we are able to decide if a user can **Allow a file**, however, we may wish to take additional precautions.

First, we need to identify the computers by opening the alert up by going to the Windows Intune console and selecting the **Endpoint Protection** in the **Alert** workspace.

If we click on the link shown as the **Source**, we will see the computers impacted.

---

*For More Information:*

www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
Monitoring and Responding to Windows Intune Alerts

We can now remotely run a number of operations on the computer in question. For malware issues, select the computer or computers that we want to inspect and then select Remote Tasks from the toolbar, or right-click on the computers. Then select either Run a Full Malware Scan or Run a Quick Malware Scan.

We will see a confirmation dialog box for the request to run a scan for a short period of time before it disappears. We can check the progress by clicking on the Remote Tasks link in the bottom-right corner of the console which will show us the status, similar to those in the following screenshot:

Remote Assistance alerts
A Remote Assistance alert is generated when a user requests help from the Windows Intune Center by clicking the link under Microsoft Easy Assist.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
When the user clicks the link on their computer, the Microsoft Easy Assist changes to look as follows:

![Microsoft Easy Assist](image)

While there are many remote administration tools available for Windows the Microsoft Easy Assist tool has the following benefits:

- Secure connection through corporate firewalls providing users access to the Internet and websites
- **Desktop sharing** – the user requesting assistance can either show the support person the problem or hand control over completely
- **Application Sharing** – rather than share a whole desktop, just an application can be shared
- **File transfers** – we can upload and download files so scripts or exported data can be shared between the support person and the computer being supported
- **Chat application** – if we can't talk to the person being supported, we can still type in an instant messaging chat window
- **Multiple person assistance** – if the particular problem needs another person to assist or offer guidance, this is possible using the Easy Assist tool

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
Preparing to deliver support

However, before we can deliver support, it is important to ensure that the Microsoft Easy Assist application is loaded onto the support person's computer and that the user's computer is configured for optimal performance when support is being delivered.

Preparing the client computer for support

Windows Intune configures Microsoft Easy Assist to provide support, however, the configuration of User Account Control (UAC) can mean that every administrative task requires interaction from the user to approve the administrative application being started. To overcome this, search for uac in the start menu. We will see the option to Change User Account Control settings appear as the top result.

Click Change User Account Control settings to start the tool.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
Before we make any adjustments, note where this setting is on the client computer – it is normally at the second notch down. Now, lower this to the third notch down and press OK. This means the user's screen will not dim when the UAC dialogs appear, but it also means that we can accept these, which may be desirable.

If the user does change this setting for us, we must change it back once we have completed the support session.

**Preparing the support agent's computer to offer support**

If the computer we are connecting from has Windows Intune installed, then we already have the client loaded. However, if it does not, we will need to install the Microsoft Easy Assist tool. To do this, go to http://davidoverton.com/r.ashx?28 and run the setup program.

If Easy Assist is not installed correctly and we try to open a remote assistance session, then we will see the following dialog box from Windows:

![Dialog Box](image)

**Providing Assistance**

There is a simple progression that describes the actual process of delivering assistance using Windows Intune. It will consist of the following steps:

- Windows Intune receives the request and creates an alert and sends e-mails
- Support agent starts communicating with the user and a remote session is initiated
- Support is provided and the remote session is terminated
- The alert is closed

Receiving alert and responding

We are first aware of a remote assistance request through the e-mail notification. Follow the steps given to start the remote assistance:

1. Open the e-mail and click the link in it to open the Windows Intune console.

2. In the Windows Intune console, we will see an alert similar to the one in the following screenshot. Click the link Approve request and launch Remote Assistance to start the remote assistance process.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
3. When the windows opens up, click on the link **Accept the remote assistance request.**

![A New Remote Assistance Request is Pending](image)

**A New Remote Assistance Request is Pending**

A Remote Assistance request is pending from user Jane-PC@Jane on computer Jane-PC

Accept the remote assistance request if you want to join the remote session, or close the alert if you do not want to join the Remote Assistance session.

4. This will open a web page that will create a `launch.eas` file. Open this file to start the session.

![Live Meeting](image)

5. Once the **Microsoft Easy Assist** tool has started and connected through the server, we will be asked to provide our display name. Enter a **Display Name** that will be meaningful to the user we are connecting to. It should also distinguish us from other support agents as we may need further colleagues to join us in the shared session. Then press the **Join** button.

![Join Session](image)

For More Information:

6. We will start the **Easy Assist Session** tool on the support agent's console as shown in the following screenshot:

![Easy Assist Session](image)

7. After a few seconds **Easy Assist** will continue on the user's desktop with a question as to whether they wish to share their desktop. We should advise them to click **OK** so that we can see what is on their desktop.

![Microsoft Easy Assist](image)

8. The user will see their desktop reformat itself for sharing, which will include turning off the Aero graphics that are part of Windows Vista and Windows 7.

9. The two way joining into the **Microsoft Easy Assist** support session is acknowledged with a dialog similar to the following screenshot:

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
10. Finally, both users are shown in the **Easy Assist Session** window under participants.

![Easy Assist Session](image)

**Provisioning remote support**

Now that we have access to the remote user's computer, we can manage it as if we were in front of it. We have the following tools available to us:

- Chatting
- Shared Desktop - View the user's desktop while they are in control
- Shared Desktop - Take control of the user's desktop and they can watch
- File transfer between the two computers
- Reboot the remote computer and continue session once logged in by the user

---

**For More Information:**

Monitoring and Responding to Windows Intune Alerts

Chat
There is nothing stopping us talking on the phone to the user who requested assistance, but if this is not available then we have a chat window that can be utilized. Type the text to send and press Send.

Shared Desktop
The desktop is shared when we can both enter the session and see the end user's desktop while they are using the computer.

Initially, this is in a view-only mode, meaning that the support agent can watch, but not do anything. Frequently, it will be desirable for the support agent to take control and this can be delivered by either the support agent requesting it or the user offering it. To take control, follow the steps given:

1. In the Microsoft Easy Assist shared desktop tool, press the Request Control button.

2. The user will have to acknowledge that we are taking control. If they are happy for us to take control, they should press Yes. They can press Esc at any time to stop the control of their computer.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
3. The user will see the small toolbox on their screen that enables them to stop control at any time by pressing the Stop sharing button or pressing Esc.

File transfer
The file transfer facility is a temporary holding area that we can upload to and download files from during the session. The files are automatically removed once the session ends and the total file size that can be stored is 100MB.

To transfer files to the holding area, follow these steps:

1. Press the button on the toolbar labeled Upload and download files.

2. Now press the Upload button. Pick the file to upload and press OK.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
3. We will now see the file in the File Transfer window.

4. Repeat this as required.

Once the files have been uploaded, they can be downloaded on another machine in the session. To do this, follow these steps:

1. Select the files to be downloaded by putting a check mark in the box to the left of the filename.

   ![File Transfer window](image)

   2. Now press the Download button to download the files.

   3. We will be asked to choose a folder for the files to be copied to. Find the right folder and press OK.

   ![File Transfer window](image)
4. The files will now transfer.

**Rebooting the remote computer**

The functionality to reboot the computer is really useful as not only does the computer reboot, but once the user logs back in, it will reconnect back to the same remote assistance session to enable further administrative activity. This is vital if a change requires a reboot mid-way through the process.

To start the process, follow the steps given:

1. Right-click on the users name in the **Participants** list and select **Request Reboot and Reconnect**.
2. We will be asked to confirm that we want to reboot the computer. Press OK to continue.

3. The user whose computer we are providing assistance to will now also be asked to confirm the restarting of their computer. If they agree, they also need to press OK on their computer.

4. We will now see confirmation that remote user has accepted the request to restart. Press OK to remove the dialog.

5. When the computer reboots, the user logs in and they will then see a message telling them that the computer is Attempting to reconnect to the Microsoft Easy Assist server. No additional credentials are required.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
6. Once the reconnection is complete, the support agent will receive confirmation that the user has joined the session. Press OK to close the notification.

![Microsoft Easy Assist dialog box](image)

7. The user will again have to confirm they are going to Share Desktop with us.

![Microsoft Easy Assist dialog box](image)

**Closing the alert**

Once we have finished providing the assistance to the user, we need to uninstall any utilities that were added to their computer and if appropriate, re-configure UAC to the pre-support level. This then leaves us with one final activity, which is to close the alert in Windows Intune.

---

For More Information:

Monitoring and Responding to Windows Intune Alerts

To do this, find the Remote Assistance Session Request in the Alerts workspace and select Close Alert in the toolbar.

Summary

In this chapter, we have examined the process of monitoring the alerts and responding with appropriate actions. These actions have included anti-malware checks as well as interacting with the users directly to understand their issues and helping them through using the Remote Assistance functionality.

In the next chapter, we will look at how to use Microsoft DaRT to resolve more challenging issues that require deeper actions to fix issues, often ones that stop a computer booting, with a skilled engineer sitting at the computer to resolve these issues.

For More Information:
www.packtpub.com/microsoft-windows-intune-2-quickstart-administration-enterprise-through-cloud/book
Where to buy this book


Free shipping to the US, UK, Europe and selected Asian countries. For more information, please read our shipping policy.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.